OMRON

STI SAFETY, TECHNOLOGY & INNOVATION

Future Safety Design

Revision of ISO13849-1 and Performance Level

NEW ISO 13849-1

realizing

Introduction

ISO 13849-1 is the most important standard for regulating the basic principles and performance required of a safety control system for machines and devices.

This standard was greatly revised in November 2006. This revision is expected to cause major changes in the fundamentals of safety system design.

This document was prepared to help explain the content of the revision.

Diagnostic Coverage

ISO13849-1: 2006 Safety Design

Common Cause Failure

Safety Related Parts of a Control System

Risk Reduction

Performance Level

Risk Assessment

Mean Time To Dangerous Failure

1 Background of ISO 13849-1 Revision

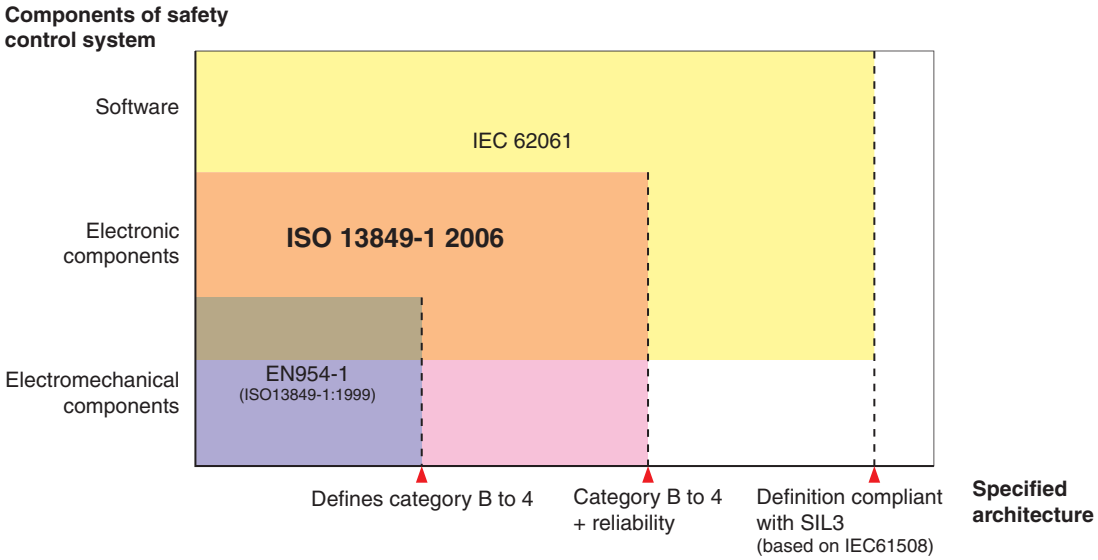
In considering safety protection in the measures to reduce machine risks, it has long been common practice to evaluate levels of risk reduction and the performance of a safety related control system in terms of Categories as specified in the international standard ISO13849-1: 1999 (based on the European standard EN954-1).

A Category is a classification of the architecture (structure) of a safety related control system. The concept was originally based on established technologies using electromechanical components such as switches and relays and simple electrical components. The behavior of these control systems in the event of a component failure can be determined to a high level of certainty because the failure modes of these components can be completely defined.

But as technology advances, electronic components such as transistors, integrated circuits and software based components such as microprocessors were adopted as core elements of safety related control systems. The failure modes of these components are more difficult to define and in some cases can only be estimated. Additionally, the deterministic classification of control systems based on structure does not adequately consider the possibility of a safety function failing due to systematic errors in the design or by the degradation of components over time.

For the past several years, work has been underway to define the performance of machine safety control systems in terms of function and reliability rather than component failure modes. This is the concept of "functional safety." IEC61508, the international standard for safety related electrical and electronic control systems, provides definitions of safety of complicated controls, down to the constituent components level such as designing reliability including life (until a loss of safety function) and programs based upon probability theory. IEC61508 has a very wide scope of application, so a new standard specifically designed for the machine control systems, IEC62061, was developed to provide for mechanical safety. However, because this standard basically assumes complicated controls, it assumes many safety control system architectures, and individual architecture requires complicated calculation of probability. This is the reason why IEC62061 was not familiar among machine designers who are accustomed to the relatively easy-to-follow definitions of "Categories."

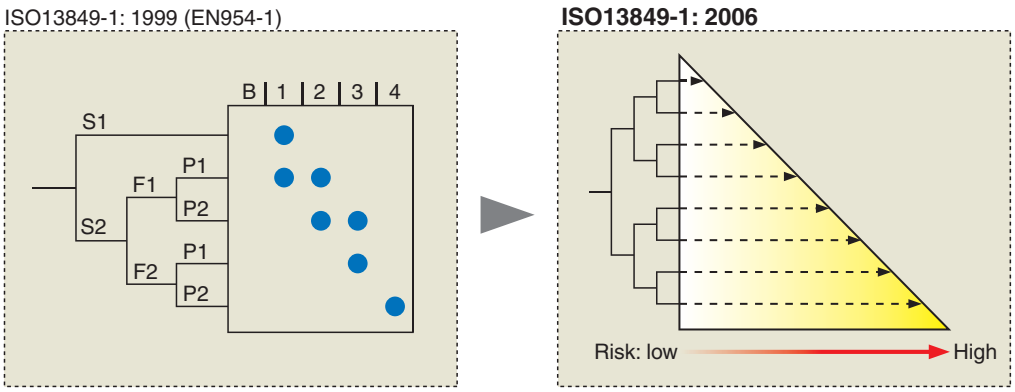
The latest version of ISO13849-1: 2006 combines the straight forward deterministic features of EN954-1's Categories with IEC62061's probabilistic and systematic design considerations (a reliability model). In other words, the revised version of ISO13849-1 selects the architecture models in IEC62061 that match the definitions of the Categories, and applies those reliability models. This version can be called a functional safety standard in its simplified version.



2 Main Changes

Changes in Risk Estimation Methods

Both methods require estimating risk of hazards at the risk assessment stages.
In estimating risks, EN954-1 evaluated and classified the results of its risk estimations into the risk levels of I to IV.
But the evaluation process did not encompass any notion of targeted performance that safety measures to reduce risks should reach. As a result, safety control system's structure Categories B to 4 are generally determined directly from the risk graph. When trying to establish a common parameter between persons who perform risk assessment (for example, users) and persons who implement risk reduction (for example, machine designers), the users may not understand the functional differences of safety control system structures from the designer's viewpoint, and the designer in turn finds it difficult to understand user requirements. Also, the overwhelming majority of risks at actual working sites are minor damage such as suspension of operation for several days, while EN954-1's risk graph gave more stress for risk estimations to serious damage. The previous standard did not accurately reflect this aspect.



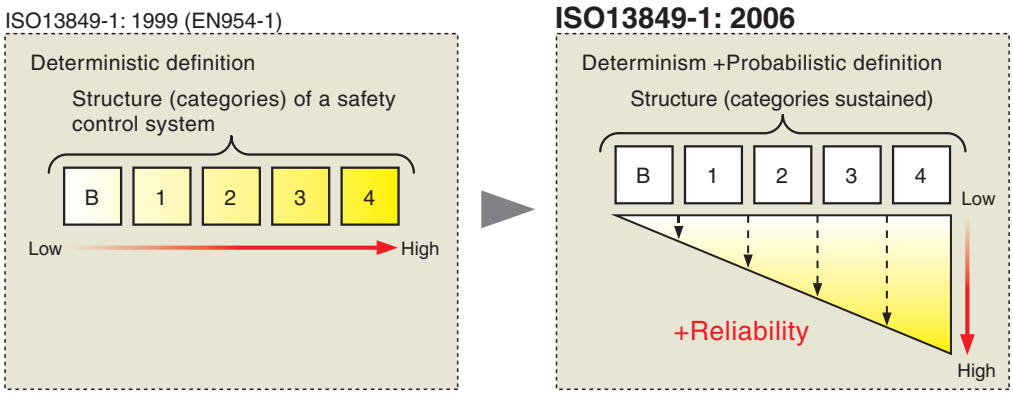
The latest revision in ISO 13849-1: 2006 allows users to determine risk estimations homogenously and uniquely, and makes risk assessment easier for persons responsible for implementing it.

Change in Definitions of Safety Control System's Performance

How should designers reduce risks?
If designers are required to satisfy Category requirements only, once determined safety control system structure will maintain the same level of safety performance.
The question is whether or not this is a correct concept considering that every machine can fail at some future time.
The components comprising the safety control system also will deteriorate and can fail at some future time. It is important to figure out in what mode the system will encounter a failure at such times.
When a machine experiences a failure that causes the expected safety function to fail during a period expected by its users, and if the failure is not detected, it is equal to non performance of safety functions. But, definitions only based upon deterministic theory cannot cover such time related elements.

2 Main Changes

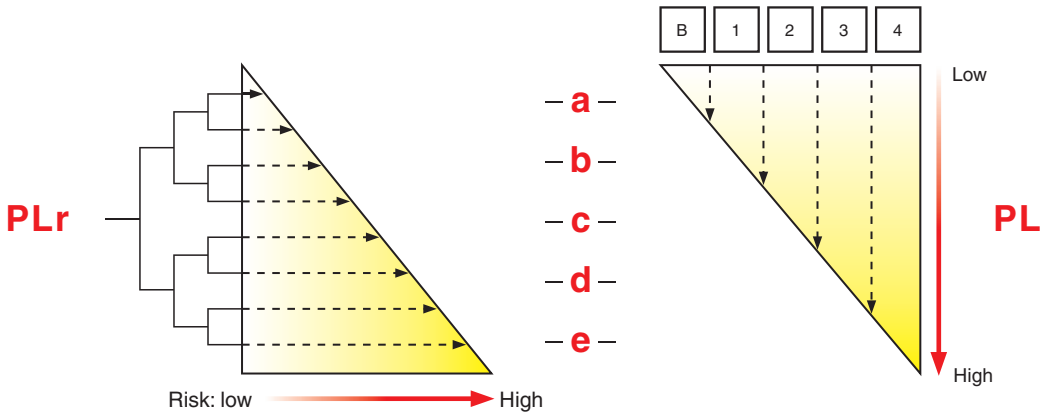
To improve this aspect, the latest revision includes additional features to the previous structure definitions with two-layer structure definitions that enable users to probabilistically evaluate a safety control system's reliability, including life to dangerous failure at the component level and detecting dangerous failure. This allows users to make quantitative evaluation according to how they actually use the machine. This is the core component of the 2006 revision.



Common Indicator Criteria

The revised standard establishes indicators of a safety control system performance level that can be clearly communicated between a person who implements risk assessment and a person who designs a machine.

These indicators are called Performance Level (hereinafter abbreviated as "PL"), and are evaluated using five levels from "a" to "e." Required performance levels as seen from the standpoint of a person who implements risk assessment are specifically called PLr. PL, the achieved performance level of a safety control system after risk reduction has been implemented, must be equal to or greater than required Performance Level (PLr).



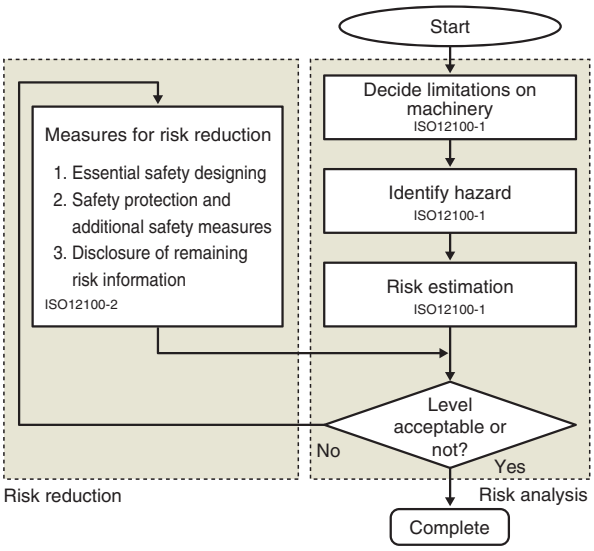
3 Recurrent Process of Risk Reduction

Procedures of risk assessment in ISO14121 follow a series of risk reduction steps that follow the risk analysis. Of these procedures, measures for risk reduction include three steps as shown in ISO12100-2.

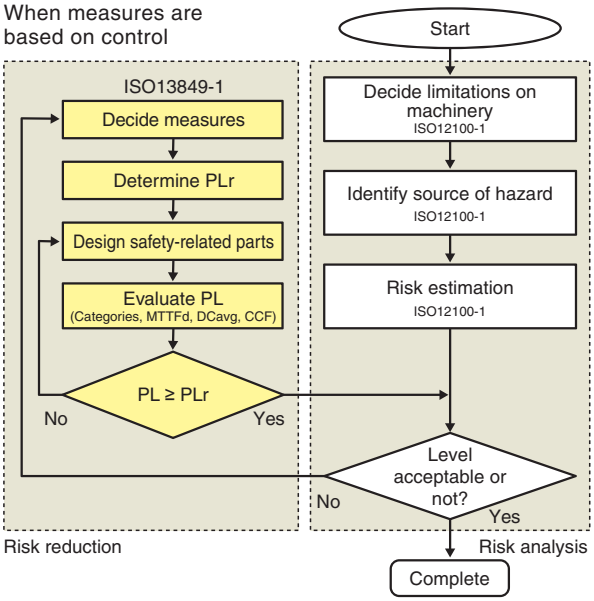
1. Essential safety designing
2. Safety protection and additional safety measures
3. Disclosure of remaining risk information

Of these, many of safety protection items and additional safety measures use interlock devices and emergency stop devices such as safety switch or safety light curtain. These instruments are rarely used as standalone devices, but are usually combined with a control circuit that uses them as an input or with an output circuit to which the results of a control circuit are transmitted to comprise a safety control system.

As shown in the right-hand figure, ISO13849-1:2006 provides a concrete picture of the risk reduction process when the risk reduction measures are based on control, in order to ensure its consistency with ISO14121 and ISO12100.



When measures are based on control



4 Benefits of Using PL

What benefits are offered to users and machine designers by this revision?

Benefits for Users

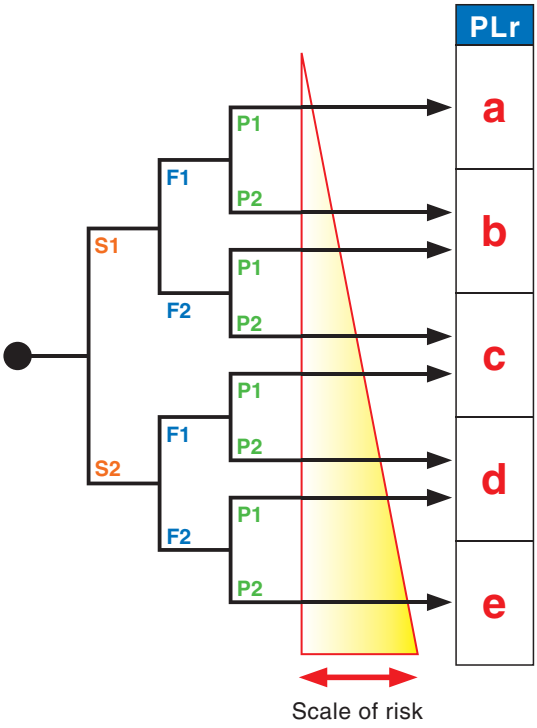
Machine users can easily describe the performance they require without stepping into the details of the designers' side by sharing easy-to-understand standards with machine designers/manufacturers. Also, for minor damage (S1), which had tended to be understated, the evaluation for its frequency (F) and possibility of avoiding hazard (P) has been added to increase the accuracy of risk quantification.

Benefits for Machine Designers

The combination of a safety control system's architecture and component's reliability provides a certain degree of flexibility. The revised standard allows users to select a combination of parameters within a range of required performance level (PLr), and also offers an increased degree of freedom for designing. Even when the system requires the same PLr, designers can choose to give priority to component reliability in designing for a system in which the safety function operates frequently (for example a power press machine), or to give priority to architecture for a system in which the safety function only operates occasionally (for example a robotic work cell).

5 How to Determine Performance Level

How to Determine Required Performance Level (PLr)



As with the risk graph in EN954-1, a required performance level is evaluated in terms of severity of injury (S), frequency and/or exposure to hazard (F) and possibility of avoiding hazard or limiting harm (P). As a result, the required performance level (PLr) ranging from “a” to “e” is determined depending on the scale of the risk.

Method to Evaluate Performance Level (PL)

Four parameters are used to evaluate a safety related control system's performance level (PL).

1. Category
2. MTTFd (Mean Time To Dangerous Failure)
3. DCavg (Average Diagnostic Coverage)
4. CCF (Common Cause Failure)

The Categories refer to the architecture of a safety related control system, and are classified into five categories as defined in the previous version of EN954-1.
MTTFd refers to an average life before the dangerous failure of a component. DC refers to the certainty of detecting failures in the entire system including software. CCF refers to the protection of the entire system from failing due to a common cause. As parameters for reliability, MTTFd and DCavg are determined by formulas, and CCF is determined with a checklist method.
Each of the parameters is classified into levels using standard values: three levels for MTTFd, three levels for DC and two levels for CCF. Performance Levels are evaluated comprehensively in terms of these four parameters.
The following sections show how each of the parameters is calculated.

5·1 Category

Safety control systems have different architectures (structures) depending on a machine's purpose, the degree of hazards, the machine's size, the frequency of operating the machine, etc. even when the systems have the same purpose of securing the machine's safety. For example (using our housing analogy), to deliver "a space to keep away from rain and wind," there are various types of different structures depending on their purpose, such as tent, wooden house, office building, etc, and the basic structure such as the foundation, frame, external walls and roof also differs. Categories as referred to in safety control systems refer to basic classifications of architecture like this.

For example

In ISO 13849-1:2006, the safety control system requirements for each of the categories are the same as those in EN 954-1:1996. However, the revised standard offers a more explicit scheme of the safety control system and its characteristics for each of the categories focused on the three sections of I (input device), L (logic operations device) and O (output device). The safety control system of most machines can be described in terms of these types of structures.

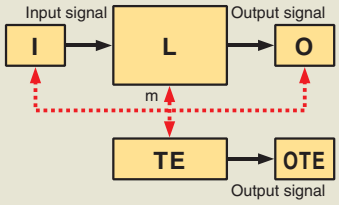
Note: Some more complex architectures that do not fit within this scheme, such as logic that has three or more input channels for majority decision, cannot be handled by ISO 13849-1. In this case, other standards, such as IEC 62061, need to be used to evaluate the safety control system's performance.

Structure applied to Categories B and 1

I : Input device e.g. Sensor
L : Logic operations device
O : Output device e.g. Contactor

Note: The MTTFd of Category 1 is higher than that of Category B, so the possibility of losing the safety function is low, but when in failure the loss of the safety function may occur.

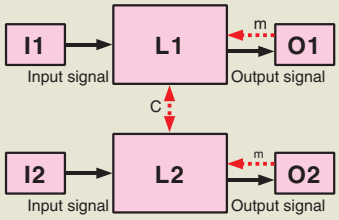
Structure applied to Category 2



m : Monitoring
TE : Inspection device
OTE : Output of inspection results

Note: Category 2 may encounter a safety function loss between inspections when a failure occurs.

Structure applied to Categories 3 and 4



m : Monitoring
C : Cross-monitoring

Note:1. In Category 3, the safety function may fail to work when undetected failures accumulate.

Note:2. The redundancy system of the architecture defined in this block diagram does not only have a physical meaning but it also means an internal logic of which the single failure resistance has been confirmed.

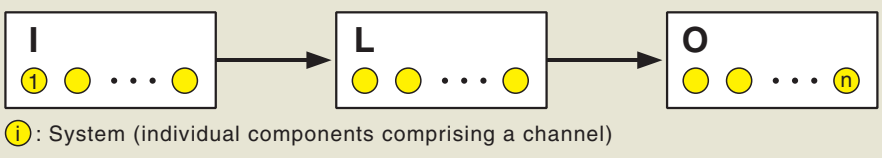
5·2 MTTFd (Mean Time To Dangerous Failure)

MTTFd refers to an average amount of time that it takes the safety control system to encounter a dangerous failure. Dangerous failure means that the safety function is not performed because of a component's failure. Each of the components comprising the safety control system has a predicted length of life, but the component's actual life can vary depending on how they are used and how frequently they are operated.
In the case of buildings, components required for the structure (tent's support pillar, wooden house's beam, building's steel frame, etc.) have their specific useful life respectively as materials. When these materials are used in actual buildings, the degree of their fatigue varies depending on how much frequently the building is used. The concept of MTTFd for safety control systems is similar to this.

For example

Each channel of a safety control system as defined in ISO13849-1: 2006 consists of an I (input device), an L (logic operations device) and an O (output device) in series. In reliability engineering, the probability of a system failure is expressed as the sum of failure probabilities of individual components comprising the channel. This also applies to dangerous failures. On the other hand, there is a relationship of reciprocity between dangerous failure rates and average dangerous failure times. Therefore, the average dangerous failure time (MTTFd) for the entire system is calculated as the reciprocal of the sum of the reciprocals of the individual component's dangerous failure times (MTTFdi).

Example of a one channel system : Categories B and 1



5·2 MTTFd (Mean Time To Dangerous Failure)

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

How should the MTTFdi for individual components be calculated?
ISO13849-1: 2006 offers the following options:

1. Use data provided by component manufacturers.
2. When manufacturers do not provide data, you can use the estimated data specified in Annex C Table C1 of ISO13849-1: 2006.

Determining MTTFd for individual parts inside the components (referred to as safety components) comprising a safety control system is a labor-consuming task. As a result, it is a common practice to evaluate the system on the level of I, L and O components. But in some cases data is not provided by manufacturers.
To address these cases, Annex C of ISO13849-1: 2006 provides values of MTTFd or B10d for typical components. These values can then be used to make the necessary calculations. B10d refers, in reliability engineering, to the number of operation it takes for 10% of the samples to experience a dangerous failure. This data is mainly used to determine the MTTFd for components that wear out through use such as electro-mechanical devices. However, to determine the MTTFd for a component, the number of times the component is operated per year (Nop) needs to be estimated.

$$MTTFd = \frac{B10d}{0.1 \times N_{OP}} \quad \text{(Eq. 2)}$$

The value of Nop is determined by the following:
· Tcycle: An average time interval for an operating cycle (Unit: seconds per cycle)
· Hop: The number of Operating hours per day (Unit: hours per day)
· Dop: The number of operating days per year (Unit: days per year)

$$Nop = \frac{dop \times hop \times 3{,}600}{tcycle} \quad \text{(Eq. 3)}$$

In other words, the machine designer needs to understand how many hours a day and how many days a year the machine is required to operate and how frequently the component is required to operate.
Also, some of the components have no data described in Table C.1. Of those components, the components certified in the functional safety standards (IEC61508 and IEC62061) can have data determined by converting the PFHd (average probability of a dangerous failure) specified in Annex K Table K.1* into MTTFd.
The resulting MTTFd of a channel is finally classified into one of the three levels of Low, Medium and High depending on the number of the years.

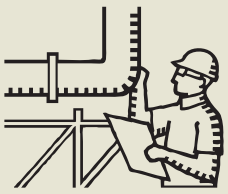
MTTFd	
Low	3years≤MTTFd<10years
Medium	10years≤MTTFd<30years
High	30years≤MTTFd≤100years

* Results of more than 100 years are classified into High.

5·3 DCavg (Average Diagnostic Coverage)

DCavg is an indicator of the reliability of a safety control system as a whole. DCavg is determined by how frequently and accurately the system performs self-diagnosis and by what measures the system takes to address the results of such diagnosis. This concerns the reliability of not just the components but also of the functionality that affects the entire system such as software.
Take buildings for comparison. Tents can be used without any problem when they are inspected and mended once a year before use. But wooden houses give trouble when problems that are found, such as termite damage and rainwater leaks, are not immediately fixed. Office buildings must be routinely inspected to find evidence of any potential problems so that preventive measures can be taken in advance; otherwise, the buildings might suffer significant damage leading to disaster. Thus, the required levels of diagnosis must be appropriate for the intended use and the type of structure (architecture).

For example

Tent	Wooden house	Office building
		
		
Repair any damage before use	Take measures as necessary Termite eradication, prevention of rainwater leaks, etc.	Discover problems in advance through regular building maintenance

The diagnosis function as implemented in safety control systems refers to the function shown as “monitoring” or “cross-monitoring” in the block diagrams of the architecture in the Categories. The function uses many different safety design principles. Items that apply to the safety principles used in each of I, L and O are chosen from Annex E Table E.1, and are set as the diagnosis ratio (DC) of individual components.
DC needs to be evaluated as well in terms of the entire channels of a safety control system. The average value of DC for the entire system (DCavg) is determined from the DC on a component-basis using this formula.

$$DCavg = \frac{\sum_{i=1}^{n} \frac{DCi}{MTTFdi}}{\sum_{i=1}^{n} \frac{1}{MTTFdi}} \quad \text{(Eq. 4)}$$

Depending on how high the diagnosis ratio is, DCavg is finally classified into the four levels: None, Low, Medium and High.

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

5·4 CCF (Common Cause Failure)

CCF is an indicator of designing reliability to show whether a safety control system incorporates considerations to ensure that its overall functionality is not damaged by common causes.
For buildings, there are possible common causes that cause significant effects on the entire system, such as typhoon, earthquake and fire. For example, a cause of earthquake can cause severe shakes as well as cracking, etc.
The system must include assumptions about whether the columns and external walls of a building are sufficiently resistant to shakes or whether the foundation is resistant to ground displacement, etc. Also, even when the roofs are resistant to typhoons, they may be vulnerable to the quaking force of an earthquake when poorly balanced.
Thus CCF refers to the degrees of such designing considerations to provide for as many different kinds of external factors as can be predicted.

Annex F Table F.1 offers a standardized, check-list of considerations based on the design principles that have been used to protect against CCF. Check appropriate items and add up their scores. The system is evaluated by determining whether or not the total score is 65 points or higher. The architecture in Category 2 or higher is required to have a CCF score of 65 points or higher.

*Notice that partial scores are not allowed. All aspects of a measure must be used in order to count the score.

5·5 Example of Evaluation Using the Graph

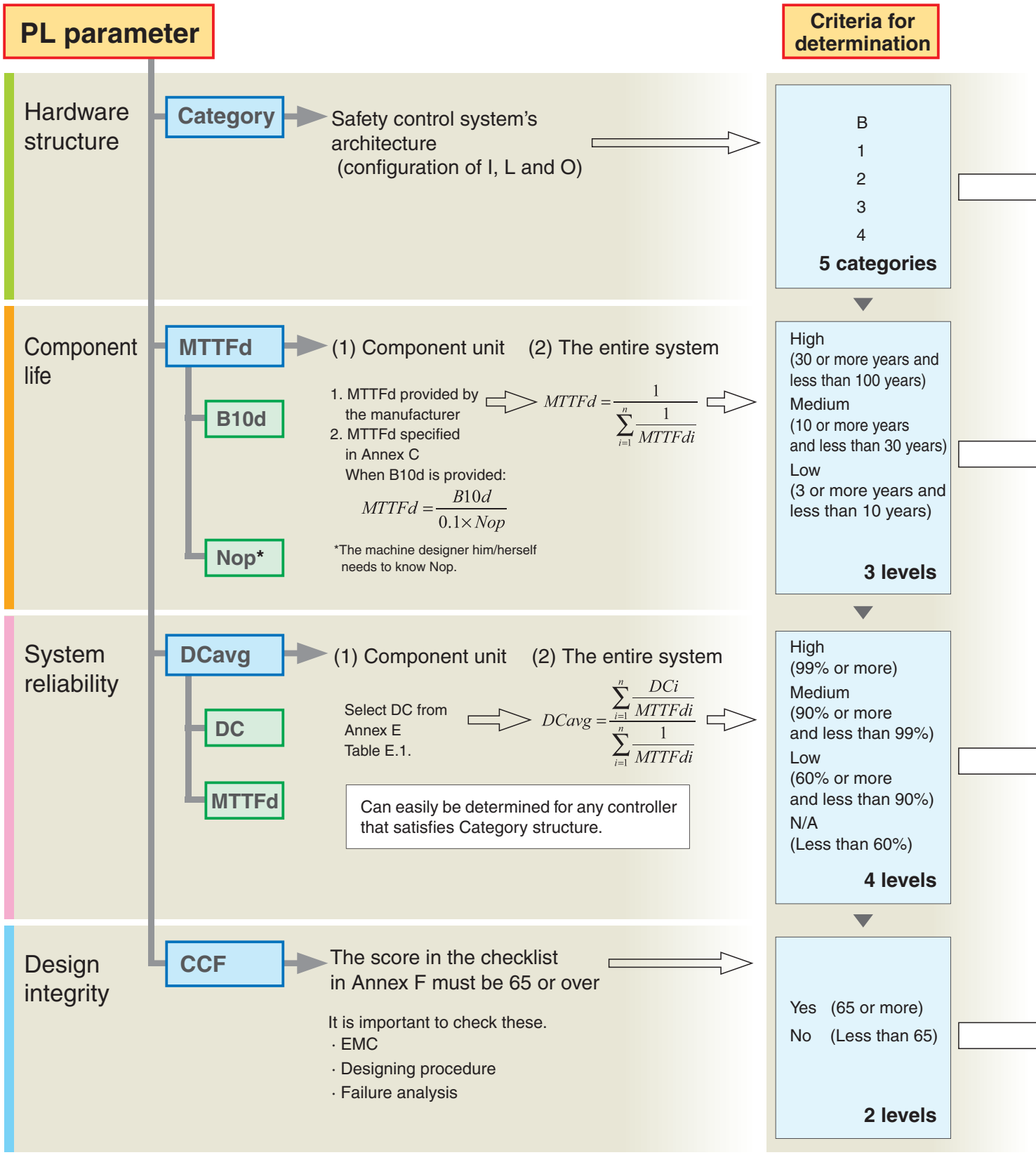
As described above, when the four parameters are calculated, the PL can be determined from the following graph:

- Category (the five categories of B, 1, 2, 3, and 4)
- MTTFd (the three levels of High, Medium, and Low)
- DCavg (the four levels of High, Medium, Low, and None)
- CCF (the two levels of 65 or more points and less than 65 points)

For example, with "Category 4, MTTFd=High, DCavg=High, CCF of 65 points or higher," then the PL is evaluated as "e". However, the thresholds in the previous graph for MTTFd determination are not easy to locate therefore this table is provided to give a more simplified view. Either the graph or the table may be used.

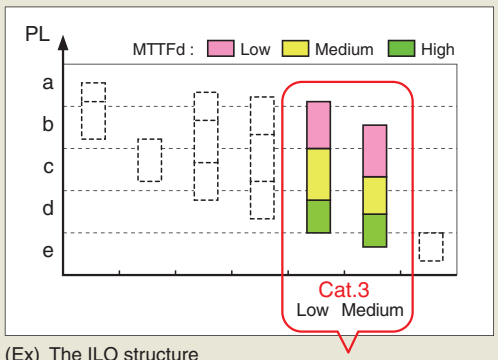
Category		B	1	2	2	3	3	4
DCavg		None	None	Low	Medium	Low	Medium	High
MTTFd of each channel								
	Low	a	---	a	b	b	c	---
	Medium	b	---	b	c	c	d	---
	High	---	c	c	d	d	d	e

*Notice that in both the graph and the table methods some combinations of parameters are not allowed. For example, combining Category 4 with medium reliability and low diagnostic coverage is not considered.


PL parameter
Criteria for determination
Hardware structure
Category
Safety control system's architecture (configuration of I, L and O)
B
1
2
3
4
5 categories
Component life
MTTFd
(1) Component unit (2) The entire system
B10d
Nop*
1. MTTFd provided by the manufacturer
2. MTTFd specified in Annex C
When B10d is provided:
$MTTFd = \frac{B10d}{0.1 \times Nop}$
$MTTFd = \frac{1}{\sum_{i=1}^{n} \frac{1}{MTTFdi}}$
*The machine designer him/herself needs to know Nop.
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
System reliability
DCavg
(1) Component unit (2) The entire system
DC
MTTFd
Select DC from Annex E Table E.1.
$DCavg = \frac{\sum_{i=1}^{n} \frac{DCi}{MTTFdi}}{\sum_{i=1}^{n} \frac{1}{MTTFdi}}$
Can easily be determined for any controller that satisfies Category structure.
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
Design integrity
CCF
The score in the checklist in Annex F must be 65 or over
It is important to check these.
· EMC
· Designing procedure
· Failure analysis
Yes (65 or more)
No (Less than 65)
2 levels

How to read graph

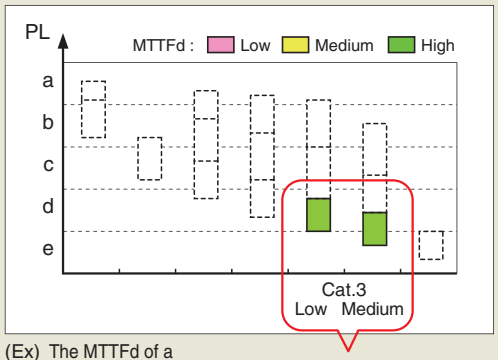
How to read table



(Ex) The ILO structure applies to Cat 3.

A bar graph that applies to Cat3 is selected

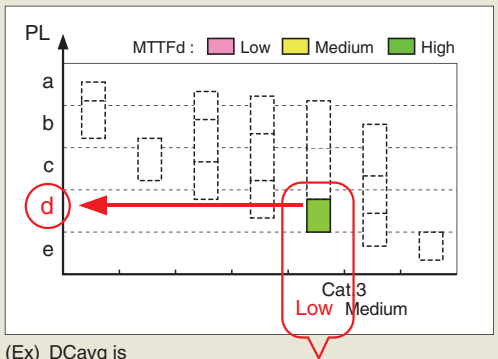
Category	B	1	2	2	3	3	4
DCavg	None	None	Low	Medium	Low	Medium	High
MTTFd of each channel							
Low	a	---	a	b	b	c	---
Medium	b	---	b	c	c	d	---
High	---	c	c	d	d	d	e



(Ex) The MTTFd of a system is calculated as 40 years.

The area that Corresponds with MTTFd High is selected

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



(Ex) DCavg is calculated as 80%.

The graph that corresponds with DCaveg Low is selected

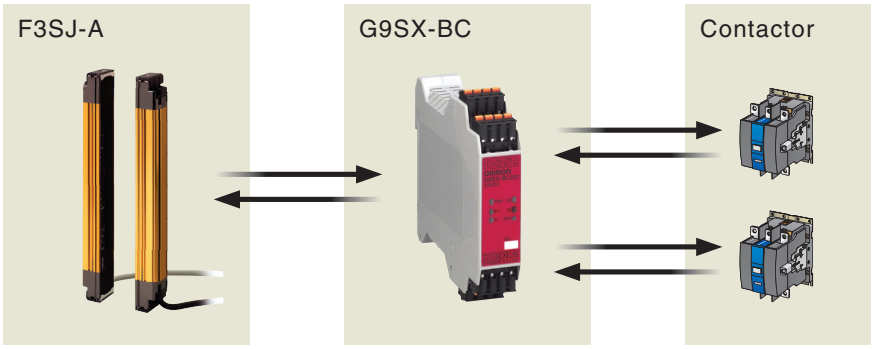
Category	B	1	2	2	3	3	4
DCavg	None	None	Low	Medium	Low	Medium	High
MTTFd of each channel							
Low	a	---	a	b	b	c	---
Medium	b	---	b	c	c	d	---
High	---	c	c	d	**d**	d	e

The letter that corresponds with the selected area refers to this system's PL.

However, the architecture of Category 2 or higher requires the CCF score of 65 points or higher.

6 Example of PL Calculations

Now, the following sections take Omron's product as example and let you navigate through the steps to evaluate its PL. Let's assume the safety circuit as illustrated in the figure. The circuit consists of safety light curtain type F3SJ-A for Input, flexible safety unit type G9SX-BC for Logic and a contactor with mirror contacts for Output.



I : Input device **L : Logic operations device** **O : Output device**

Also, feedback of the contactor's mirror contacts is provided to the Logic to perform monitoring of the Output's status; the circuit is activated by a manual reset method; and the stop Category is a safety circuit at "0".

Step1: Identify Category

Signals transmission from the light emitting/receiving unit of a safety light curtain of Type 4 to the Output uses a redundancy system and diversity for its internal logic processing, and so the output is assumed as the one made dual. Therefore, this architecture applies to Category 4.

Step2: Calculate the Components' MTTFd

Calculate the MTTFd for individual components.

Of the components, it is known that type F3SJ-A and type G9SX-BC have an MTTFd of 100 or more years respectively. For the contactor, Annex C Table C.1 provides a B10d value of 2,000,000 times. Therefore, this B10d value needs to be used to calculate the MTTFd.

Step3: Identify Operating Conditions

To calculate the MTTFd from a B10d value, the operating conditions for this application need to be identified in advance. Here, we assume as a sample:

tcycle (a time interval for operations) : 60 sec. per cycle
hop (operating hours per day) : 8 hours per day
dop (operating days per year) : 240 days per year

From this assumption, the contactor's number of times of operation per year is calculated as 115,200 times per year, and so the contactor's MTTFd is 173.6 years.

$$Nop = \frac{dop \times hop \times 3{,}600}{tcycle} = \frac{240 \times 8 \times 3{,}600}{60} = 115{,}200 \quad (cycle/year)$$

$$MTTFd = \frac{B10d}{0.1 \times NOP} = \frac{2{,}000{,}000}{0.1 \times 115{,}200} = 173.6$$

Step 4: Calculate the Entire Channel's MTTFd

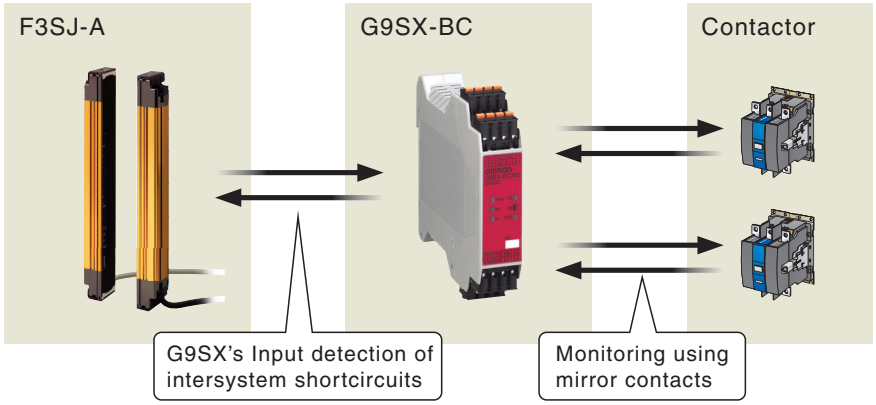
From the individual component's MTTFd as seen above, the MTTFd of the entire system is calculated. The MTTFd for each component is entered into this formula, and the MTTFd of 38.8 years is obtained. Because the condition for an MTTFd to be classified as "High" is 30 ≤ MTTFd ≤ 100, the MTTFd for this entire system is classified as "High."

$$MTTFd = \frac{1}{\sum_{i=1}^{3} \frac{1}{MTTFdi}} = \frac{1}{\frac{1}{100} + \frac{1}{100} + \frac{1}{173.6}} = \frac{1}{0.02576} = 38.8$$

6 Example of PL Calculations

Step 5: Calculate the Individual DC

Type F3SJ-A and type G9SX-BC have a self-diagnosis function for their respective internal circuits, and are certified under the functional safety standard IEC61508. This section describes failure diagnosis for interfaces between the individual components.



Between type F3SJ-A and type G9SX-BC

Intersystem short-circuits between two input channels are diagnosed by the intersystem short-circuit monitoring function of type F3SJ-A and type G9SX.

This type of failures applies to "Cross-monitoring of input signals and interim results within the Logic (L), temporal and logical software monitoring of program flows and detection of static failures and short-circuits (for multi I/O)" in Annex E's Table E.1 (page 24), and therefore the DC between the two can be determined as 99%.

Between type G9SX-BC and the contactor

The contactor's contact failures are monitored by providing a feedback of the contactor's mirror contacts to type G9SX-BC.

This type of failures applies to "Direct monitoring (e.g. Monitoring of a control valve's electrical position, monitoring of an electromechanical device using mechanically linked contact elements)" in Annex E Table E.1, and therefore the DC between the two can be determined as 99%.

Step 6: Calculate the DCavg

Assigning the values of the DC between type F3SJ-A and type G9SX-BC, the DC between type G9SX-BC and the contactor, the MTTFd of type G9SX-BC and the contactor's MTTFd into this formula determines the DCavg as 99%. Because the condition for a DCavg to be classified as "High" is 99%　DC, the DCavg is classified as "High."

$$DCavg = \frac{\sum_{i=1}^{2} \frac{DCi}{MTTFdi}}{\sum_{i=1}^{2} \frac{1}{MTTFdi}} = \frac{\frac{0.99}{100} + \frac{0.99}{173.6}}{\frac{1}{100} + \frac{1}{173.6}} = 0.99$$

Step 7: Evaluating PL

Because Category 4, MTTFd="High", DCavg="High", the PL is evaluated as "e". However, it is assumed that the CCF is 65 or higher.

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

Note: The MTTFd and DC of the parts may differ from the values used in the examples above depending on the state of progress and interpretation of the standards for each part.

7 FAQ

Keyword: PL

Q When using the graph to determine the performance level (PL), what do you do for the parts where the ranges overlap?

A Detailed information for the graph is included in Annex K, in the appendices of ISO 13849-1:2006. The final PL is determined based on the MTTFd level.

Q What is the difference between using the graph and the table to determine the PL?

A There is no difference. Use whichever is easier.

Keyword: Category

Q Are there any changes to the example circuits of the current catalog?

A No, there are no changes. They are grouped by category as before.

Q How should architectures such as triple-layer systems, which are not specified by the standard, be treated?

A Systems that are not specified by ISO 13849-1 should be evaluated using other standards, such as IEC 61508.

Keyword: MTTFd

Q When the MTTFd is determined from B10d, can Nop be set to any desired value?

A First, the machine manufacturer estimates how the machine will be used. It can then determine the maintenance cycle and frequency of parts replacement. These details must be clearly outlined, such as in the manual, for the user's understanding.

Q A situation where the emergency stop device needs to be operated may not even occur once a year. What should the Nop value be for a case like this?

A Even if it is rarely used, any emergency stop device must be subject to regular operation tests. Machine manufacturers must indicate the frequency of tests in the operation manual, for example with a precaution like, “Correct emergency stop operation must be confirmed once a day."

Q Can the MTTFd be considered the number of years of use or the expected lifetime of the machine?

A The MTTFd is a calculation, and is unrelated to the number of years it has been used or how long it is expected to be useful.

Keyword: DC

Q Input tests are not shown in Category 3 and 4 block diagrams. Is the DC calculation required?

A If the ISO 13849-2 fault exception item is not applicable, the DC must be taken into account.

Q If the DCavg is below 60% in a Category 3 circuit, does it become the same as a Category 1 circuit?

A Yes. Simple double-layer systems cannot reach high PL values.

Keyword: CCF

Q There is no problem with factors that can be clearly identified (such as signal path separation, EMC, or diversity), but what should I do for factors like operator ability and training, which can't be clearly identified?

A A written record must be kept as a means of evidence.

Keyword: General

Q What is included in safety parts?

A All parts related to safety functions are included. For example, if a safety function is compromised by incorrect signals from a general-purpose PLC, the general-purpose PLC will also become a safety part.

Q Is the machine manufacturer charged with the final judgment and responsibility as previously?

A Yes. It is important that written proof is kept stating that it is suitable.

Q Can't the EN 954-1 (or ISO 13849-1:1999) standard still be used?

A These standards can be used until the end of the grace period (Nov 2009).

8 Appendix

International Standards dealing with MTTFd or B10d for components

(Based on ISO 13849-1: 2006 Annex C)

	Basic and well-tried safety principles according to ISO 13849-2:2003	Other relevant standards	Typical values: MTTFd (years) B10d (cycles)
Mechanical components	Tables A.1 and A.2	—	MTTFd = 150
Hydraulic components	Tables C.1 and C.2	EN 982	MTTFd = 150
Pneumatic components	Tables B.1 and B.2	EN 983	B10d = 20 000 000
Relays and contactor relays with small load (mechanical load)	Tables D.1 and D.2	EN 50205 IEC 61810 IEC 60947	B10d = 20 000 000
Relays and contactor relays with maximum load	Tables D.1 and D.2	EN 50205 IEC 61810 IEC 60947	B10d = 400 000
Proximity switches with small load (mechanical load)	Tables D.1 and D.2	IEC 60947 EN 1088	B10d = 20 000 000
Proximity switches with maximum load	Tables D.1 and D.2	IEC 60947 EN 1088	B10d = 400 000
Contactors with small load (mechanical load)	Tables D.1 and D.2	IEC 60947	B10d = 20 000 000
Contactors with nominal load	Tables D.1 and D.2	IEC 60947	B10d = 2 000 000
Position switches independent of load *	Tables D.1 and D.2	IEC 60947 EN 1088	B10d = 20 000 000
Position switches (with separate actuator, guard-locking) independent of load *	Tables D.1 and D.2	IEC 60947 EN 1088	B10d = 2 000 000
Emergency stop devices independent of the load *	Tables D.1 and D.2	IEC 60947 ISO 13850	B10d = 100 000
Emergency stop devices with maximum operational demands *	Tables D.1 and D.2	IEC 60947 ISO 13850	B10d = 6 050
Push buttons (e.g. enabling switches) independent of the load) *	Tables D.1 and D.2	IEC 60947	B10d = 100 000

Note:1. For the definition and use of B10d, see ISO 13849-1: 2006 Annex C table C.4.
Note:2. B10d is estimated as two times B10 (50 % dangerous failure).
Note:3. “Small load” means, for example, 20 % of the rated value (for more information, see EN 13849-2).
* If fault exclusion for direct opening action is possible.

Examples of diagnostic coverage (DC)

(Based on ISO 13849-1: 2006 Annex E)

Measure	DC
Input device	
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 %

Measure	DC
Input device	
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	
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 %, depending 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 estimations for DC, see, e.g., IEC 61508-2:2000, Tables A.2 to A.15.
Note:2. If medium or high DC is claimed for the logic, at least one measure for variable memory, invariable memory and processing unit with each DC at least 60 % has to be applied. There may also be measures that used other than those listed in this table.

8 Appendix

Scoring process and quantification of measures against CCF

(Based on ISO 13849-1: 2006 Annex F)

No.	Measure against CCF	Score
1	**Separation/ Segregation**	
	Physical separation between signal paths: separation in wiring/piping, sufficient clearances and creep age distances on printed-circuit boards.	**15**
2	**Diversity**	
	Different technologies/design or physical principles are used, for example: first channel programmable electronic and second channel hardwired, kind of initiation, pressure and temperature, Measuring of distance and pressure, digital and analog. Components of different manufactures.	**20**
3	**Design/application/experience**	
3.1	Protection against over-voltage, over-pressure, over-current, etc.	**15**
3.2	Components used are well-tried.	**5**
4	**Assessment/analysis**	
	Are the results of a failure mode and effect analysis taken into account to avoid common-cause-failures in design.	**5**
5	**Competence/training**	
	Have designers/ maintainers been trained to understand the causes and consequences of common cause failures?	**5**
6	**Environmental**	
6.1	Prevention of contamination and electromagnetic compatibility (EMC) against CCF in accordance with appropriate standards. Fluidic systems: filtration of the pressure medium, prevention of dirt intake, drainage of compressed air, e.g. in compliance with the component manufacturers' requirements concerning purity of the pressure medium. Electric systems: Has the system been checked for electromagnetic immunity, e.g. as specified in relevant standards against CCF? For combined fluidic and electric systems, both aspects should be considered.	**25**
6.2	Other influences Have the requirements for immunity to all relevant environmental influences such as, temperature, shock, vibration, humidity (e.g. as specified in relevant standards) bee considered?	**10**
	Total	**[max. achievable 100]**

Total score	**Measures for avoiding CCF ***
65 or better	Meets the requirements
Less than 65	Process failed → choose additional measures

* Where technological measures are not relevant, points attached to this column can be considered in the comprehensive calculation.

MTTFd and B10d for OMRON Products

B10d

	Product Name	Model	B10d (cycles)	Corresponding Items to ISO 13849-1: 2006 Annex C Table C.1
I (Input device)	Safety Door Switch	D4NS	2 000 000	Position switches (with separate actuator, guard-locking) independent of load *
		D4GS-N		
		D4BS		
	Guard Lock Safety-door Switch	D4GL		
		D4JL		
		D4NL		
		D4BL		
	Safety-door Hinge Switch	D4NH	20 000 000	Position switches independent of load *
	Safety Limit Switch	D4N	20 000 000	Position switches independent of load *
		D4F		
		D4B-N		
		D4N-R		
	Emergency Stop Switch	A22E	100 000	Emergency stop devices independent of the load *
		A165E		
	Enabling Switch	A4E	100 000	Push buttons (e.g. enabling switches independent of the load) *
	Enabling Grip Switch	A4EG		
L (Logic)	Relays with Forcibly Guided Contacts	G7S	20 000 000	Relays and contactor relays with small load (mechanical load)
		G7SA		
O (Output device)	Power Relays	G7Z	2 000 000	Contactors with nominal load

Note: The above B10d data are reference values as indicated in C.1 of the ISO 13849-1: 2006 Annex C table for MTTFd calculation. They do not imply a guarantee of the product's actual number of operations.

* Applies to contacts for direct circuit operation.

MTTFd

	Product Name	Model	MTTFd (years)
I (Input device)	Safety Light Curtain	F3SJ	100 and more
L (Logic)	Flexible Safety Unit	G9SX-AD	100 and more
		G9SX-ADA	100 and more
		G9SX-BC	100 and more
		G9SX-GS	100 and more
	Safety Network Controller	NE1A-SCPU01-V1	100 and more
		NE1A-SCPU02	100 and more
	Safety I/O Terminals	DST1-ID12SL-1	100 and more
		DST1-MD16SL-1	100 and more
		DST1-XD0808SL-1	100 and more
		DST1-MRD08SL-1	100 and more

Note:1. Data for other OMRON products will be made available as soon as possible. Please wait for this data.

Note:2. The MTTFd and DC of the parts may differ from the values stated above depending on the state of progress and interpretation of the standard for each part.

OMRON Corporation
Industrial Automation Company
Safety Devices Dvision
Shiokoji Horikawa, Shimogyo-ku,
Kyoto, 600-8530 Japan
Tel: (81) 75-344-7093/Fax: (81) 75-344-8197

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 94555-3605 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:

OMRON Industrial Automation Global: **www.ia.omron.com**

Cat. No. Y115-E1-01

Printed in Japan
0507-?M (0507) (H)