

Safety of machinery
- Guidelines of Functional Safety PLC -

First Edition: May 20, 2011



一般社団法人日本電機工業会

The Japan Electrical Manufacturers' Association

PLC Technical Committee

Safety PLC WG

Foreword

This document is committee material compiled based on the deliberation of the Safety PLC WG under the PLC Technical Expert Committee.

This document is a copyrighted work protected by the Copyright Act.

Attention is drawn to the potential conflict of part of this document with any patent right of a technical nature, any patent application after it is opened, any utility model right, or any application for utility model registration after it is opened. The Japan Electrical Manufacturers' Association (JEMA) is not responsible for confirming any such patent right of a technical nature, any patent application after it is opened, utility model right, or application for utility model registration after it is opened.

History

Ver.	Date	Revised part	Content of revision
1.00	May 20, 2011	Whole document	First version created
1.01	June 20, 2011	Whole document	Sources of figures specified; typos corrected

Table of Contents

	Page
1 Preface	1
2 Reference	2
3 Terms and Definitions	4
3.1 FS-PLC (A Functional Safety PLC)	4
3.2 SRP/CS (Safety-Related Parts of a Control System)	4
3.3 PL (Performance Level)	4
3.4 PLr (Required Performance Level)	4
3.5 Safety Block Diagram	5
3.6 B10d	5
3.7 MTTFd (Expectation of the Mean Time to Dangerous Failure)	5
3.8 DCavg (average of Diagnostic Coverage)	6
3.9 CCF (Common Cause Failure)	6
3.10 PFHd (Probability of Dangerous Failure per Hour)	6
3.11 Stop functions	6
3.12 EDM (External Device Monitoring)	7
3.13 Unexpected/Unintended Start-up	7
4 Features of the FS-PLC	8
4.1 Hardware multiplexing, redundancy and safety related self-diagnostic circuits	8
4.2 Application multiplexing operations and the detection of inconsistency in operation results	8
4.3 Complete separation between safety- and non-safety related parts	8
4.4 Dedicated safety application development tools and dedicated communication protocols to communicate with FS-PLCs	8
5 Usage of the FS-PLC	9
5.1 Emergency stop and start-up/restart	9
5.2 Diagnosis of external devices (EDM and pulse test)	10
6 Performance level (PL)	11
6.1 Software requirements	11
6.2 Procedures for calculating hardware PL (Example of calculating PL of SRP/CS)	11
7 Safety Circuit Examples	14
7.1 Introduction	14
7.2 Emergency stop: Emergency stop switch	15
7.3 Emergency stop of a machine by regenerative braking: Off-delay timer	18
7.4 Machine start/stop in unlocked guard: Guard monitoring	21
7.5 Machine start-up/stop in locking type guard: locking-type interlock	24

7.6	Start-up of press: Two-hand control switches	27
7.7	Pendant-based robot teaching: 3-position enabling switch	30
7.8	Automatic/teaching mode selection for industrial robot application: Mode selector switch	34
7.9	Intrusion detection by light curtain: Light curtain	38
7.10	Detection of presence by laser scanner: Laser scanner	42
7.11	Muting function of the light curtain: Cross muting	45

Safety of machinery

- Guidelines of Functional Safety PLC -

1 Preface

It is common knowledge among machinery and equipment users and manufacturers that, when exporting production machines and equipment to Europe, the confirmation of, and in technical documents for third-party certification and the self-declaration of safety compliant with the EU's Machinery Directive, Low Voltage Directive and EMC Directive are required. However, we have received many remarks and questions concerning the international safety standards referenced in the Machinery Directive, such as "We cannot understand the specific functions and actions of the safety circuits," "We would like to obtain the safety certification, are there any examples of application documents?" "We are implementing safety-related systems with software - what should we do to gain safety certification?" This situation itself is considered proof that Japanese machinery and equipment are compliant with safety standards and that their international competitiveness has increased. It is hard to avoid the feeling, however, that Japanese users and manufacturers are lagging behind foreign counterparts in terms of productivity and the development of machinery and equipment compliant with the standards.

Under these circumstances, on May 25, 2009, the Safety PLC WG devised and issued a "Guide to functional safety certification in machinery and equipment safety-related system engineering" as a handbook in response to functional safety, which is considered the most difficult hurdle to overcome. Efforts were made to ensure that this guide describes, as concretely as possible, the mindset for functional safety, example compositions of application documents for certification, etc. as an introductory book to functional safety, based on the requirements of IEC 62061:2005 (JIS B 9961:2008). Because the guide did refer to the performance level (PL) introduced by ISO 13849-1:2006, however, it could not respond to opinions such as "How should we use the Safety PLC concretely?" and "How should we calculate the PL for FS- PLCs and peripheral circuits?"

This time therefore, in addition to the guide, we have decided to prepare and publish this document with the purpose of preparing a collection of safety circuit examples using the FS-PLC, based on the requirements of ISO 13849-1:2006, and introducing the way of using the FS-PLC, wiring examples, and the PL calculation method.

Further, this document presumes its readers are those who are users of general-purpose PLCs and who have understood the basic contents of international safety standards. For international safety standards in general, please refer to the "Safety Guidebook" issued by the Nippon Electric Control Equipment Industries Association (NECA).

We would be happy if this document were useful in any way in helping machinery and equipment users and manufacturers comply with the Machinery Directive and international safety standards and to rationalize the work of producing technical documents to apply for certification.

This document was prepared with the cooperation of:

The Japan Machinery Federation (JMF),
Japan Printing Machinery Association (JPMA),
The Nippon Electric Control Equipment Industries Association (NECA),
TÜV-SÜD Japan Ltd., and
TÜV-Rheinland Japan Ltd.

We express our deep appreciation for the cooperation of the parties concerned.

2 Reference

ISO 12100-1:2003 (JIS B 9700-1:2004)

Safety of machinery - Basic concepts, general principles for design -- Part 1: Basic terminology, methodology

ISO 12100-2:2003 (JIS B 9700-2:2004)

Safety of machinery - Basic concepts, general principles for design -- Part 2: Technical principles

ISO 14121-1:2007 (JIS: Not yet issued)

Safety of machinery - Risk assessment -- Part 1: Principles

ISO 13849-1:2006 (JIS: Not yet issued)

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

ISO 13849-2:2003 (JIS: Not yet issued)

Safety of machinery - Safety-related parts of control systems -- Part 2: Validation

IEC 61508 Ed. 2.0:2010 (JIS: Not yet issued)

Functional safety of electrical/electronic/programmable electronic safety-related systems

IEC 61800-5-2:2007 (JIS: Not yet issued)

Adjustable speed electrical power drive systems - Part 5-2: Safety requirements – Functional

IEC 62061:2005 (JIS B 9961:2008)

Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems

IEC 60204-1:2005 (JIS B 9960-1:2008)

Safety of machinery -- Electrical equipment of machines -- Part 1: General requirements

BGIA Report 2/2008e

Functional safety of machine controls. -Application of ISO 13849-

BGIA Report 2/2008e provides abundant system examples and calculation examples for ISO 13849-1:2006 and PL calculation software SISTEMA. (in English)

Downloadable for free from: <http://www.dguv.de/ifa/en/pub/rep/pdf/rep07/biar0208/rep22008e.pdf>

JEMA 7206 (Tech. 09-03)

Guide to functional safety certification in machinery and equipment safety-related system engineering

Downloadable for free from: http://www.jema-net.or.jp/jema/data/fs_indus05.pdf

The Japan Machinery Federation (JMF) 21 Standardization-2 (March 2010)

Research report on the functional safety of printing machinery for FY2010

Downloadable for free from: http://www.jpma-net.or.jp/data/21_4.pdf

Safety Guidebook

Issued by the Nippon Electric Control Equipment Industries Association (NECA)

Available for purchase from: http://www.neca.or.jp/pub/books/books_books.cfm

3 Terms and Definitions

3.1 FS-PLC (A Functional Safety PLC)

Functional Safety Programmable Logic Controller

Definition: In this document, the PLC for which third-party safety certification is obtained based on the international standard on functional safety (IEC 61508), etc. is described as FS-PLC.

Explanation: Functional safety is defined in IEC 61508-4:2010 as follows:

Part of the overall safety relating to the EUC and the EUC control system that depends on the correct functioning of the E/E/PE safety-related systems and other risk reduction measures.

Further, functional safety is often misunderstood to “cover only Electrical/Electronic/Programmable Electronic (E/E/PE) equipment,” but IEC 61508 stipulates the overall “function of safety,” including maintenance, to ensure the safety degree of the Equipment Under Control (EUC).

For the main safety-related functions of the FS-PLC, please see Section 4.

3.2 SRP/CS (Safety-Related Parts of a Control System)

Safety-Related Parts of a Control System

Definition: Part of a control system that responds to safety-related input signals and generates safety-related output signals.

Explanation: Safety control systems comprising hydraulic, pneumatic and other mechanical elements, and electrical components such as sensors, FS-PLCs and relays. Among these, the electrical system is defined as an SRECS (Safety Related Electrical Control System) in IEC 62061:2005 (JIS B 9961:2008). If a monitoring system is used to diagnose the operation of SRP/CS, it is also considered part of the SRP/CS. Also, it is necessary to clearly distinguish between an ordinary control system and SRP/CS, and if they are indistinguishable, the whole control system must be considered SRP/CS. Further, in this document, a component of SRP/CS may be described as a “subsystem” in some cases.

3.3 PL (Performance Level)

Performance Level

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

Explanation: The quantitative safety degrees are stipulated for PL_a to PL_e by incorporating hardware failure rates and software safety requirements, as compared to the qualitative requirements for Category B, 1 to 4, as stipulated in EN 954-1 and ISO 13849-1:1999 (JIS B 9705-1:2000). For details of the PL, please see Section 6.

3.4 PL_r (Required Performance Level)

Required Performance Level

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

Explanation: PL_r is derived, based on Fig. A.1 - Risk graph - in the Annex A of ISO 13849-1:2006.

Because PL is the safety degree specific to ISO 13849-1:2006, risk graphs other than that in Fig. A.1,

for example, the risk matrix in IEC 62061:2005 and the risk graph in IEC 61508 Ed.2:2010, should not be used to derive PLr. Further, the relationship between PL and SIL is shown in Table 4 in ISO 13849-1:2006.

3.5 Safety Block Diagram

The components of SRP/CS shown in the form of a block diagram

Definition: For calculating the PL of SRP/CS, this diagram is used to clarify the subsystem configuration.

Explanation: SRP/CS usually comprises three subsystems: “input, control and output subsystems.” Also, each subsystem may have a redundant configuration to increase the degree of safety in some cases. Therefore, in order to clarify each subsystem configuration and explain the procedures for calculating the PL of SRP/CS, a safety block diagram is used (for an example description, please see Fig. 5 in Section 6.2).

3.6 B10d

Number of operating cycles required for 10% of components to reach dangerous failure (Unit: cycles)

Definition: Number of cycles until 10% of the components fail dangerously (for pneumatic and electromechanical components)

Explanation: To calculate MTTFd, the figures should be requested from the component manufacturers. In Annex C of ISO 13849-1, the MTTFd values for mechanical and hydraulic components can be estimated at 150 years, if the conditions are satisfied. For the pneumatic and electrical components with a mechanical life dependent on the number of operating cycles, such as push buttons, relays and magnetic contactors, B10d values may be taken from Table C.1 of Annex C of ISO 13849-1 if they meet the requirements in Annex C, or should be obtained from the respective component manufacturers. Further, semiconductors, such as transistors and IGBT, and safety system components, such as FS-PLCs and safety inverters without relay output, have no B10d value because their life cannot be considered dependent on the number of operating cycles.

3.7 MTTFd (Expectation of the Mean Time to Dangerous Failure)

Estimates of the Mean Time to Dangerous Failure

Definition: Expectation of the mean time to dangerous failure

Explanation: This is the reciprocal value of a dangerous failure rate λ_d , and is usually annualized. The MTTFd values for components with B10d values are calculated using the following equation, but may be considered determinable simply by the operating cycles per year.

For more details, please see Annex C.4 of ISO 13849-1:2006.

$$MTTFd = B10d / (0.1 \times n_{op})$$

Where, $n_{op} = d_{op} \times h_{op} \times 3,600 [s/h] / t_{cycle}$

d_{op} : Operating days/year [d/y], h_{op} : Operating hours per day [h/d],

t_{cycle} : Operating cycle time [s/cycle]

For the MTTFd values for semiconductors, etc., reference must be made to Tables C.2 - C.7 of Annex C of ISO 13849-1:2006, or failure rate databases quoted, such as SN 29500 and MIL-HDBK-217F, which are recognized by third-party certification organizations. For safety system components, such as

FS-PLC, certified by third-party organizations, confirmation of the MTTFd values from respective component manufacturers must be requested.

3.8 DCavg (average of Diagnostic Coverage)

DCave (Average of Diagnostic Coverage) [Category: none/medium/high]

Definition: Average of Diagnostic Coverage specific for individual components composing the SRP/CS.

Explanation: The average of DC for individual components is considered to be the self-diagnostic coverage for the SRP/CS, and categorized to estimate the PL. This categorization is specific to ISO 13849-1:2006, and for more detail, please see Annex E.2 of ISO 13849-1:2006. The definition of DC is identical to that in IEC 61508-4:2010.

$$DC = \lambda_{DD} / \Sigma \lambda_{Dtotal}$$

Where, λ_{DD} : Detectable dangerous failure rate

λ_{Dtotal} : Total dangerous failure rate ($\lambda_{DD} + \lambda_{DU}$: Undetectable dangerous failure rate)

3.9 CCF (Common Cause Failure)

Common cause failure [Score]

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

Explanation: There are causes due to external environmental factors, such as electromagnetic noise, high temperature and corrosive gas, producing random failures, and organizational and structural causes, such as component designer's ability, producing systematic failures. They are causes of major hardware failures in redundant systems, quantification methods of which are described in detail in Annex D of IEC 61508-6:2010.

In ISO 13849-1:2006, measures against CCF are scored in Table F.1 of Annex F, and in the case of the SRP/CS in categories 2, 3 and 4, additional measures are required unless the total score is 65 or better.

3.10 PFHd (Probability of Dangerous Failure per Hour)

Probability of dangerous failure per hour (PFHd)

Definition: Average probability of SRP/CS (\supset SRECS) of dangerous failure within 1 hour

Explanation: This indicator is not clearly expressed in ISO 13849-1:2006. However, the probability values of a dangerous failure per hour listed in Table 3 in Section 4.2.2 and Table K.1 in Annex K of ISO 13849-1:2006 are identical to PFH in IEC 61508 and PFHd in IEC 62061. The PL of the SRP/CS can be also calculated by obtaining the total of PFHd values of individual components.

3.11 Stop functions

The stop control function of machinery stipulated in Section 9.2.2 of IEC 60204-1:2005 (JIS B 9960-1:2008)

Definition: Categories of stop function of safety-related machinery and equipment.

Explanation: There are three categories of stop functions as follows:

- Stop category 0: Stopping by immediate removal of power to the machine actuators (i.e. an uncontrolled stop)

- Stop category 1: A controlled stop with power available to the machine actuators to achieve the stop and then removal of power when the stop is achieved

- Stop category 2: A controlled stop with power left available to the machine actuators

For example, Category 0 includes the motor power-off in an emergency stop, category 1 includes regeneration braking by an inverter, and category 2 includes an elevator floor leveling control after the elevator has reached a destination floor.

3.12 EDM (External Device Monitoring)

Safety-related external device monitor

Definition: means by which the FS-PLC monitors the state of control devices which are external to the FS-PLC.

Explanation: Emergency stop switches and magnetic contactors themselves connected to the FS-PLC have no self-diagnostic function. Therefore, the FS-PLC would check their actions, and if any action is abnormal, stop their output. Such a function is called EDM or back-check.

For EDM actions, please see Section 5.2.

3.13 Unexpected/Unintended Start-up

False start-up of machinery as defined in ISO 12100-1:2003 (JIS B 9700-1:2005)

Definition: Any start-up which, because of its unexpected nature, generates a hazard.

Explanation: Concrete examples of unexpected/unintended start-up are shown below:

- Start-up due to a logic control subsystem malfunction caused by external noise, parts failure, etc.
- False start-up command caused by failure of any push button, magnetic contactor, etc.
- Automatic start-up unexpected by operator when the power source returns after interruption.
- False start-up caused by effects within and outside machinery and equipment, such as gravity, wind, spontaneous combustion of internal combustion engine, etc.
- Operator's misoperation.

4 Features of the FS-PLC

A Functional Safety PLC (FS-PLC) is a controller whose safety-related system control PL (generally PLe*) is certified by third-party organizations, such as TÜV Rhineland and TÜV SÜD. For the PLe, DCavg must be 99% or higher, hence the degree of safety required for a general-purpose PLC is set to be two or more digits higher. To achieve PL, an FS-PLC often includes, in addition to the functions of a general-purpose PLC, the following safety functions:

- Hardware multiplexing, redundancy and safety-related self-diagnostic circuits.
- Application multiplexing operations and the detection of any inconsistency in operation results.
- Complete separation between safety- and non-safety related parts.
- Dedicated safety-related application development tools.

*: An FS-PLC often has concurrent certifications obtained from ISO 13849-1:2006 PLe; EN954-1/ISO 13849-1:1999 Category 4; IEC 61508 SIL 3 and IEC 62061 SIL 3.

4.1 Hardware multiplexing, redundancy and safety related self-diagnostic circuits

Circuits whose hardware main part structures (input, logic control and output parts) are made multiplexed and redundant to retain the safety control function, even in the event of component failure. Also, they always self-diagnose safety control related components to detect any failure promptly and control the system to stop on the safe side (fail-safe). Moreover, it generally follows that the more hardware is used, the higher the overall failure rate becomes, hence the reliability (MTTF) of an FS-PLC will be lower, compared with that of a general-purpose PLC of equivalent scale. However, the safety (MTTFd) has been raised by the multiplexing, redundancy and diagnostic functions as mentioned above (reliability≠safety).

4.2 Application multiplexing operations and the detection of inconsistency in operation results

By operating user applications, for example, using positive and negative logic, and checking the consistency of the results, a FS-PLC prevents unsafe actions due to any trouble involving the firmware performing user applications.

4.3 Complete separation between safety- and non-safety related parts

Safety related information processing systems, including a RAM area for storing safety information, and firmware and communication protocol processing parts for processing and transmitting the same, are made completely separated from non-safety information processing systems (for example, an upper-level communication processing part with Ethernet). This prevents any non-safety related processing system malfunction from affecting safety-related information processing systems.

4.4 Dedicated safety application development tools and dedicated communication protocols to communicate with FS-PLCs

Some dedicated safety application development tools are the same in the user interface with general-purpose PLC tools, but others are constructed as very different internal processing systems to prevent any unexpected FS-PLC malfunction due to applications. For example, various kinds of processing to increase the degree of safety, such as strict grammar checking, positive logic/negative logic object code generation, and double

checking in communication with FS-PLCs, are performed internally.

5 Usage of the FS-PLC

5.1 Emergency stop and start-up/restart

For a control system (CS), safety-related parts (SRP/CS) and non-safety-related parts must be clearly separated. The key functions performed by an FS-PLC as a logic control subsystem of the SRP/CS are the monitoring and control of a) emergency stop, b) start-up, and c) restart of machine and equipment. The relationship of these functions is shown in Fig. 1.

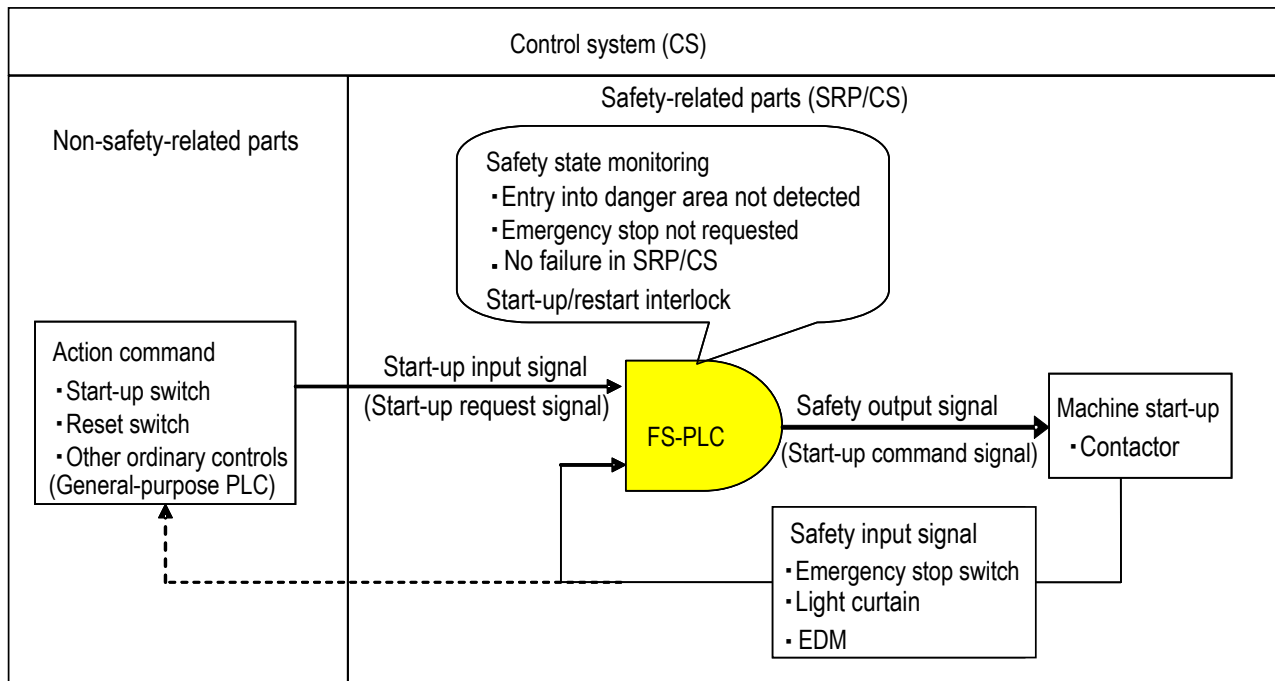


Fig. 1: Functions and actions of FS-PLC

a) Emergency stop

When the safety state is maintained by safety state monitoring, ensuring no entry into the danger area detected by safety sensors, no emergency stop requested and no failure found in the SRP/CS, the FS-PLC receives a safety input signal from the safety state monitoring, and issues a safety output signal permitting the machine operation. If emergency stop requests, etc. are issued, the safety input signal is turned off, and the FS-PLC turns off the safety output signal to bring the machine to an emergency stop.

b) Start-up

Start-up means that a machine actually begins operating, and only when the safety state is secured by the safety state monitoring, the FS-PLC sends a start-up command signal to the machine, then the machine starts up. Unless the safety state is secured, the machine will not start up, even if the start-up switch is pushed. Therefore, the action command relating to start-up (start-up switch, etc.) is the non-safety-related parts, but the control relating to start-up is included in the safety-related parts.

c) Monitoring and control of restart

“Unexpected start-up,” where a machine restarts suddenly due to power returning, etc. after a temporary machine stoppage due to power failure, is extremely dangerous. The FS-PLC and safety state monitoring prevent the machine’s unexpected start-up by issuing a machine start-up command signal when a start-up request signal is generated in the state whereby safety is secured. This function is known as a start/restart interlock.

Further, even when the start-up/restart interlock is configured, any welding of the start-up switch may result in the unexpected start-up of the machine, hence the falling of the start-up switch signal must be used in the start-up request.

5.2 Diagnosis of external devices (EDM and pulse test)

Usually the FS-PLC has, in addition to the emergency stop and start-up/restart interlock as mentioned above, a) a diagnostic function of operational switches (input subsystem of the SRP/CS) and magnetic contactors (output subsystem), and b) a diagnostic function of input/output wiring by a pulse test.

a) Diagnosis of the input/output subsystem

In constructing a circuit of category 3 or higher, safety input devices with safety certifications, such as emergency stop switches, have duplex contacts, and are often wired to the FS-PLC respectively. By monitoring the mismatch of duplex contacts (in the case of NC: normally closed /NO : normally open, duplex contacts are matching), the contact welding of input devices can be diagnosed.

Further, for force-guided relays or contactors of output subsystems, it is possible to diagnose the welding of the main contacts by monitoring the action of the b-contact (NC contact) linked with a main contact. (EDM)

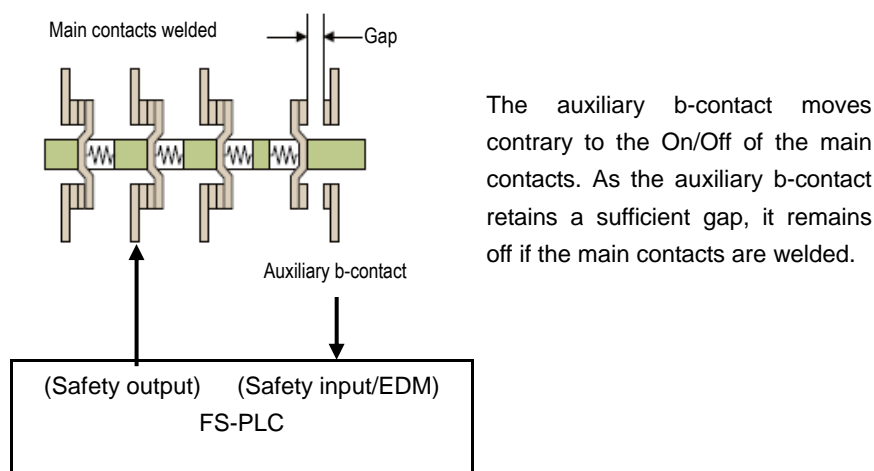


Fig. 2 Diagnosis of contacts (EDM) by monitoring contactor b-contact (NC contact)

b) Diagnosis of shorts in input/output wiring by pulse test

One of the most serious faults in the SRP/CS is that real signals remain on due to the I/O signal lines becoming shorted with other signals, even if the circuit is turned off by the operating switch or on the FS-PLC side. The pulse test is a function involving occasional transmission of an OFF pulse to the I/O circuit in

the ON state, and diagnosing that wiring is proper if the OFF pulse returns and a wiring is short circuited if OFF pulse does not return.

Further, the pulse test is effective for NC circuits of operating switches, etc., but cannot diagnose the wiring of non-NC circuits such as light curtain. The details of the pulse test differ depending on the FS-PLC used, and it is necessary to refer to the manufacturer's instruction manual.

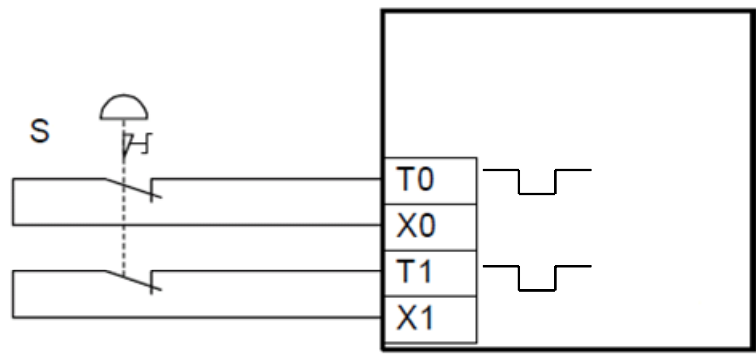


Fig. 3 Example of input wiring connection of the FS-PLC when conducting a pulse test

6 Performance level (PL)

When safety-related parts of control systems (SRP/CS) are designed, a risk assessment is initially carried out to identify the hazard sources. And PL (PLr) required from the hazard sources is determined based on Figure A.1 - Risk graph - of Annex A of ISO 13849-1:2006. Next, the scope of the SRP/CS (software and hardware) in the control system is determined, and the selection, design and manufacture of devices are carried out so that the category of PL of the SRP/CS may be equivalent to or higher than that of the specified PLr. As for the testing process of the SRP/CS, verification is carried out to check that individual subsystems are satisfying the PL of the requirements specifications. After that, validation is carried out to check the whole SRP/CS is satisfying the specified PLr (verification and validation).

6.1 Software requirements

The PL for application software in the FS-PLC is considered to have satisfied the basic conditions of PLa to PLe if the development, testing and validation are carried out in conformity with the “Figure 6 - Simplified V-model of the software lifecycle” of ISO 13849-1:2006. As for the application of PLc to PLe, the additional requirements in Section 4.6.2 a) to j) must be met. It may initially appear difficult, but it is manageable if the management system for development and testing in accordance with ISO-9001 is established.

6.2 Procedures for calculating hardware PL (Example of calculating PL of SRP/CS)

The PL for hardware can be obtained from B10d, MTTFd, DCavg, CCF, PFHd and the safety category of each subsystem. Descriptive examples used for calculating the PL of the SRP/CS for an emergency stop system are shown below.

a) System configuration diagram

- If an emergency stop switch is pushed, the contactors are turned off and the motor is powered off.
- Emergency stop switches and contactors are constantly monitored by the EDM function of the FS-PLC.

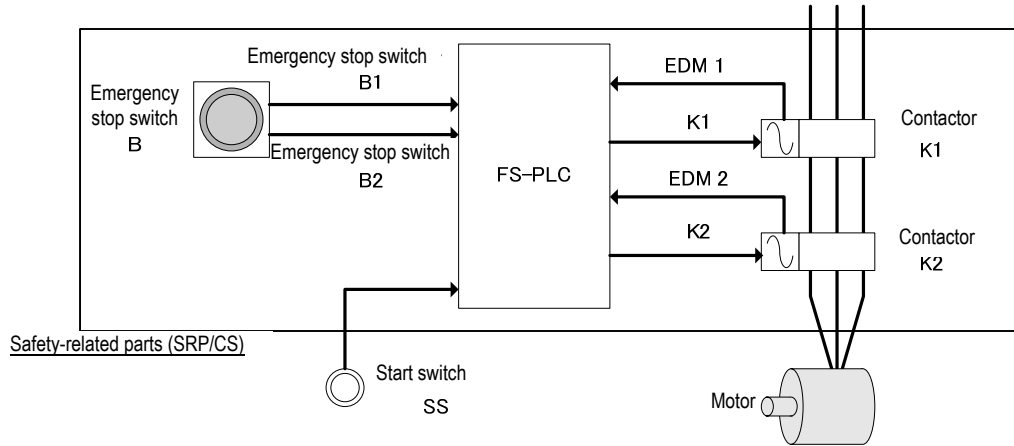


Fig. 4: Emergency stop system configuration diagram

b) Safety block diagram

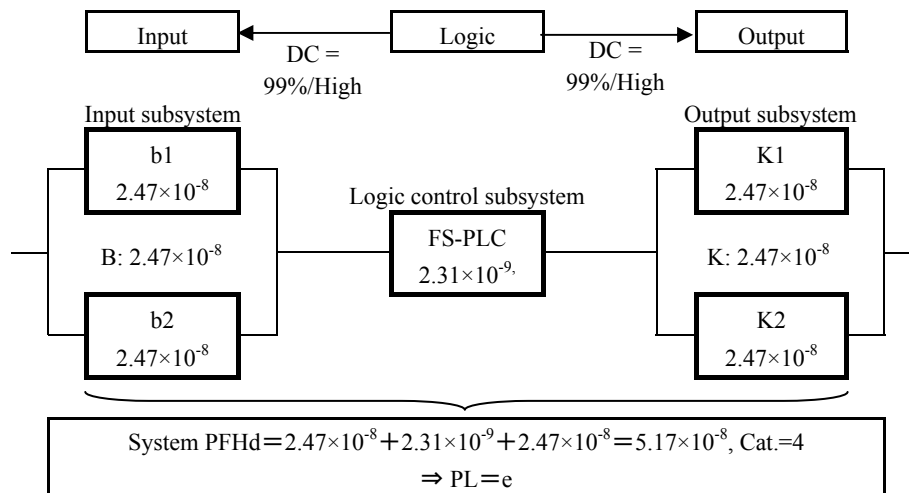


Fig. 5: The safety block diagram of the emergency stop system

c) The parameters of safety devices

Table 1: The parameters of the emergency stop system safety devices

Sub-system	Part number	Part name	B10d 1,000times	MTTFd [Year]	MTTFd Value[Year]	DCavg [%]	PFHd [/hour]	Category
Input	B	Emergency stop switch	1,000	833k	100	99	2.47×10^{-8}	4
Logic	FS-PLC	FS-PLC	-	-	100	99	2.31×10^{-9}	4
Output	K1	Contactor	2,000	3,424	100	99	2.47×10^{-8}	4
	K2	Contactor	2,000	3,424	100	99		
System PFHd= $2.47 \times 10^{-8} + 2.31 \times 10^{-9} + 2.47 \times 10^{-8} = 5.17 \times 10^{-8}$, Category=4 \Rightarrow PL=e								

1) Input subsystem

- B10d=1,000 thousand times for the emergency stop switch B: Values provided by the device

manufacturer

- Number of operating times per year $n_{op}=12$ times
 - $MTTFd=B10d/(0.1 \times n_{op})=833 \times 10^3$ year (MTTFd value=100 years)
 - $DCavg=99\%$: Table E.1 - Input device - of Annex E (Duplex input monitoring of NC contacts by the FS-PLC)
- $\Rightarrow PFHd=2.47 \times 10^{-8}$: Table K.1 of Annex K (MTTFd value =100 years, Cat.=4, $DCavg=high$)

2) Logic subsystem

- $PFHd=2.31 \times 10^{-9}$: Values provided by the device manufacturer
- $DCavg=99\%$: Values provided by the device manufacturer
- Cat.=4 : Values provided by the device manufacturer

3) Output subsystem

- $B10d=B10 \times 2=2,000$ thousand times for contactor K: $B10=1,000$ thousand times provided by the device manufacturer
 - Operating days=365days/year, operating hours=16 hours/day, cycle time= 1 cycle/hour
 - $MTTFd=B10d/(0.1 \times n_{op})=2,000k/(0.1 \times 365 \times 16 \times 1)=3,424$ years (MTTFd value=100 years)
 - $DCavg=99\%$: Table E.1 - Output device - of Annex E (Constant operation monitoring of NC contacts by the FS-PLC)
- $\Rightarrow PFHd=2.47 \times 10^{-8}$: Table K.1 of Annex K (MTTFd value=100 years, Cat.=4, $DCavg=high$)

4) PFHd calculation and PL values for the emergency stop system

- From Fig. 5, $PFHd_{total} = PFHd_{in}:2.47 \times 10^{-8} + PFHd_{logic}:2.31 \times 10^{-9} + PFHd_{out}:2.47 \times 10^{-8}$
 $=5.17 \times 10^{-8}$
 - From 1) to 3) mentioned above , $DCavg_{total}=(DCavg_{in}:99\% + DCavg_{logic}:99\% + DCavg_{out}:99\%)/3=99\%$
 - From Fig. 5, Cat.=4: Section 6.2.7 Category 4 (Figure 12 - Architecture for category 4)
- $\Rightarrow PLe/PFHd=5.17 \times 10^{-8}$: Table K.1 of Annex K (MTTFd value=100 years, category=4, $DCavg=high$)

Reference: In this example, the safety index was calculated using PL evaluation software, SISTEMA, provided free of charge by the IFA (former BGIA; the Institute for Occupational Safety and Health of the German Social Accident Insurance). SISTEMA is downloadable from the following website:

<http://www.dguv.de/ifa/en/pra/softwa/sistema/index.jsp>

Further, parameters of the safety devices for use in SISTEMA are available from the NECA catalog site:

<http://www.necagate.com/safety/>

7 Safety Circuit Examples

7.1 Introduction

This chapter presents actual examples of safety circuits. Each section is commonly structured as shown in Table 2. It is possible to understand the outline of the safety functions in Sections 7.x.1 and 7.x.2, and the configurations and action examples of safety functions in Sections 7.x.3 and 7.x.4. In Sections 7.x.5 and 7.x.6, PL values are obtained based on the respective configuration examples.

The values of PL_r described in this document are tentative in order to show the calculation process. Actually, PL_r values must be derived after conducting a risk assessment of individual machines.

Table 2: Structure of Chapter 7

Section No.	Title	Contents
7.x.1	Image of machinery/equipment	Outlines of machinery and equipment to which the safety functions are applied are illustrated in figures.
7.x.2	Function	The purpose and action of safety functions are described. Particularly, how the state changes following a specific event is explained using a state transition table.
7.x.3	Circuit configuration	Assuming FS-PLCs are used, the method of connecting them with safety sensors, switches and actuators is illustrated in figures. In particular, safety related parts are shown in half-tone dot meshing in figures. Terminal names and numbers are only exemplary, and peripheral circuits such as ground circuits are not shown in figures, so the actual wiring connections must be made correctly according to the products' instruction manuals. In this section the duplex mismatch treatment and the back-check (EDM) of safety relay/contactors, explanation is omitted except in "7.2 Emergency stop switch."
7.x.4	Timing chart	The actions and relationships of the switches and contacts illustrated in 7.x.3 are shown in the timing chart. As it is difficult to chart the combination of all actions, only a timing chart of representative actions is shown to help understand actions.
7.x.5	The parameters of safety devices	The safety devices used in 7.x.3 and their parameters are listed. However, in calculating the individual values of MTTF _d , n _{op} of 6.2 c) is used. To calculate the PL actually, the failure rate and diagnostic rate values of each product must be used.
7.x.6	Safety block diagram	The safety system components and architecture are clarified, and the PL of the whole safety system is calculated using the indicators shown in 7.x.5. For details of the calculation, please see Chapter 6.
7.x.7	Others	Other contents to be specially explained about the safety function are described, if any.

7.2 Emergency stop: Emergency stop switch

7.2.1 Examples of use in machinery and equipment

An emergency stop switch and a safety relay are connected to the FS-PLC to bring a machine to an emergency stop by turning off the main contact of the contactor, which switches the power supply to the machine on/off, at the contact of the safety relay by the operation of the emergency stop switch (in the emergency stop signal OFF state). In this connection state, the FS-PLC controls the safety relay to turn on/off the main contact of the contactor, which is programmed to switch the power supply to the machine on/off.

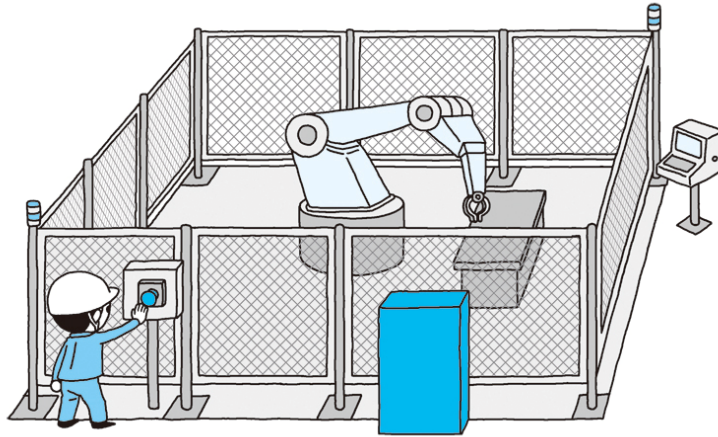


Fig. 6: Emergency stop switch

* Prepared with reference to the illustration in p. 29 of the “Safety Guidebook,” Nippon Electric Control Equipment Industries Association (NECA), 2004 (3rd edition)

7.2.2 Function

- If the emergency stop switch (B) is pushed down, the FS-PLC will shut off the power source to the machine by turning off the start-up command and contactors (K1, K2). This ensures the safety of the machine.
- When the emergency stop switch (B) is released (signal ON), contactors (K1, K2) are turned on by the operation ready switch, enabling the machine to start up, and the start-up switch turns on the start-up command to start up the motor.
- Particularly if safety is ensured, it is also possible to start up the machine motor by using only the start-up switch and not the operation ready switch, by turning on the contactors when the emergency stop switch is released.
- Unless the contactor monitoring b-contacts (EDM1, EDM2) are turned on within a specified time after the contactors (K1, K2) are turned off, or conversely, unless the contactor monitoring b-contacts are turned off within a specified time after the contactors are turned on, the contactors are deemed to be out of order and the start-up of the motor is prohibited. If this EDM error is detected, the output of the FS-PLC will be turned off.

The FS-PLC program realizes the functions listed in Table 3.

Table 3: State transition table

State	Event (change)	Action	Next state
(1) Emergency stop Motor=Stop B1, B2=Operation (Signal OFF) K1, K2=OFF	B1, B2=Released	None	(2) Emergency stop released
	Remain at EDM1 or EDM2=OFF after a specified time	None	(5) EDM error state
(2) Emergency stop released Motor=Stop B1, B2=Released (signal ON) K1, K2=OFF	Operation ready switch RS=ON	K1, K2=ON	(3) Operation ready
	B1, B2=Operation	None	(1) Emergency stop
(3) Operation ready Motor=Stop B1, B2=Released (signal ON) K1, K2=ON	Start-up switch SS=ON	Start-up command M=ON	(4) In operation
	B1, B2=Operation	K1, K2=OFF	(1) Emergency stop
	Remain at EDM1 or EDM2 = ON after a specified time	K0,K1=OFF	(5) EDM error state
(4) In operation Motor=ON B1, B2=Released (signal ON) K1, K2=ON	B1, B2= Operation	K1, K2=OFF Start-up command M=OFF	(1) Emergency stop
(5) EDM error state Motor=Stop B1, B2=Indefinite K1, K2=OFF	If B1, B2=OFF, EDM1=EDM2=ON	None	(1) Emergency stop
	If B1, B2=ON, in the state of EDM1=EDM2=ON, operation ready switch=ON	K1,K2=ON	(3) Operation ready

7.2.3 Circuit configuration

An example circuit configuration of emergency stop switches is shown in Fig. 7.

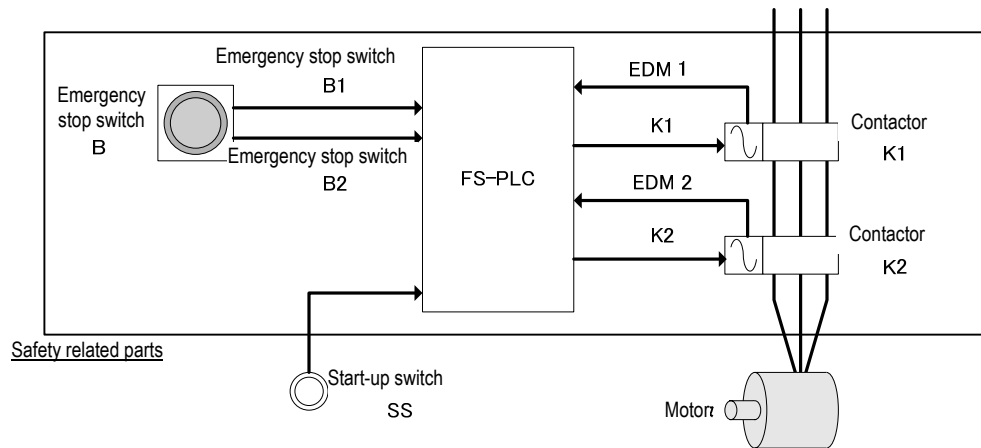


Fig. 7: Example circuit configuration of emergency stop switches

7.2.4 Timing chart

The timing chart for emergency stop switches is as shown in Fig. 8.

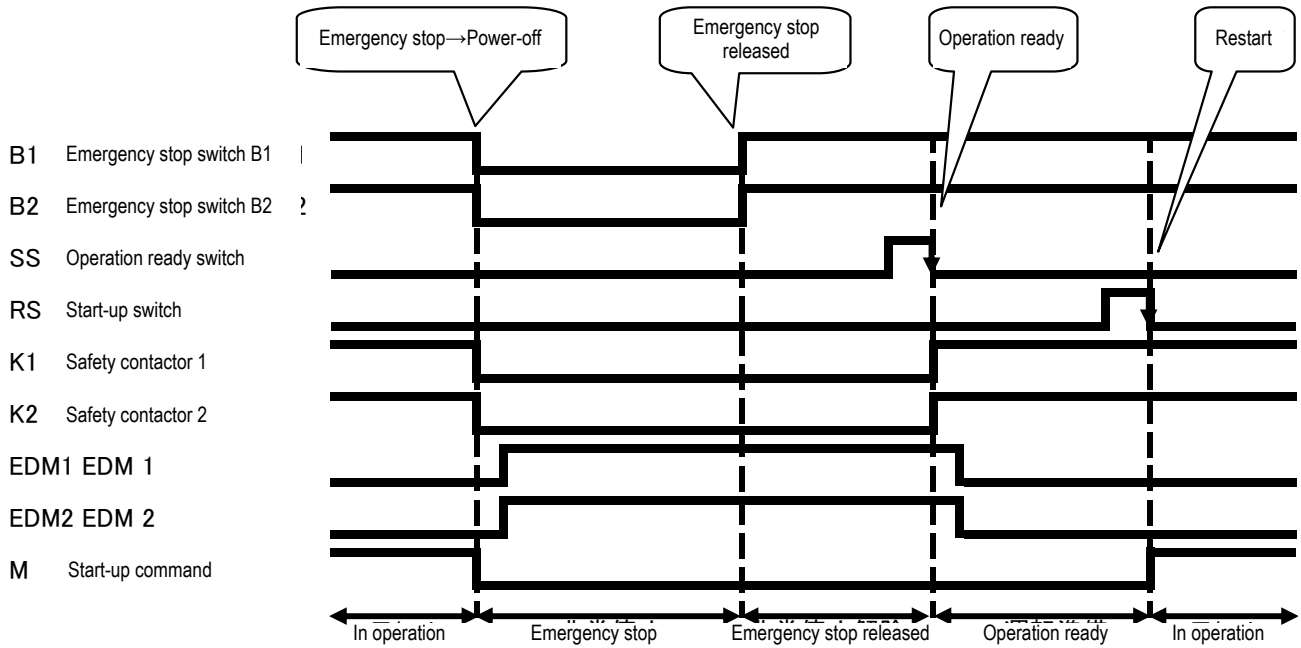


Fig. 8: The timing chart for emergency stop switches

7.2.5 Parameters of safety devices

The parameters of the safety devices for an emergency stop switch are as shown in Table 4.

Table 4: The parameters of the safety devices for an emergency stop switch

Part No.	Part name	B10d [1,000 times]	MTTFd [year]	MTTFd value [year]	DCavg [%]	PFHd [hour]
B	Emergency stop switch	1,000	833k	100	99	2.47×10^{-8}
FS-PLC	FS-PLC	—	—	100	99	2.31×10^{-9}
K1	Contactor	2,000	4,167	100	99	2.47×10^{-8}
K2	Cntactor	2,000	4,167	100	99	2.47×10^{-8}

$$B: n_{op}=12[\text{cycle/y}], K1/K2 : n_{op}=1[\text{cycle/h}] \times 16[\text{h/d}] \times 300[\text{d/y}]=4,800[\text{cycle/y}]$$

7.2.6 Safety block diagram

A safety block diagram of emergency stop switches is as shown in Fig. 9.

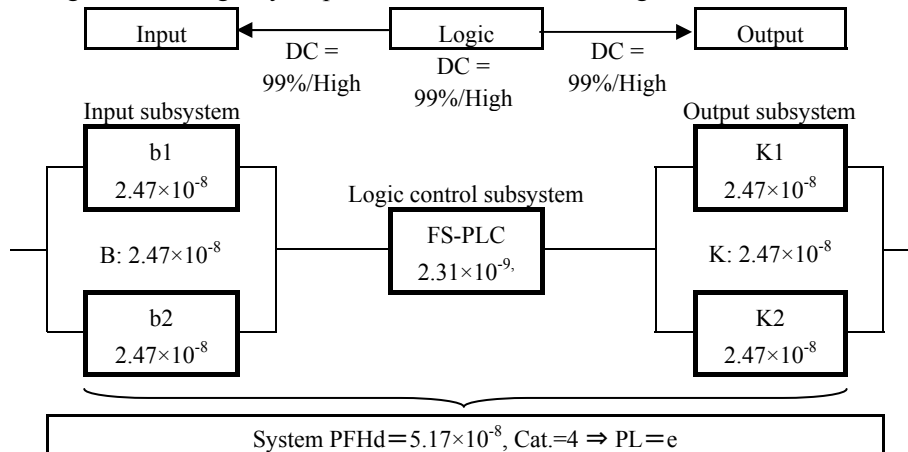


Fig. 9: The safety block diagram of emergency stop switches

7.3 Emergency stop of a machine by regenerative braking: Off-delay timer

7.3.1 Image of machinery and equipment

An example application of an off-delay timer to the emergency stop of a processing machine is shown in Fig. 10. If the door is opened, an emergency stop function activates regenerative braking to stop the motor of the processing machine, and then the off-delay timer shuts off the power (stop category 1). In this example, PLr=d is decided by a result of risk assessment. The door is unlocked, considering the response time to the stop of the hazard.

If it takes time for the machine to stop, a interlocking with guard locking is often used in combination with this application for guard locked until the machine stops (Please see Section 7.5).

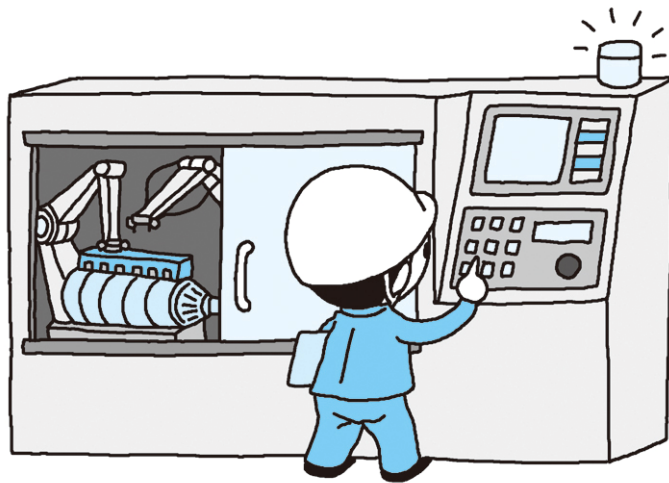


Fig. 10: Image of application of an off-delay timer

* Prepared with reference to the illustration in p. 19 of the "Safety Guidebook," Nippon Electric Control Equipment Industries Association (NECA), 2007 (5th edition)

7.3.2 Function

The stopping system by stop category 0 will stop the drive unit in free run mode, but if it takes too long to stop, The stopping system by stop category 1 is used. Generally, an off-delay timer is used for power-off of hazard after the stop.

- When the contact of door interlock switch is opened, the FS-PLC will turn off the start-up command (M) and start to decelerate the motor by regenerative braking
- After a delay time, the FS-PLC will turn off contactors (K1, K2) by off-delay timer and shut off the power of the motor. This ensures the safety of the machine.
- The delay time of an off-delay timer is needed more than the stopping time of the motor.
- When the contact of door interlock switch (B) is closed (signal ON) and the operation ready switch (RS) is turned on, the contacts of contactors (K1, K2) are closed, the motor is ready for start-up, and then the

motor is start-up by the start-up command (M) of the start-up switch (SS).

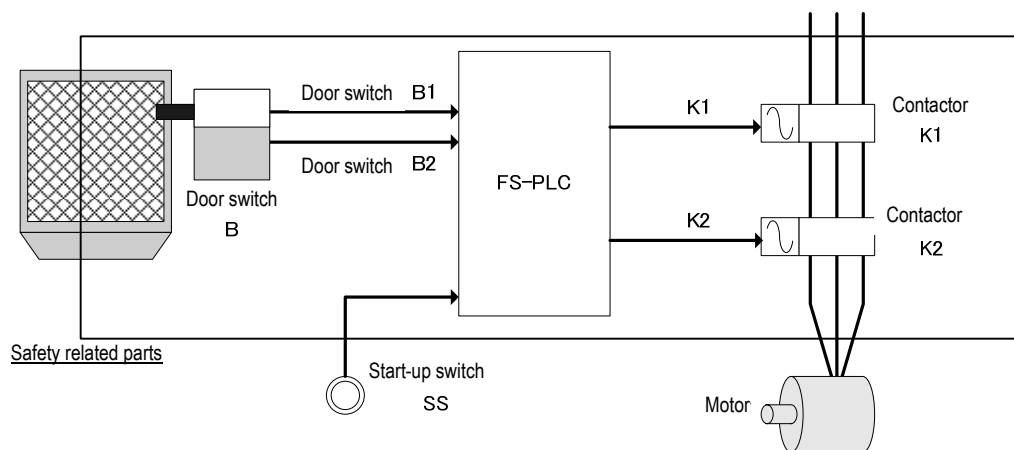
- Especially if the operator don't remain inside this machin, it can be start up of the machine only by the start-up switch (SS) which turning on the contactors (K1, K2)when the door is closed, not to use the operation ready switch (RS). .

Table5: State transition table

State	Event (change)	Action	Next state
(1) Stop Motor stop Start-up command M=OFF Contactors K1, K2=OFF	Operation ready switch RS=ON	Contactors K1, K2=ON	(2) Operation ready
(2) Operation ready Motor stop Start-up command M =OFF Contactors K1, K2=ON	Door switch (B)=Open, Signals (B1, B2)=OFF	None	(4) In deceleration (In the motor stop state, transition to the stop state after off-delay time has elapsed)
	Start-up switch (SS)=ON	Start-up command M =ON	(3) In operation
(3) In operation Motor operating Start-up command M =ON Contactors K1, K2=ON	Door switch (B)=Open, Signals (B1, B2)=OFF	Start-up command M =OFF (Deceleration start)	(4) In deceleration
(4) In deceleration Motor operating Start-up command M =OFF Contactors K1, K2=ON	Off-delay time has elapsed	Contactors K1, K2=OFF	(1) Stop

7.3.3 Circuit configuration

An example circuit configuration of an off-delay timer is shown in Fig. 11.



* Separately, an EDM monitoring circuit is necessary to input the contactor b-contact into the FS-PLC.

Fig. 11: Example circuit configuration of an off-delay timer

7.3.4 Timing chart

The timing chart for an off-delay timer is as shown in Fig. 12.

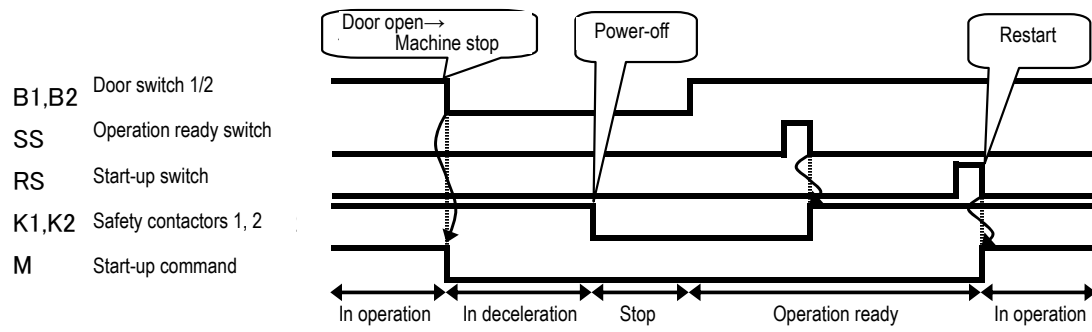


Fig. 12: The timing chart for an off-delay timer

If a door switch is opened, a forced stop of the drive will start with the drive stop contact OFF, and after the off-delay time, safety relays K0 and K1 will be OFF to power off the drive.

7.3.5 Parameters of safety devices

The parameters of the safety devices in stop category 1 (off-delay timer) are as shown in Table 6.

Table 6: The parameters of the safety devices in stop category 1 (off-delay timer)

Part No.	Part name	B10d [1,000 times]	MTTFd [year]	MTTFd value [year]	DCavg [%]	PFHd [hour]
B	Door switch	500	520	100	99	2.47×10^{-8}
FS-PLC	FS-PLC	—	—	100	99	2.31×10^{-9}
K1	Contactor	2,000	2,080	100	99	2.47×10^{-8}
K2	Contactor	2,000	2,080	100	99	2.47×10^{-8}

$$B/K1/K2: n_{op}=2[\text{cycle/h}] \times 16[\text{h/d}] \times 300[\text{d/y}] = 9,600[\text{cycle/y}]$$

7.3.6 Safety block diagram

The safety block diagram of an off-delay timer is as shown in Fig. 13.

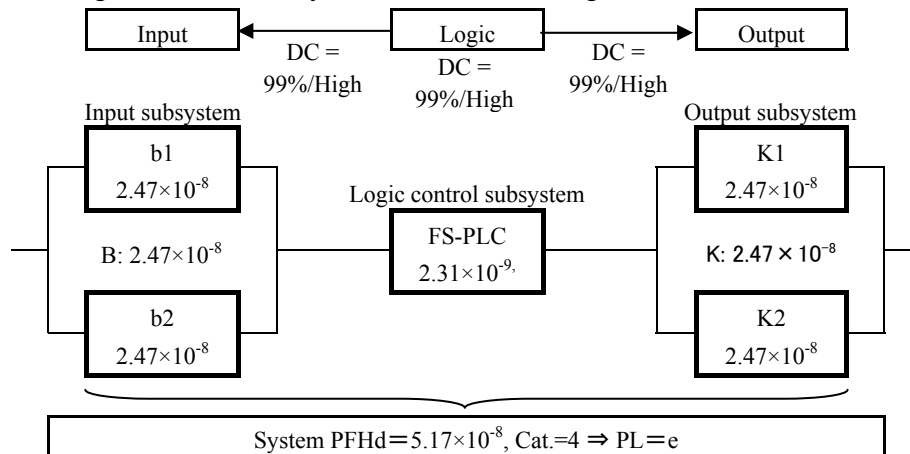


Fig. 13: The safety block diagram of an off-delay timer

7.3.7 Others

There are also some inverters incorporating an off-delay timer and safety relay functions and providing safety control.

7.4 Machine start/stop in unlocked guard: Guard monitoring

7.4.1 Image of machinery and equipment

In the image shown below, the movable guard is closed during the work processing by a robot. If a worker opens the movable guard while the robot is in operation, the robot will make an emergency stop. It is necessary to confirm that the movable guard is closed before starting up the robot, and the start-up must be made from outside the guard (safety fence).

The open/close state of the movable guard of the safety fence is constantly monitored by the localization switch. If the safety system fails, including the localization switch, there is a possibility of contact between the robot in operation and the worker, which may cause serious injury. For such reasons, based on the risk assessment, the required performance level (PLr) is determined to be e. As for operating conditions, the robot is supposed to operate 16 hours a day, 365 days a year, with a cycle time of 1 hour.

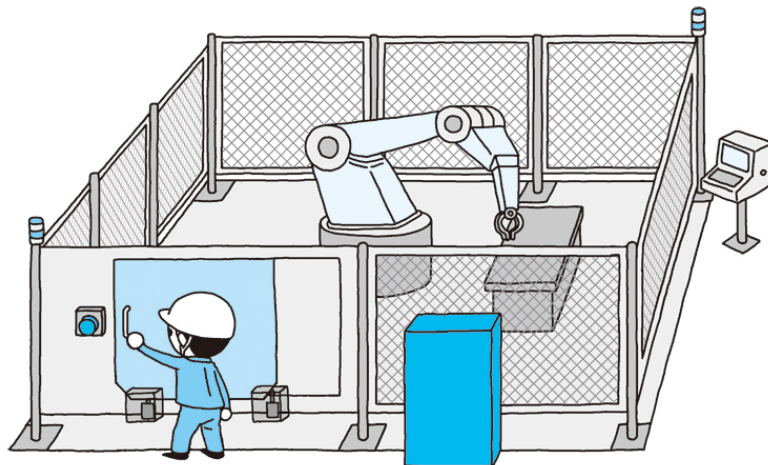


Fig. 14: Robot processing system

* Prepared with reference to the illustration in p. 29 of the “Safety Guidebook,” Nippon Electric Control Equipment Industries Association (NECA), 2004 (3rd edition)

7.4.2 Function

The danger zone is protected by a fixed guard (a safety fence) and a movable guard. The opening of the movable guard is detected by two door-monitoring switches (B1/B2). Both NC- and NO-type door monitoring switches are used in combination, and the FS-PLC checks the open/close state of the door and any failure of the contacts based on the state of the two switches. The FS-PLC prevents any dangerous action or state by driving two contactors (K1, K2) and shutting off K1 and K2.

- Any failure of contactors (K1, K2) is detected by EDM monitoring of the FS-PLC, and only when normal, K1 and K2 will be ON. No start-up test featuring the opening/closing of protective devices is necessary.

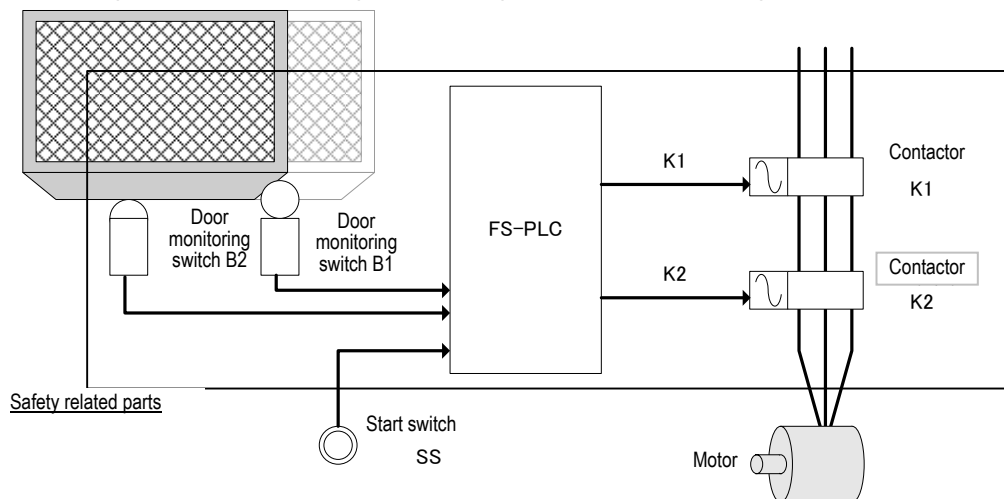
Table 7: State transition table

State	Event (change)	Action	Next state
(1) Door open Door open (B1=ON, B2=OFF) Motor stop (K1, K2=OFF)	Door closed (B1=OFF, B2=ON)	None	(2) Door closed, stop
(2) Door closed, stop Door closed (B1=OFF, B2=ON) Motor stop (K1, K2=OFF)	Door open (B1=ON, B2=OFF)	None	(1) Door open
	Start-up switch (SS=ON)	K1, K2=ON	(3) In operation
(3) In operation Door closed (B1=OFF, B2=ON) Motor in operation (K1, K2=ON)	Door open (B1=ON, B2=OFF)	K1, K2=OFF	(1) Door open

7.4.3

7.4.4 Circuit configuration

The circuit configuration of monitoring a movable guard is as shown in Fig. 15.



* Separately, an EDM monitoring circuit is necessary to input the contactor b-contact into the FS-PLC.

Fig. 15: The circuit configuration of monitoring a movable guard

7.4.5 Timing chart

The timing chart of monitoring a movable guard is as shown in Fig. 16.

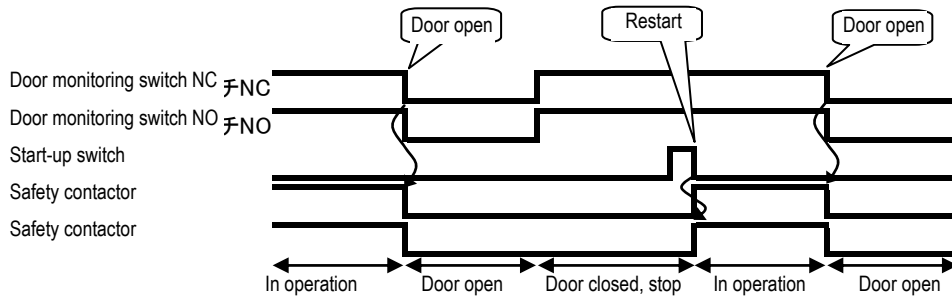


Fig. 16: The timing chart of monitoring a movable guard

7.4.6 Parameters of safety devices

The parameters of the safety devices are as shown in Table 8.

Table 8: The parameters of the safety devices of a movable guard

Part No.	Part name	B10d [1,000 times]	MTTFd [year]	MTTFd value [year]	DCavg [%]	PFHd [/hour]
B1	Door switch	500	1,042	100	99	2.47×10^{-8}
B2	Door switch	500	1,042	100	99	2.47×10^{-8}
FS-PLC	FS-PLC	—	—	100	99	2.31×10^{-9}
K1	Contactor	2,000	4,167	100	99	2.47×10^{-8}
K2	Contactor	2,000	4,167	100	99	2.47×10^{-8}

$$B1/B2/K1/K2: n_{op}=1[\text{cycle/h}] \times 16[\text{h/d}] \times 300[\text{d/y}] = 4,800[\text{cycle/y}]$$

7.4.7 Safety block diagram

The safety block diagram of a movable guard is as shown in Fig. 17.

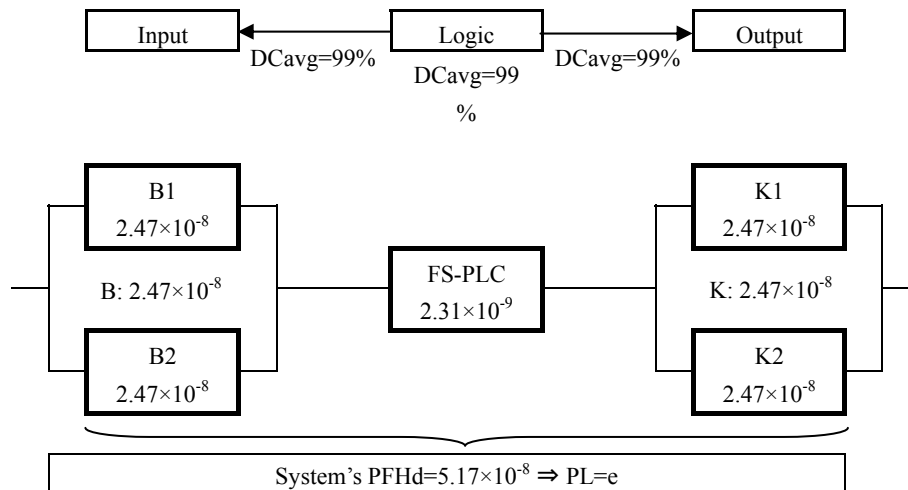


Fig. 17: The safety block diagram of a movable guard

7.5 Machine start-up/stop in locking type guard: locking-type interlock

7.5.1 Image of machinery and equipment

An installation example of a locking-type interlock with a safety switch and with a locking mechanism mounted on the door of the guarded area is shown in Fig. 18.

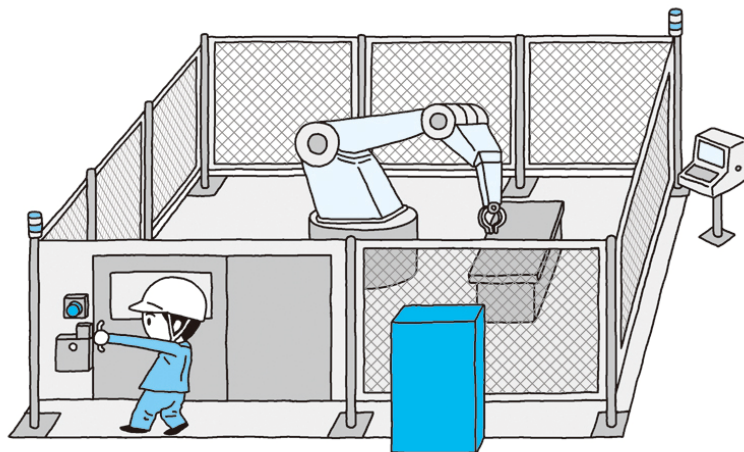


Fig. 18: Installation example of a locking-type interlock

* Prepared with reference to the illustration in p. 29 of the “Safety Guidebook,” Nippon Electric Control Equipment Industries Association (NECA), 2004 (3rd edition)

7.5.2 Function

A spring lock type safety switch mounted on the door of the safety fence ensures that the door will not open until the robot is powered off. The spring lock type safety switch is usually locked by the force of the spring, but when an electric current is applied to the solenoid, the lock is unlocked to enable the door to be opened.

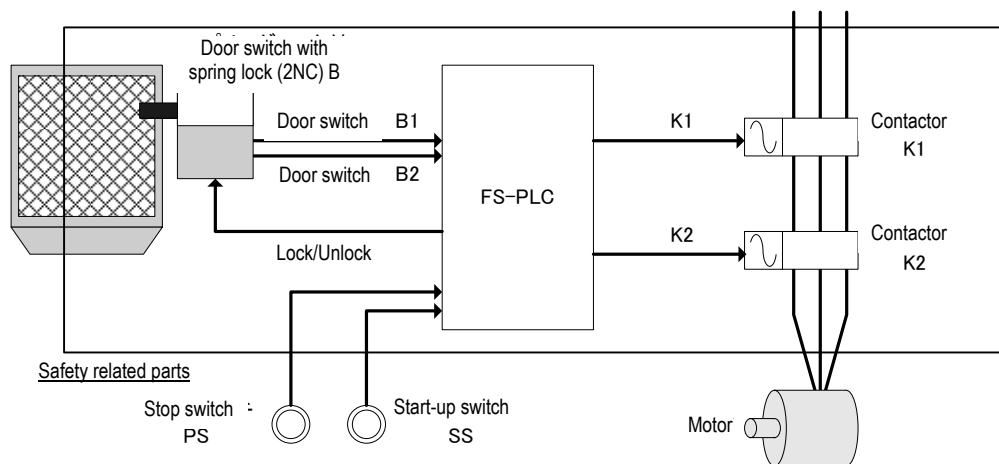
- The door open state refers to the state where the door is open (door switches B1, B2=OFF), the lock is unlocked (L=ON) and the machine is stopped (K1, K2=OFF).
- When the door is closed (B1, B2=ON), the state will be that the door is closed and the lock is unlocked (L=ON), but the machine remains stopped.
- Pushing the start-up switch in the door-closed and lock-unlocked state (SS=ON), it will be possible to lock the lock (L=OFF) and start up the machine.
- The machine is in operation only in the door closed and locked state. The machine is stopped (K1, K2=OFF) by the stop switch (PS=ON), and the lock is unlocked (L=ON).
- If the door is forcibly opened while the machine is in operation (B1, B2=OFF), the door will be in the open state, and the machine will be stopped (K1, K2=OFF) and the lock unlocked. (L=ON)

Table 9: State transition table

State	Event (change)	Action	Next state
(1) Door open Door open (B1, B2=OFF) Lock=Unlocked (L=ON) Machine=Stopped (K1, K2=OFF)	Door closed (B1, B2=ON)	None	(2) Door closed and lock unlocked
(2) Door closed and lock unlocked Door closed (B1, B2=ON) Lock=Unlocked (L=ON) Machine=Stop (K1, K2=OFF)	Door open (B1, B2=OFF)	None	(1) Door open
	Start-up switch (SS=ON)	Contactors K1, K2=ON Lock L=OFF	(3) In operation
(3) In operation Door closed (B1, B2=ON) Lock=Locked (L=OFF) Machine=Operating (K1, K2=ON)	Stop switch (PS=ON)	Contactors K1, K2=OFF Unlock L=ON	(2) Door closed and lock unlocked
	Door open (B1, B2=OFF)	Contactors K1, K2=OFF Unlock L=ON	(1) Door open

7.5.3 Circuit configuration

The circuit configuration of a locking-type interlock is as shown in Fig. 19.



* Separately, an EDM monitoring circuit which inputs the contactor b-contact into the FS-PLC is necessary to.

Fig. 19: The circuit configuration of a locking-type interlock

7.5.4 Timing chart

The timing chart for a locking-type interlock is as shown in Fig. 20.

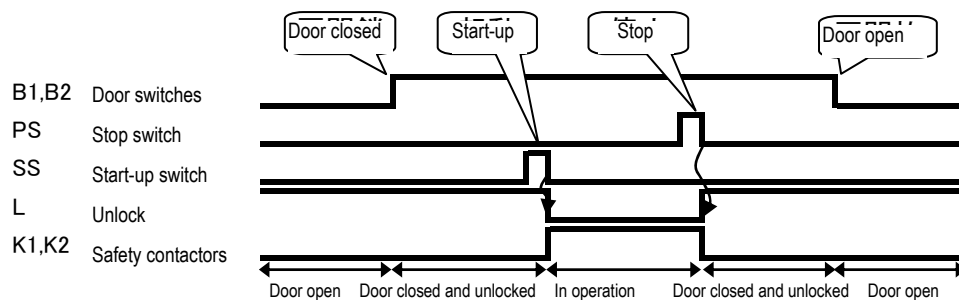


Fig. 20: The timing chart for a locking-type interlock

7.5.5 Parameters of safety devices

The parameters of the safety devices of a locking type interlock are as shown in Table 10.

Table 10: The parameters of the safety devices of a locking type interlock

Part No.	Part name	B10d [1,000 times]	MTTFd [year]	MTTFd value [year]	DCavg [%]	PFHd [hour]
B	Door switch with spring lock	500	1,042	100	99	2.47×10^{-8}
FS-PLC	FS-PLC	—	—	100	99	2.31×10^{-9}
K1	Contactor	2,000	4,167	100	99	2.47×10^{-8}
K2	Contactor	2,000	4,167	100	99	2.47×10^{-8}

$$B/K1/K2: n_{op}=1[\text{cycle/h}] \times 16[\text{h/d}] \times 300[\text{d/y}] = 4,800[\text{cycle/y}]$$

7.5.6 Safety block diagram

The safety block diagram of a locking-type interlock is as shown in Fig. 21.

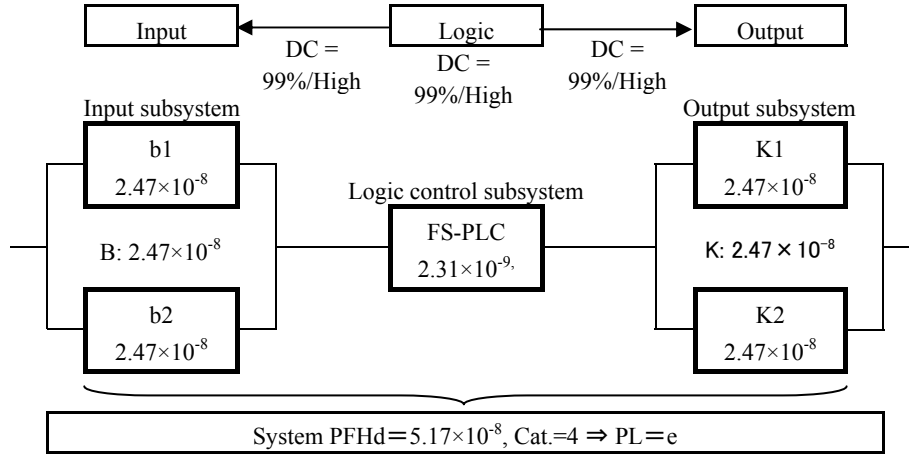


Fig. 21: The safety block diagram of a locking-type interlock

7.6 Start-up of press: Two-hand control switches

7.6.1 Image of machinery and equipment

This is a protective device to check action commands by two-hand control switches as a mechanism to prevent accidents involving hands touching active hazard sources, such as press machine dies.

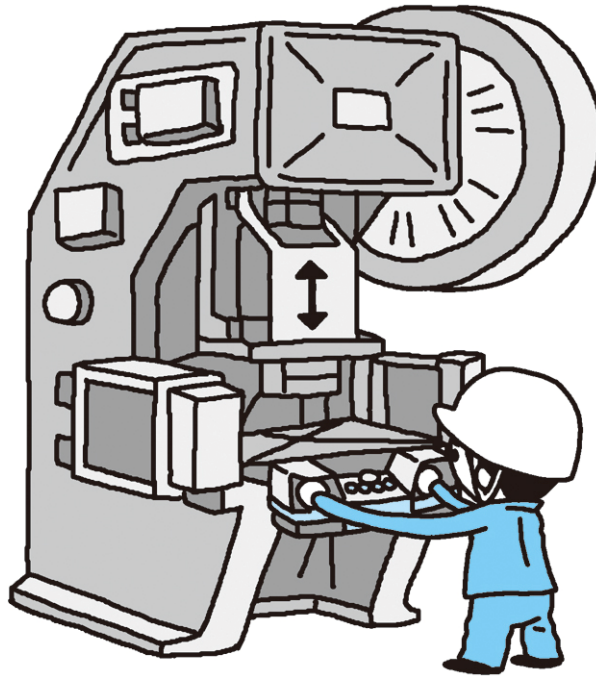


Fig. 22: Example installation of two-hand control switches

7.6.2 Function

Only the simultaneous operation (within 500ms) of the two-hand control switches (B1, B2) can start up the machine (contactors K1, K2=ON). The operation of only B1 or B2, or the simultaneous operation over 500ms cannot start up the machine. The two-hand control switches are composed of two switches featuring a combination of NC and NO types, and the FS-PLC evaluates the failure in the state and contact of the two switches, based on their state and push-down time difference.

- “After release of the operation of two-hand control switches B1, B2” means the state in which both of the two-hand control switches B1 and B2 are not pushed down (B11/B12, B21/B22=OFF) and the machine is at a stop (K1, K2=OFF).
- “Before release of the operation of two-hand control switches B1, B2” means the state where at least either one of the two-hand control switch B1 and B2 is pushed down (B11/B21=ON or B21/B22=ON) and that the machine is at a stop because the start-up conditions of the machine are not satisfied (K1, K2=OFF).
- “Motor in operation” means the state where the machine is started up and running (K1, K2=ON) by the simultaneous operation of the two-hand control switches B1, B2 (B11/B12=ON and B21/B22=ON, push-down time difference within 500ms).
- The machine will not be started up by the simultaneous operation of the two-hand control switches B1,

B2 (B11/B12=ON and B21/B22=ON, push-down time difference over 500ms).

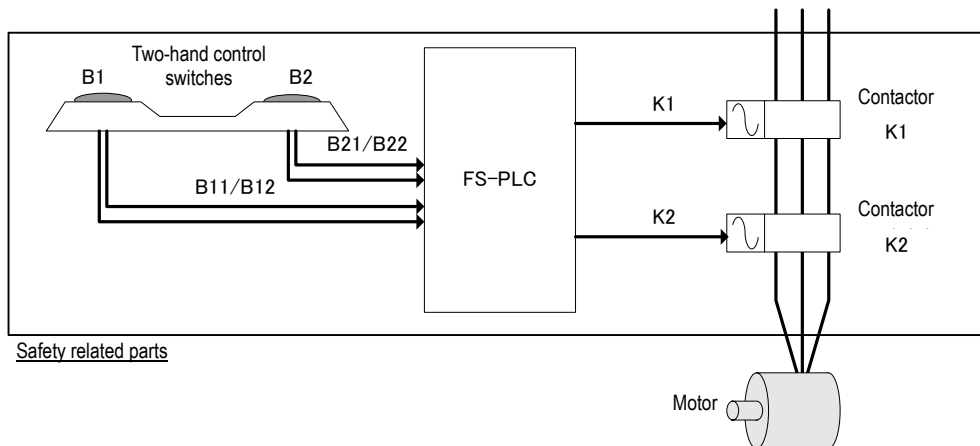
Note: The two-hand control switches covered by this document are of the Type IIIC specified in ISO 13851 (JIS B 9712).

Table 11: State transition table

State	Event (change)	Action	Next state
(1) After release of the operation of two-hand control switches B1, B2 (B11/B12, B21/B22=OFF) Machine=Stop (K1, K2=OFF)	Two-hand control switches B1, B2 pushed down (Push-down time difference within 500ms) (B11/B12=ON and B21/B22=ON)	Contactors K1, K2=ON	(3) Motor in operation
	Two-hand control switches B1, B2 pushed down (Push-down time difference over 500ms)	None	(2) Before release of the operation of two-hand control switches B1, B2
(2) Before release of the operation of two-hand control switches B1, B2 (At least either of B11/B21=ON or B21/B22=ON is realized) Machine =Stop (K1, K2=OFF)	Operation of two-hand control switches B1, B2 released (B11/B12=OFF and B21/B22=OFF)	None	(1) After release of the operation of two-hand control switches B1, B2
(3) Motor in operation Before release of the operation of two-hand control switches B1, B2 (B11/B12=ON, B21/B22 = ON, Push-down time difference within 500ms) Machine=Start-up (K1, K2=ON)	Operation of two-hand control switches B1, B2 released (B11/B21=OFF, B21/B22=OFF)	Contactors K1, K2=OFF	(1) After release of the operation of two-hand control switches B1, B2
	Operation of either of two-hand operation switch B1 or B2 released	Contactors K1, K2=OFF	(2) Before release of the operation of two-hand control switches B1, B2

7.6.3 Circuit configuration

The circuit configuration of two-hand control switches is as shown in Fig. 23.



* Separately, an EDM monitoring circuit is necessary to input the contactor b-contact into the FS-PLC.

Fig. 23: The circuit configuration of two-hand control switches

7.6.4 Timing chart

The timing chart for operating switches is as shown in Fig. 24.

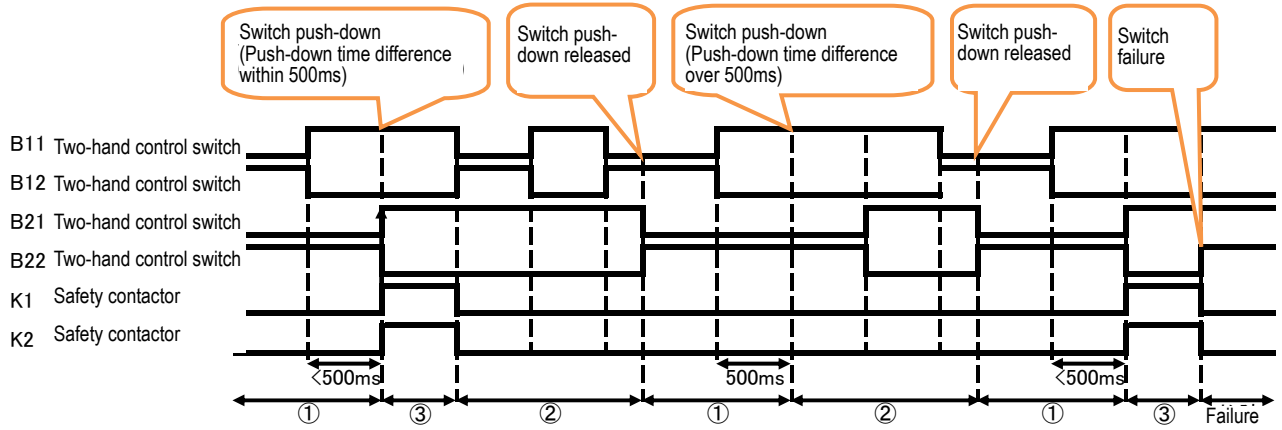


Fig. 24: The timing chart for two-hand control switches

7.6.5 Parameters of safety devices

A usage list of the safety devices of two-hand control switches is as shown in Table 12.

Table 12: Usage list of the safety devices of two-hand control switches

Part No.	Part name	B10d [1,000 times]	MTTFd [year]	MTTFd value [year]	DCavg [%]	PFHd [hour]
B1	Two-hand control switch	1,000	104	100	99	2.47×10^{-8}
B2	Two-hand control switch	1,000	104	100	99	2.47×10^{-8}
FS-PLC	FS-PLC	—	—	100	99	2.31×10^{-9}
K1	Contactor	2,000	208	100	99	2.47×10^{-8}
K2	Contactor	2,000	208	100	99	2.47×10^{-8}

$$B1/B2/K1/K2: n_{op}=20[\text{cycle/h}] \times 16[\text{h/d}] \times 300[\text{d/y}] = 96,000[\text{cycle/y}]$$

7.6.6 Safety block diagram

The safety block diagram of two-hand control switches is as shown in Fig. 25.

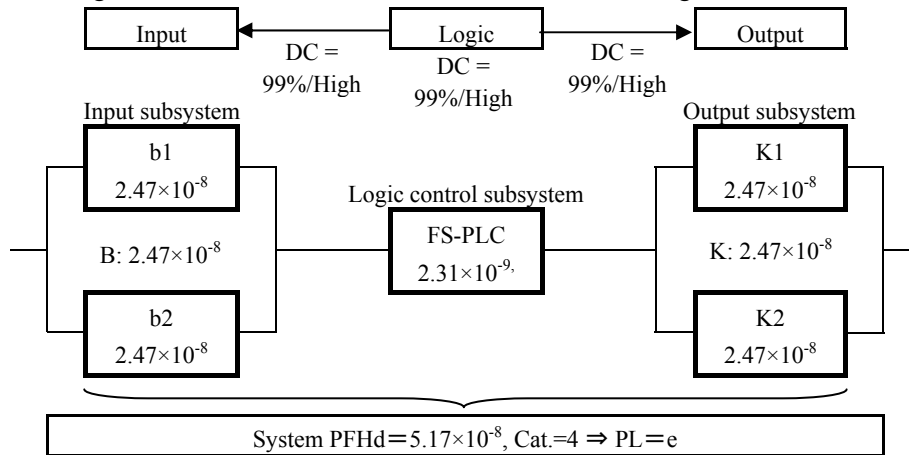


Fig. 25: The safety block diagram of two-hand control switches

7.7 Pendant-based robot teaching: 3-position enabling switch

7.7.1 Examples of use in machinery and equipment

An example of teaching using a pendant with a 3-position enabling switch is shown below. Based on the risk assessment considering the use of a 3-position enabling switch, etc., PL_r=d with structure category 3 is employed.



Fig. 26: An example of installing a pendant (3-position enabling switch)

* Prepared with reference to the illustration in p. 53 of the “Safety Guidebook,” Nippon Electric Control Equipment Industries Association (NECA), 2007 (5th edition)

As long as the 3-position enabling switch is pushed and held to the prescribed position, the manual operation of machine and robot will be permitted. During manual operation, regardless of whether a worker releases his/her hand from, or firmly grips, the 3-position enabling switch in response to an unexpected action of the machine, the 3-position enabling switch will shut off the circuit and stop the machine and robot.

The operational requirements for the 3-position enabling switch, as defined in IEC 60204-1:2005 (JIS B 9960-1:2008) and IEC 60947-5-8:2006, are as follows:

- To define the state of being not pushed as position 1, and turn off the switch.
- To define the state of being pushed to the intermediate position (a center enabled position) as position 2, and turn on the switch. (Permit of machine operation)
- To define the state of being pushed past the intermediate position as position 3, and turn off the switch.
- If the pendant is returned from position 3 to position 1, the switch must not be turned on at position 2 on the way.

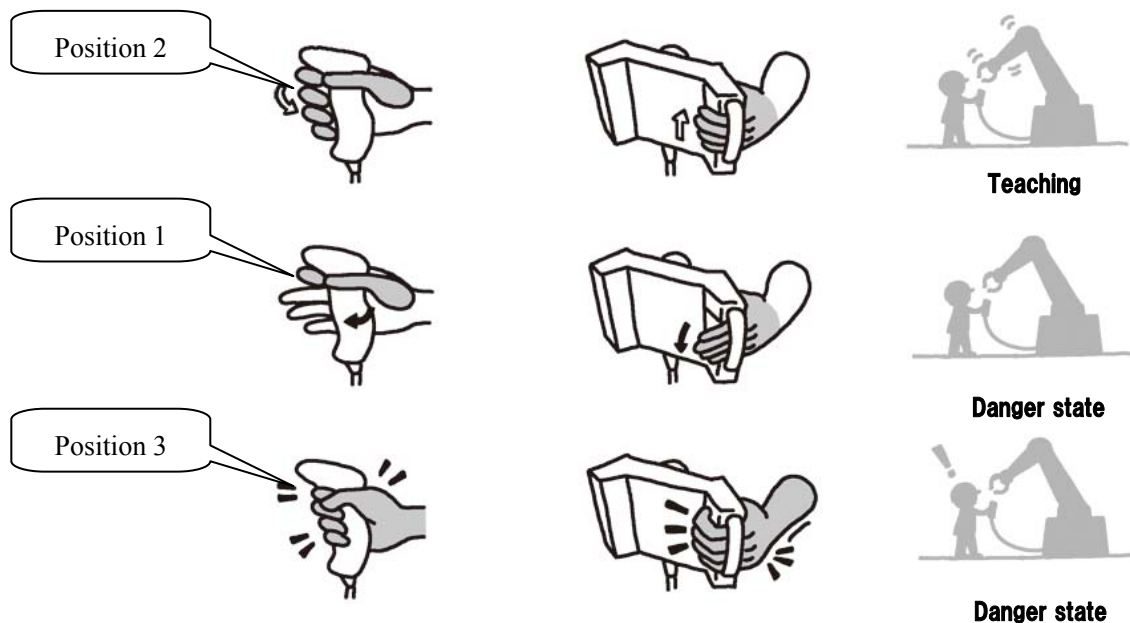


Fig. 27: Operation of a pendant (3-position enabling switch)

* Prepared with reference to the illustration in p. 54 of the “Safety Guidebook,” Nippon Electric Control Equipment Industries Association (NECA), 2007 (5th edition)

A 3-position enabling switch with a forced opening mechanism shall be used.

7.7.2 Function

The start-up and stop of the robot are controlled by contactor switching on/off the power source of the robot subject to manual operation.

3-position enabling switches and contactors are connected with the FS-PLC.

The FS-PLC controls the ON/OFF of contactors by program.

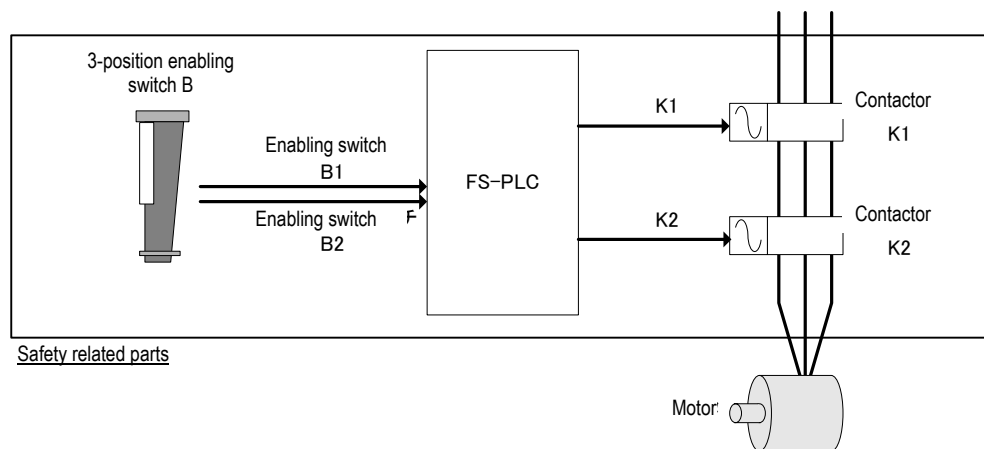
If the FS-PLC detects any error via self-diagnosis, the contactor will go off, without using the program. The contactor remains off until it is reset.

- When the 3-position enabling switch is slightly pushed down (position 2: ON), the contactor or power source of the machine is turned on. However, the operation of the machine is limited (Teaching mode).
- Where the 3-position enabling switch is not gripped (position 1: OFF), the FS-PLC will turn off the contactor to shut off the power source of the machine. This ensures the safety of the worker.
- If the 3-position enabling switch is gripped firmly (position 3: OFF), the FS-PLC will switch off the contactor to shut off the power source of the machine. This ensures the safety of the worker.

Table 13: State transition table

State	Event (change)	Action	Next state
(1) Position 1 or 3 (B1, B2=OFF) Machine = Stop (K1, K2=OFF)	Position 1->2 (Grip lightly) (B1, B2=ON)	Contactors K1, K2=ON	(2) Position 2
	Position 3->1 (Release hand) (Remain at B1, B2=OFF)	None	(1) Position 1
	Switch failure (B1=ON, B2=OFF or B1=OFF, B2=ON)	None	(3) Switch failure
(2) Position 2 (B1, B2=ON) Machine =Operation (K1, K2=ON)	Position 2->1 (Release hand) (B1, B2=OFF)	Contactors K1, K2=OFF	(1) Position 1
	Position 2->3 (Grip firmly) (B1, B2=OFF)	Contactors K1, K2=OFF	(1) Position 3
	Switch failure (B1=ON, B2=OFF or B1=OFF, B2=ON)	Contactors K1, K2=OFF	(3) Switch failure
(3) Switch failure Machine=Stop (K1, K2=OFF)	None	—	—

7.7.3 Circuit configuration



* Eparately, an EDM monitoring circuit is necessary to input the contactor b-contact into the FS-PLC.

Fig. 28: The circuit configuration of the pendant (3-position enabling switch)

7.7.4 Timing chart

The timing chart for the pendant (3-position enabling switch) is as shown in Fig. 29.

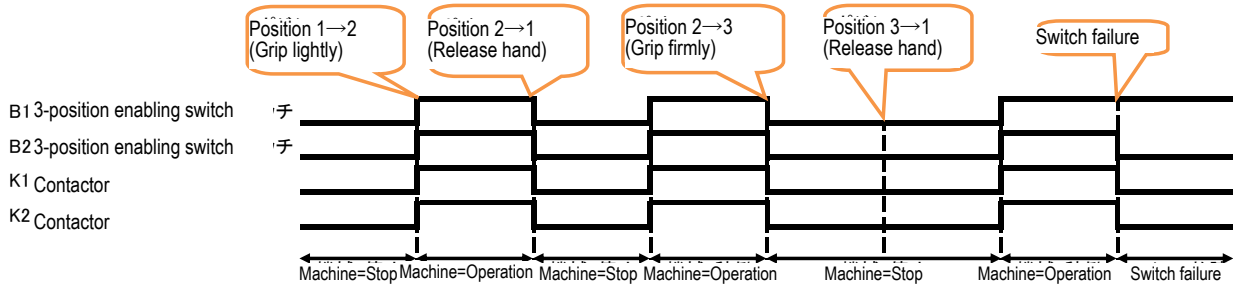


Fig. 29: The timing chart for the pendants (3-position enabling switches)

7.7.5 Parameters of safety devices

The parameters of the safety devices of a pendant (3-position enabling switch) are as shown in Table 14.

Table 14: The parameters of the safety devices of a pendant (3-position enabling switch)

Part No.	Part name	B10d [1,000 times]	MTTFd [year]	MTTFd value [year]	DCavg [%]	PFHd [/hour]
B	Pendant (3-position enabling switch)	100	333	100	99	2.47×10^{-8}
FS-PLC	FS-PLC	-	-	100	99	2.31×10^{-9}
K1	Contactor	2,000	4,167	100	99	2.47×10^{-8}
K2	Contactor	2,000	4,167	100	99	2.47×10^{-8}

$$B: n_{op}=10[\text{cycle/d}] \times 300[\text{d/y}] = 3,000[\text{cycle/y}]$$

$$K1/K2: n_{op}=1[\text{cycle/h}] \times 16[\text{h/d}] \times 300[\text{d/y}] = 4,800[\text{cycle/y}]$$

7.7.6 Safety block diagram

The safety block diagram of the pendant (3-position enabling switch) is as shown in Fig. 30.

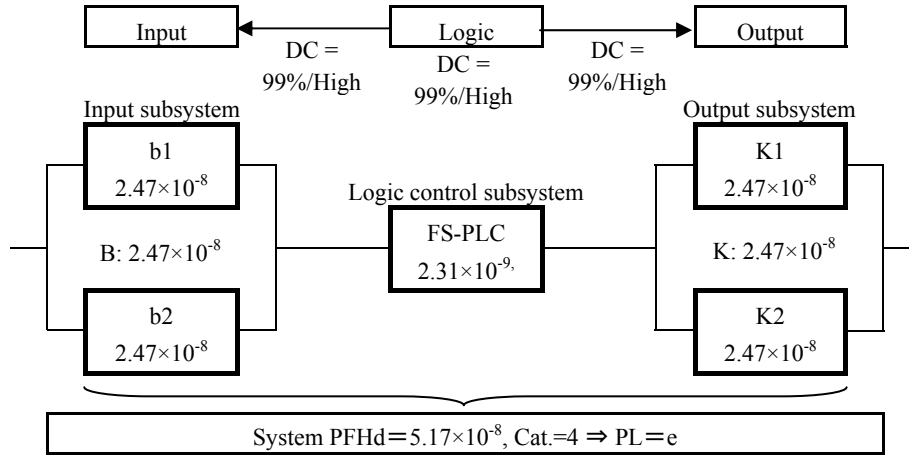


Fig. 30: The safety block diagram of the pendant (3-position enabling switch)

7.8 Automatic/teaching mode selection for industrial robot application: Mode selector switch

7.8.1 Overview of machinery and equipment

An example of teaching operation for industrial robots utilizing a teaching pendant with a mode selector switch and a 3-position enabling switch is shown below. PLr = d is adopted, based on the risk assessment considering the use of a 3-position enabling switch.

In this guideline, the mode selector switch is not included in the safety related system, but the failure of the switch can be detected by the FS-PLC.

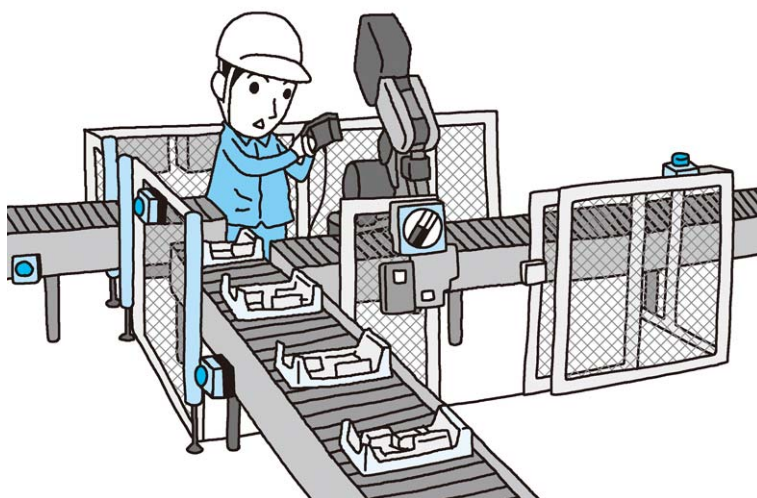


Fig. 31: Application sample of the mode selector switch for the industrial robots



* Prepared with reference to the illustration in p. 53 of the “Safety Guidebook,” Nippon Electric Control Equipment Industries Association (NECA), 2007 (5th edition)

7.8.2 Function

The FS-PLC controls the contactor, judging 1) teaching mode, 2) auto mode, or 3) mode selector failure from the output signal of the mode selector.

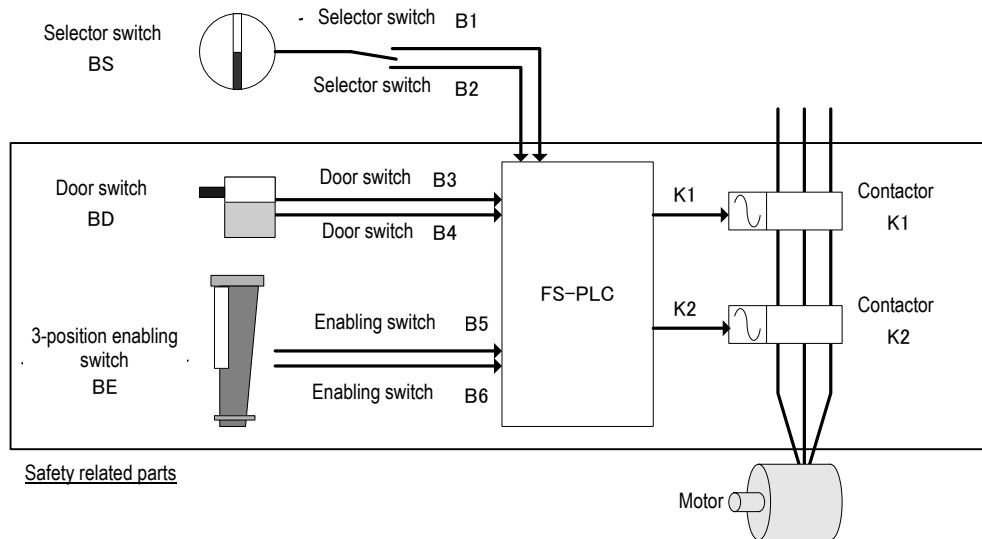
- (1) In the teaching mode, the manual operation of a machine or robot is permitted only when the operation button of the 3-position enabling switch is lightly pressed and held to the specified position.
- (2) In automatic mode, the operation of a machine or robot is permitted while the door is closed. While, the 3-position enabling switch is invalid.
- (3) Mode selector failure is the situation which neither teaching nor automatic mode is set, or which both teaching and automatic modes are set. When the mode selector switch is failed, contactors should be turned OFF.

Table 15: State transition table

State	Event (change)	Action	Next state
(1) Teaching mode  (B1=ON, B2=OFF) Machine=Operation(K1, K2=ON)	Teaching mode -> Auto mode (B1=OFF, B2=ON)	3-position enabling switch invalid Door switch valid	(2) Auto mode
	Teaching mode -> Mode selector failure (B1, B2=ON or B1, B2=OFF)	Contactors K1, K2=OFF 3-position enabling switch invalid	(3) Mode selector failure
(2) Auto mode  (B1=OFF, B2=ON) Machine=Operation(K1, K2=ON)	Auto mode -> Teaching mode (B1=ON, B2=OFF)	3-position enabling switch valid Door switch invalid	(1) Teaching mode
	Auto mode -> Mode selector failure (B1, B2=ON or B1, B2=OFF)	Contactors K1, K2=OFF 3-position enabling switch invalid	(3) Mode selector failure
(3) Mode selector failure (B1, B2=ON or B1, B2=OFF) Machine=Stop(K1, K2=OFF)	None	-	-

7.8.3 Circuit configuration

The circuit configuration of the mode selector is as shown in Fig. 32.

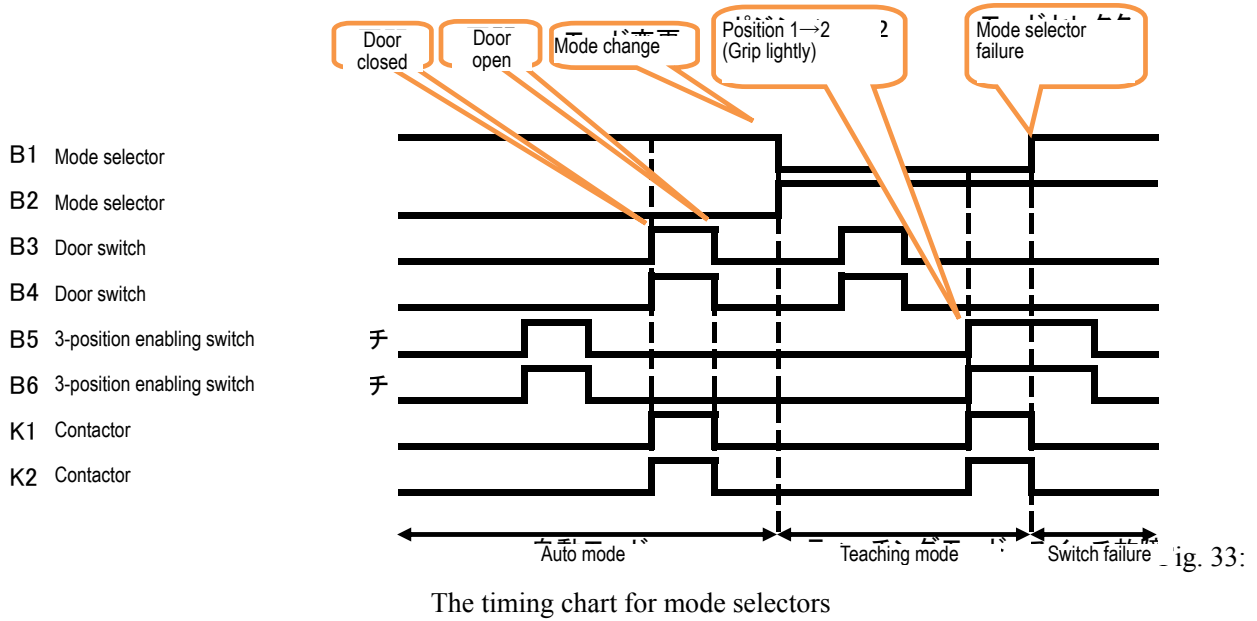


* Separately, an EDM monitoring circuit is necessary to input the contactor b-contact into the FS-PLC.

Fig. 32: The circuit configuration of a mode selector

7.8.4 Timing chart

The timing chart for mode selectors is as shown in Fig. 33.



The timing chart for mode selectors

7.8.5 Parameters of safety devices

The parameters of the safety devices of the mode selector are as shown in Table 16.

Table 16: The parameters of the safety devices of the mode selector

Part No.	Part name	B10d [1,000 times]	MTTFd [year]	MTTFd value [year]	DCavg [%]	PFHd [hour]
BD	Door switch	500	3,333	100	99	2.47×10^{-8}
BE	Pendant (3-position enabling switch)	100	333	100	99	2.47×10^{-8}
FS-PLC	FS-PLC	-	-	100	99	2.31×10^{-9}
K1	Contactor	2,000	4,167	100	99	2.47×10^{-8}
K2	Contactor	2,000	4,167	100	99	2.47×10^{-8}

$$\text{BD: } n_{\text{op}} = 5[\text{cycle/d}] \times 300[\text{d/y}] = 1,500[\text{cycle/y}]$$

$$\text{BE: } n_{\text{op}} = 10[\text{cycle/d}] \times 300[\text{d/y}] = 3,000[\text{cycle/y}]$$

$$\text{K1/K2: } n_{\text{op}} = 1[\text{cycle/h}] \times 16[\text{h/d}] \times 300[\text{d/y}] = 4,800[\text{cycle/y}]$$

7.8.6 Safety block diagram

a) Auto mode

The safety block diagram of the mode selector (auto mode) is as shown in Fig. 34.

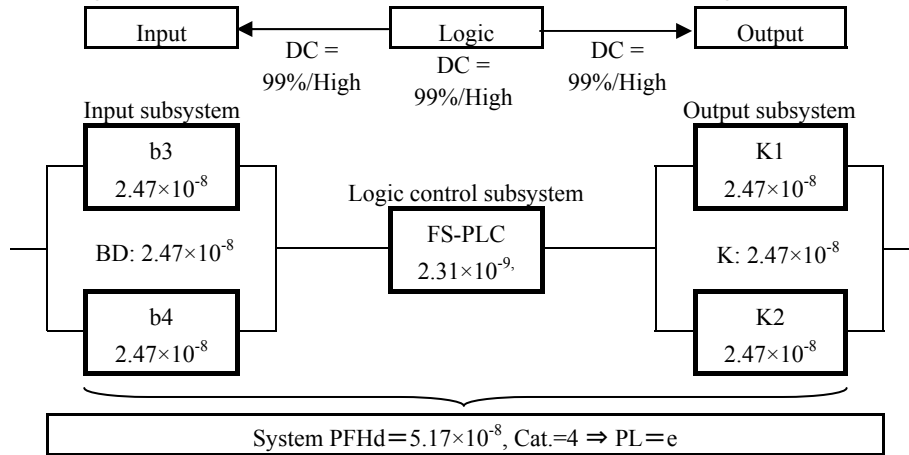


Fig. 34: The safety block diagram of the mode selector (auto mode)

b) Teaching mode

The safety block diagram of the mode selector (teaching mode) is as shown in Fig. 35.

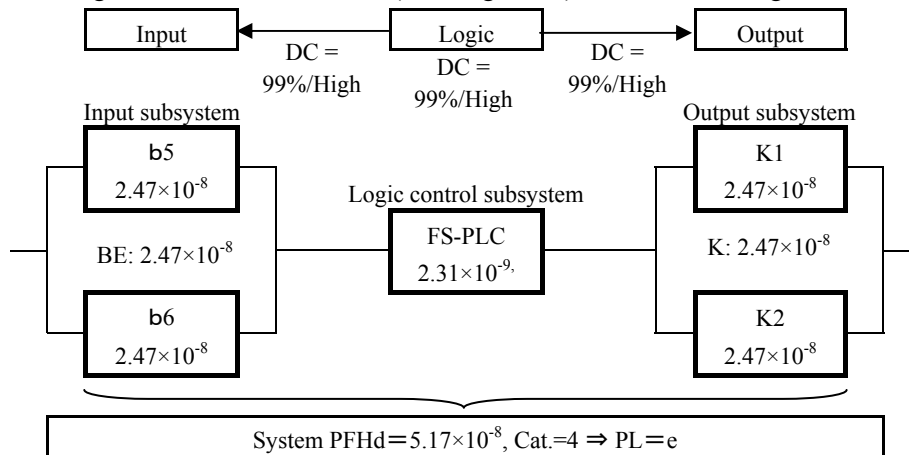


Fig. 35: The safety block diagram of the mode selector (teaching mode)

7.9 Intrusion detection by light curtain: Light curtain

7.9.1 Image of machinery and equipment

This is an application with a light curtain installed in the entrance area to bring the robot to an emergency stop when a worker enters the danger area for supply or taking out of materials while the robot is in operation (when the light curtain is intercepted).

Because of the possibility of contact between the working robot and the worker in the event of failure in the safety system, including the light curtain, PL_r=e is adopted as a result of risk assessment, considering possible serious injuries, etc.

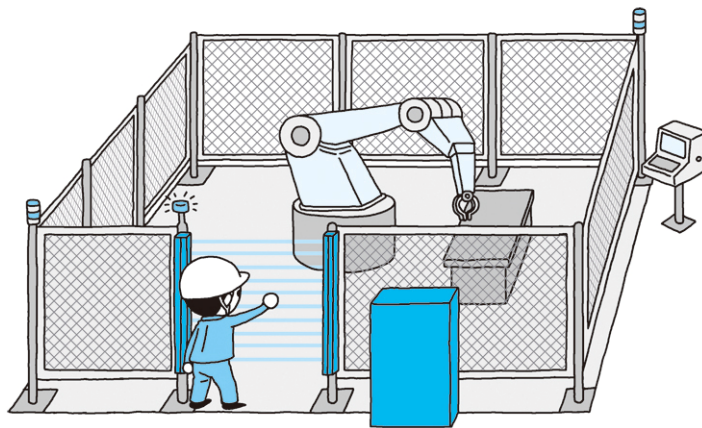


Fig. 36: Example installation of the light curtain type 4

* Prepared with reference to the illustration in p. 29 of the “Safety Guidebook,” Nippon Electric Control Equipment Industries Association (NECA), 2004 (3rd edition)

7.9.2 Function

In view of PL_r=e, a type-4 product certified under IEC 61496-2 shall be used for the light curtain (F1). The product certified under IEC 61496-2 has a self-diagnostic function, whose detection system is of the “transmission type”; turning on the output only when all the light axes are in the state of light entrance.

The light curtain (F1) and the contactors (K1, K2) controlling the output connect to the FS-PLC. The FS-PLC controls the ON/OFF of the contactors (K1, K2) by a program to stop the robot. The FS-PLC also turns off the output if it detects any anomaly by self-diagnosis, not by the program.

The program of the FS-PLC will realize the following functions:

- Where operation is ready, if the operation ready switch (RS) is pushed after light enters the light curtain (F1) (OSSD1 and OSSD2) are turned on, the output of the FS-PLC will be turned on to put the machine into operation.
- Where operation is ready, if the light curtain (F1) is intercepted and the input of OSSD1 or OSSD2 is turned off, the output of the FS-PLC will be turned off to apply an emergency stop to the machine.
- Where an emergency stop occurs, the output of the FS-PLC will remain OFF, even if the operation ready switch (RS) is pushed down.
- Where an emergency stop occurs, the machine will revert to an operationally ready state if the light

curtain (F1) is turned on (OSSD1, OSSD2=ON),

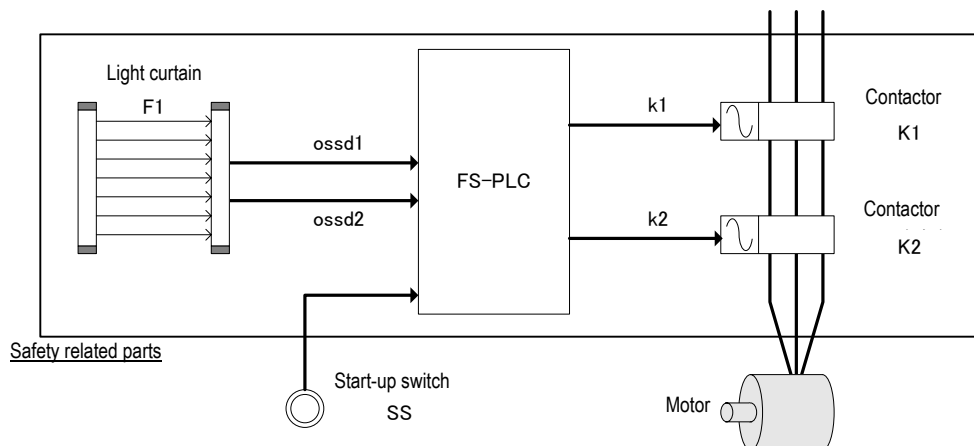
- To prevent any accidental start-up due to failure of the operation ready switch (RS), the ON→OFF falling shall be a condition for the reset of the operation ready switch (RS).
- When turning on the power, the output of the FS-PLC will remain OFF, even if the output of the light curtain (F1) is turned on (Start-up interlock).
- The output of the FS-PLC will remain OFF, even if light enters the light curtain (F1) after the output of the FS-PLC is turned off (Restart interlock).

Table 17: State transition table

State	Event (change)	Action	Next state
(1) Operation ready Motor stop (K1, K2=OFF) Light curtain (F1) Entrance of light (OSSD1, OSSD2=ON)	Operation ready switch (RS) Pushed down (RS=ON)	Contactors K1, K2=ON Motor action	(2) In operation
(2) In operation Motor action (K1, K2=ON) Light curtain (F1) Entrance of light (OSSD1, OSSD2=ON)	Light curtain (F1) Intercepted (OSSD1 or OSSD2=OFF)	Contactors K1, K2=OFF Motor stop	(1) Operation ready
(3) Emergency stop Motor stop (K1, K2=OFF)	Operation ready switch (RS) Pushed down (S1=ON)	-	(1) Operation ready
	Light curtain (F1) Entrance of light (OSSD1, OSSD2=ON)	-	(1) Operation ready

7.9.3 Circuit configuration

The circuit configuration of the light curtain type 4 is as shown in Fig. 37.



* Separately, an EDM monitoring circuit is necessary to input the contactor b-contact into the FS-PLC.

Fig. 37: The circuit configuration of the light curtain type 4

7.9.4 Timing chart

The timing chart for the light curtain type 4 is as shown in Fig. 38.

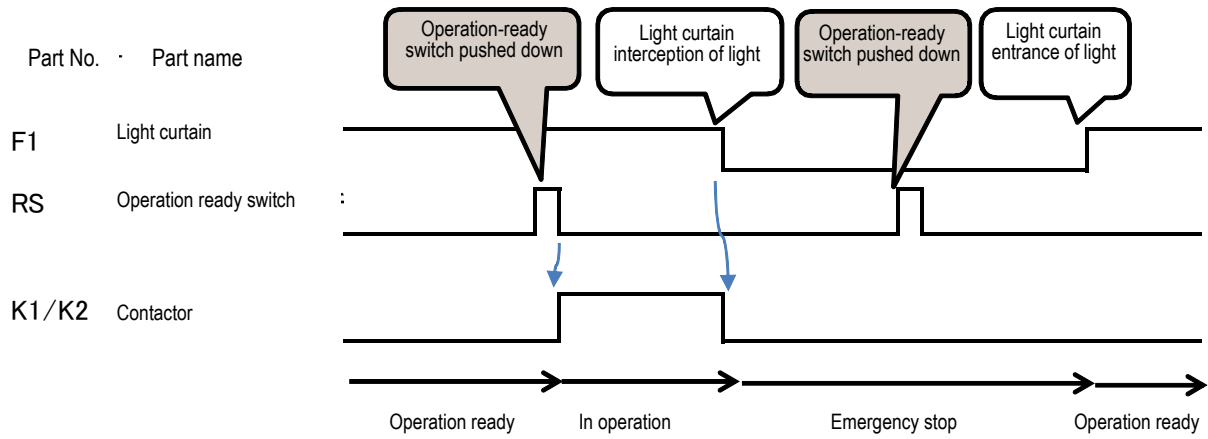


Fig. 38: The timing chart for the light curtain type 4

7.9.5 Parameters of safety devices

The parameters of the safety devices of the light curtain type 4 are as shown in Table 18.

Table 18: The parameters of the safety devices of the light curtain type 4

Part No.	Part name	B10d [1,000 times]	MTTFd [year]	MTTFd value [year]	DCavg [%]	PFHd [hour]
F1	Light curtain	—	—	100	99	2.47×10^{-8}
FS-PLC	FS-PLC	—	—	100	99	2.31×10^{-9}
K1	Contactor	2,000	4,167	100	99	2.47×10^{-8}
K2	Contactor	2,000	4,167	100	99	2.47×10^{-8}

$$K1/K2: n_{op}=1[\text{cycle/h}] \times 16[\text{h/d}] \times 300[\text{d/y}]=4,800[\text{cycle/y}]$$

7.9.6 Safety block diagram

The safety block diagram of the light curtain type 4 is as shown in Fig. 39.

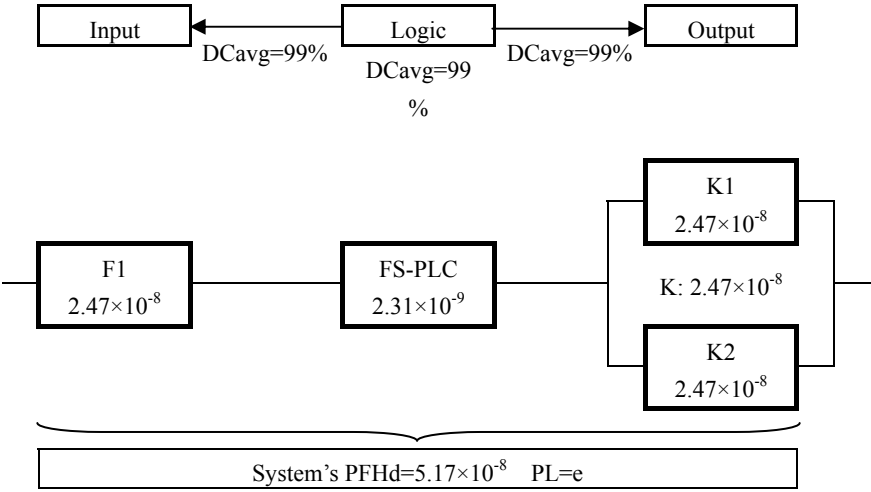


Fig. 39: The safety block diagram of the light curtain type 4

7.10 Detection of presence by laser scanner: Laser scanner

7.10.1 Image of machinery and equipment

This is an application to install a laser scanner in the robot operation area, detect the presence of any worker in the danger area while the robot is in operation, and stop (not start up) the robot.

When a worker is in the danger area, even when out of sight of other workers, he/she can be detected and protected from inadvertent start-up/restart.

In this example, the required performance level (PLr) is determined to be PLr=d as a result of risk assessment.

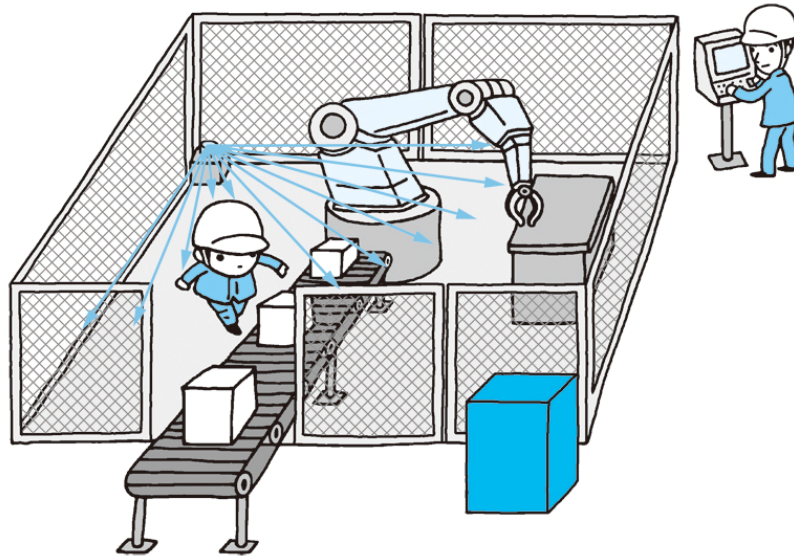


Fig. 40: Example installation of a laser scanner

* Prepared with reference to the illustration in p. 29 of the “Safety Guidebook,” Nippon Electric Control Equipment Industries Association (NECA), 2004 (3rd edition)

7.10.2 Function

The laser scanner (F1) monitors safety in the area by scanning a laser beam and monitoring the reflected beam (calculating the distance to a surrounding object using the time until the beam is reflected against the object and received). For the laser scanner (F1), a product certified under IEC 61496-3 shall be used. A product certified under IEC 61496-3 has a self-diagnostic function and turns on the output only when nothing is present in the specified area. A detection of failure by the self-diagnosis or a disturbance of the laser scanner (F1) by ambient light will turn off the output.

The laser scanner (F1) and the contactors (K1, K2) controlling the output connect to the FS-PLC.

The program of the FS-PLS will realize the following functions:

- Where operation is ready, if the operation ready switch (RS) is pushed after the output of the laser scanner (F1) (OSSD1 and OSSD2) are turned on, the output of the FS-PLC will be turned on to put the machine into operation.
- Where the machine is in operation, if the output of the laser scanner (F1) (OSSD1 or OSSD2) is turned off, the output of the FS-PLC will be turned off to apply an emergency stop to the machine.
- Where an emergency stop occurs, the output of the PLC will remain OFF, even if the operation ready

switch (RS) is pushed down.

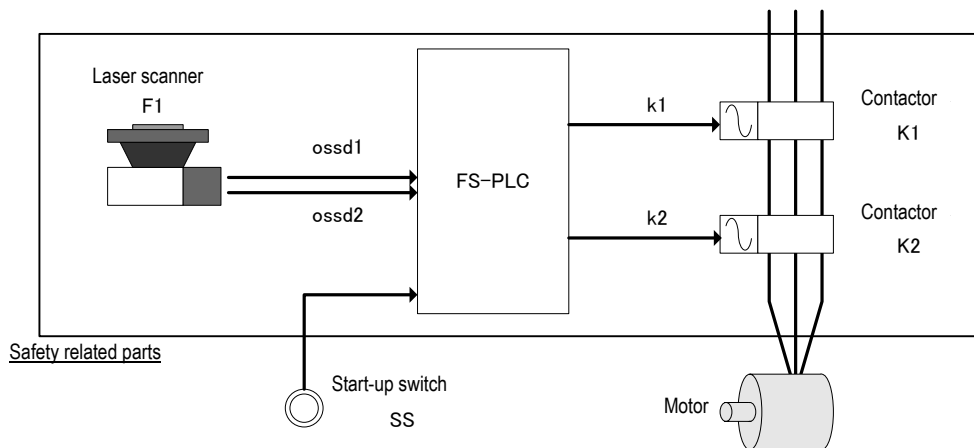
- Where an emergency stop occurs, the machine will revert to a state of operational readiness if the laser scanner (F1) is turned on (OSSD1, OSSD2=ON).
- To prevent any accidental start-up due to failure of the operation ready switch (RS), the reset of the operation ready switch (RS) shall be conditional on the ON→OFF falling.

Table 19: State transition table

State	Event (change)	Action	Next state
(1) Operation ready Motor stop (K1, K2=OFF) Laser scanner (F1) output ON (OSSD1, OSSD2=ON)	Operation ready switch (RS) pushed down (RS=ON)	Contactors K1, K2=ON Motor operation	(2) In operation
(2) In operation Motor operation (K1, K2=ON) Laser scanner (F1) output ON (OSSD1, OSSD2=ON)	Laser scanner (F1) output OFF (OSSD1 or OSSD2=OFF)	Contactors K1, K2=OFF Motor stop	(3) Emergency stop
(3) Emergency stop Motor stop (K1, K2=OFF)	Operation ready switch (RS) pushed down (RS=ON)	—	(3) Emergency stop
	Laser scanner switch (F1) output ON (OSSD1, OSSD2=ON)	—	(1) Operation ready

7.10.3 Circuit configuration

The circuit configuration of the laser scanner is as shown in Fig. 41.



* Separately, an EDM monitoring circuit is necessary to input the contactor b-contact into the FS-PLC.

Fig. 41: The circuit configuration of the laser scanner

7.10.4 Timing chart

The timing chart for the laser scanner is as shown in Fig. 42.

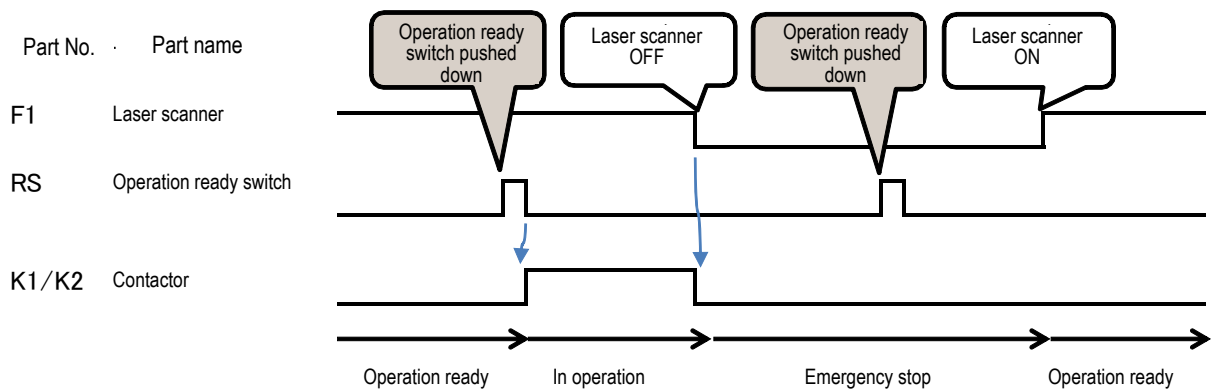


Fig. 42: The timing chart for the laser scanner

7.10.5 Parameters of safety devices

The parameters of the safety devices of the laser scanner are as shown in Table 20.

Table 20: The parameters of the safety devices of the laser scanner

Part No.	Part name	B10d [1,000 times]	MTTFd [year]	MTTFd value [year]	DCavg [%]	PFHd [/hour]
F1	Laser scanner	—	—	100	90	1.03×10^{-7}
FS-PLC	FS-PLC	—	—	100	99	2.31×10^{-9}
K1	Contactor	2,000	4,167	100	99	2.47×10^{-8}
K2	Contactor	2,000	4,167	100	99	2.47×10^{-8}

$$K1/K2: n_{op}=1[\text{cycle/h}] \times 16[\text{h/d}] \times 300[\text{d/y}] = 4,800[\text{cycle/y}]$$

7.10.6 Safety block diagram

The safety block diagram of the laser scanner is as shown in Fig. 43.

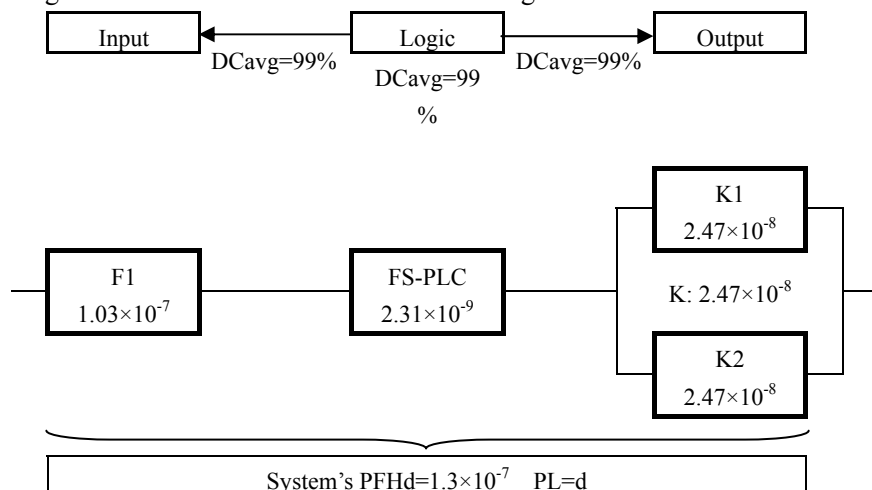


Fig. 43: The safety block diagram of the laser scanner

7.11 Muting function of the light curtain: Cross muting

7.11.1 Image of machinery and equipment

Muting is an application used to install a light curtain in the conveyor opening section, and shut off the robot power source if any worker enters the danger area (when the light curtain is intercepted), but continue operation without shutting off the robot power source if a workpiece traverses the light curtain.

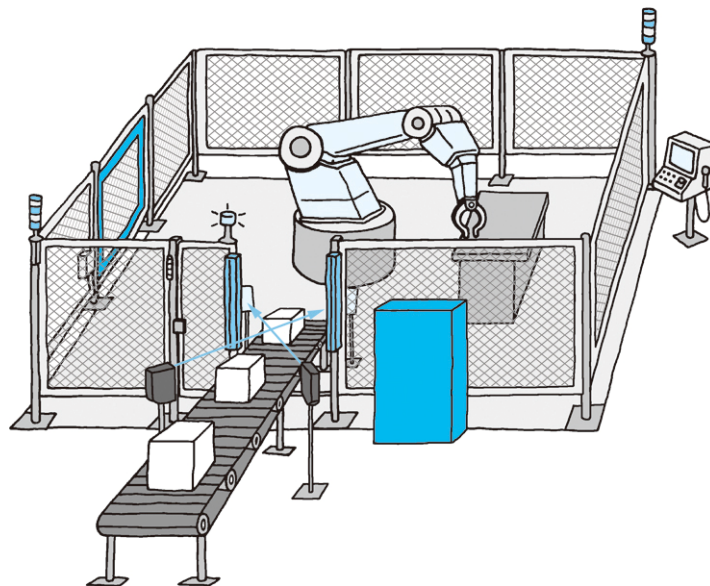


Fig. 44: Example installation of muting

* Prepared by reference to the illustration in p. 29 of the “Safety Guidebook,” Nippon Electric Control Equipment Industries Association (NECA), 2004 (3rd edition)

A muting sensor discriminates between a workpiece and the human body, and, if a workpiece is detected, disables the safety detection function of the light curtain. This means the muting sensor mounting position is important to discriminate properly between a workpiece and the human body. Measures must also be taken to prevent the entrance of any human body while muting.

When using two units of muting sensors as shown in Fig. 45, the crossing position of the light axes of muting sensors F2 and F3 is set in the area after traversing the light curtain (on the danger area side). Further, as the muting sensors are intercepted in order of F2 and F3 in a short time, it is possible to determine that the invading object is a workpiece.

The installation positions and detection directions of the muting sensors F2 and F3 shall be adjusted so that neither muting sensors F2 nor F3 may be intercepted simultaneously by the passage of a human body. This arrangement prevents the muting function being triggered by the passage of a person in the crossing position.

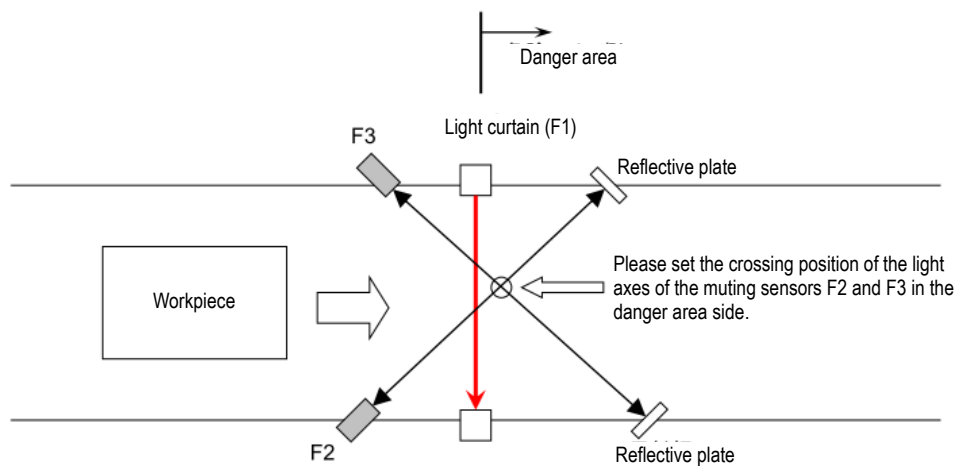


Fig. 45: Example installation of muting sensors

7.11.2 Function

The light curtain (F1), the contactors (K1, K2) controlling output, and the muting sensors (F2, F3) detecting workpieces are connected to the FS-PLC.

The FS-PLC controls the ON/OFF of the contactors (K1, K2) by program.

The program of the FS-PLC will realize the following functions:

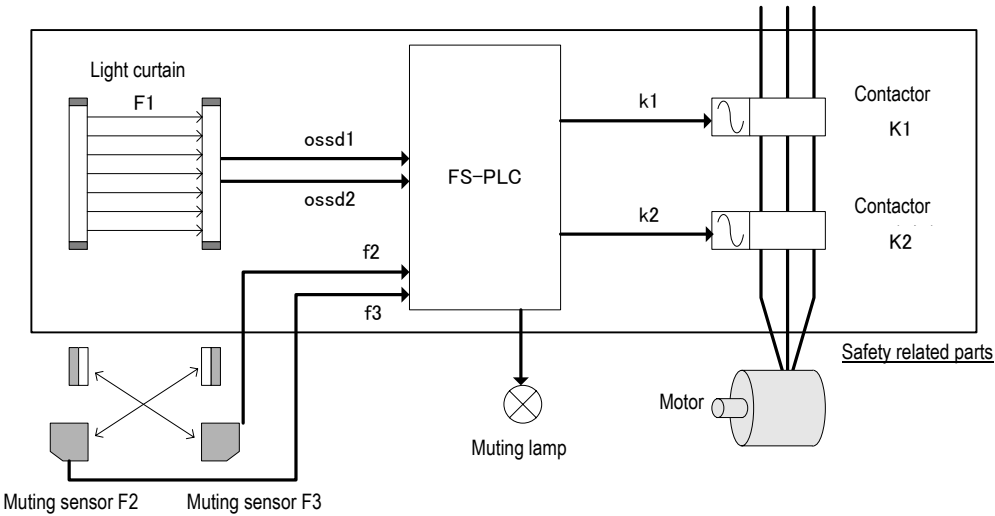
- While in operation, if the muting sensors (F2, F3) are turned on in the correct order and timing, the program will keep the FS-PLC output ON and the machine in operation even if the light curtain (F1) is intercepted (OSSD1, OSSD2=OFF). In this case, the program will determine that the light curtain is in muting mode, and turn on the muting lamp.
- While in operation, if the muting sensors (F2, F3) are turned on in the incorrect timing or sequence, the program will determine a synchronous failure or sequence failure, and turn off the output of the FS-PLC to bring the machine to an emergency stop. In this case, the muting lamp will be turned off.

Table 21: State transition table

State	Event (change)	Action	Next state
(1) In operation (without work piece) Light curtain Entrance of light (OSSD1, OSSD2=ON) Muting sensors F2, F3=OFF Contactors K1, K2=ON Muting lamp OFF	A work piece enters, and muting sensors and light curtain operate in correct timing. Muting sensors F2, F3=ON Light curtain Light intercepted (OSSD1, OSSD2=OFF)	Contactors K1, K2=ON Muting lamp ON	(2) In operation (In muting)
	Muting sensors and light curtain operate in incorrect timing. Muting sensors F2, F3=ON Light curtain Light intercepted (OSSD1, OSSD2=OFF)	Contactors K1, K2=OFF Muting lamp OFF	(3) Synchronous failure
	Muting sensors and light curtain operate in incorrect sequence. Muting sensors F2, F3=ON Light curtain Light intercepted (OSSD1, OSSD2=OFF)	Contactors K1, K2=OFF Muting lamp OFF	(4) Sequence failure
(2) In operation (In muting) Light curtain Light intercepted (OSSD1, OSSD2=OFF) Muting sensors F2, F3=ON Contactors K1, K2=ON Muting lamp ON	Work piece taken out, light entered light curtain, and muting sensors turned off. Light entered light curtain (OSSD1, OSSD2=ON) Muting sensors F2, F3=OFF	Contactors K1, K2=ON Muting lamp OFF	(1) In operation (without work piece)
(3) Synchronous failure Light curtain Light intercepted (OSSD1, OSSD2=OFF) Muting sensors F2, F3=ON Contactors K1, K2=OFF Muting lamp OFF	Power supply restarted	Contactors K1, K2=ON Muting lamp OFF	(1) In operation (without work piece)
(4) Sequence failure Light curtain Light intercepted (OSSD1, OSSD2=OFF) Muting sensors F2, F3=ON Contactors K1, K2=OFF Muting lamp OFF	Power supply restarted	Contactors K1, K2=ON Muting lamp OFF	(1) In operation (without work piece)

7.11.3 Circuit configuration

The circuit configuration for muting is as shown in Fig. 46.



* Separately, an EDM monitoring circuit is necessary to input the contactor b-contact into the FS-PLC.

Fig. 46: The circuit configuration for muting

7.11.4 Timing chart

a) Normal action

The timing chart in normal action is as shown in Fig. 47.

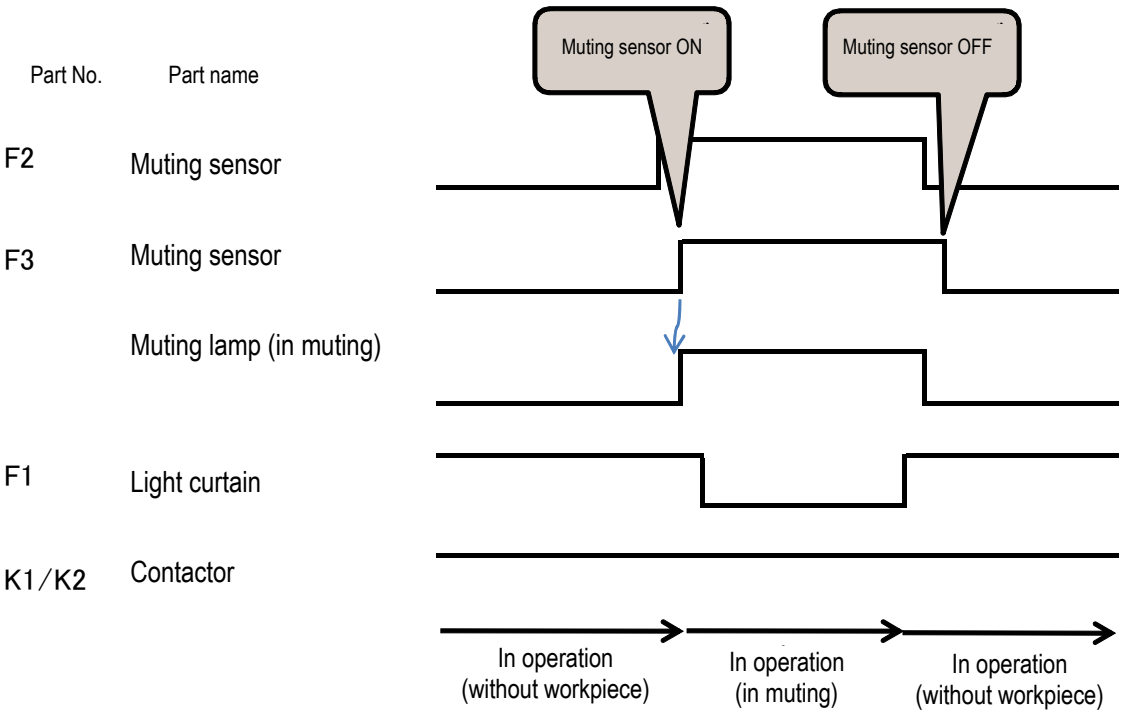


Fig. 47: The timing chart in normal action

b) Synchronous failure

The timing chart in synchronous failure is as shown in Fig. 48.

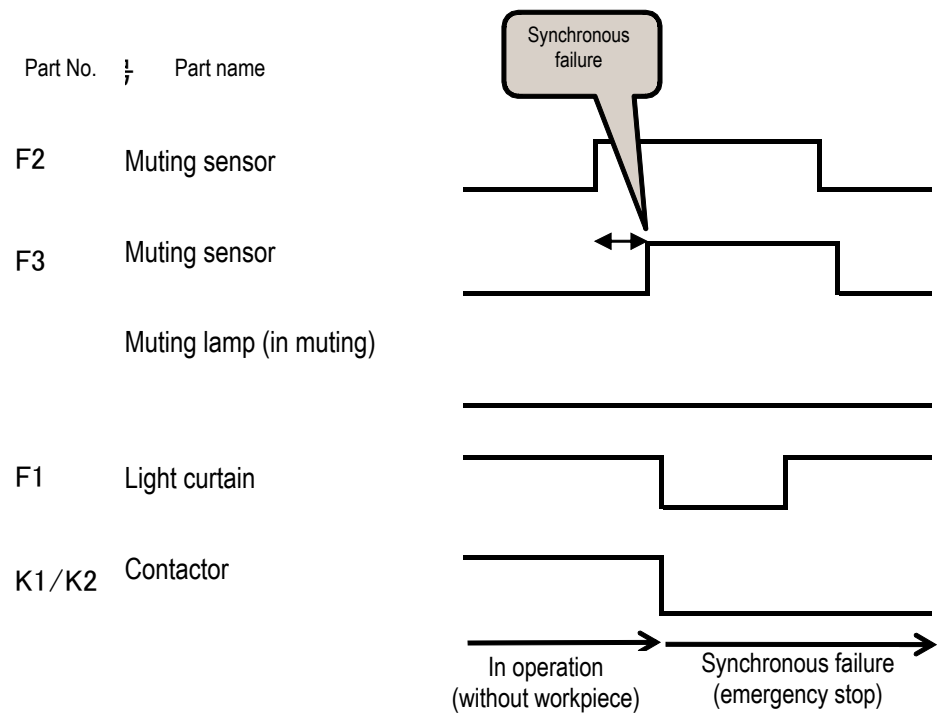


Fig. 48: The timing chart in synchronous failure

c) Sequence failure

The timing chart in sequence failure is as shown in Fig. 49.

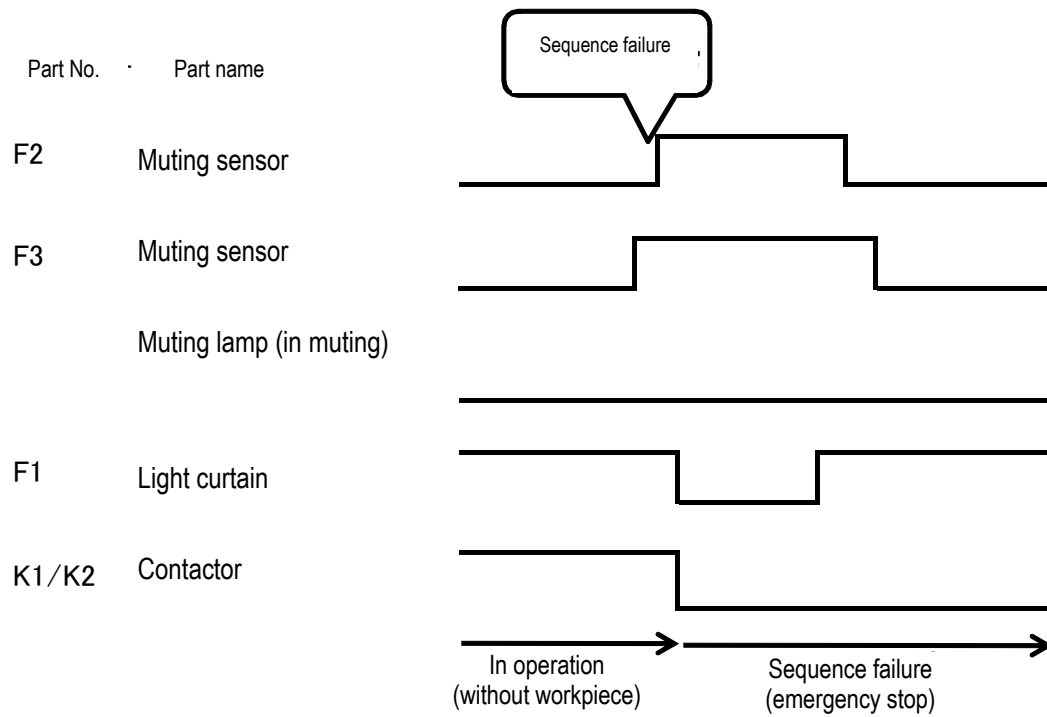


Fig. 49: The timing chart in sequence failure

7.11.5 Parameters of safety devices

Parameters of safety devices for muting are as shown in Table 22.

Table 22: Parameters of safety devices for muting

Part No.	Part name	B10d [1,000 times]	MTTFd [year]	MTTFd value [year]	DCavg [%]	PFHd [/hour]
F1	Light curtain	—	—	100	99	2.47×10^{-8}
FS-PLC	FS-PLC	—	—	100	99	2.31×10^{-9}
K1	Contactor	2,000	4,167	100	99	2.47×10^{-8}
K2	Contactor	2,000	4,167	100	99	2.47×10^{-8}

$$K1/K2: n_{op}=1[\text{cycle/h}] \times 16[\text{h/d}] \times 300[\text{d/y}] = 4,800[\text{cycle/y}]$$

7.11.6 Safety block diagram

The safety block diagram for muting is as shown in Fig. 50.

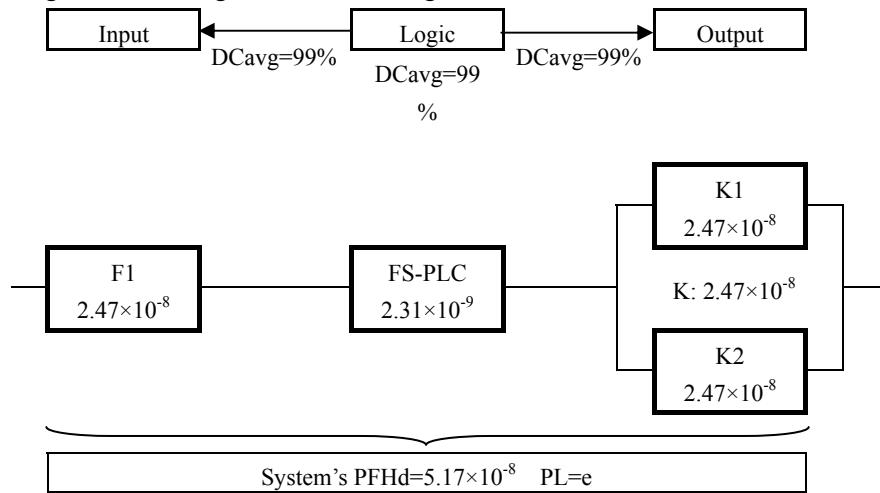


Fig. 50: Safety block diagram for muting

List of document development committee members

	Name	Belonging to
(Chairman)	Tsuyoshi TOEDA	Fuji Electric Co., Ltd.
(Members)	Nobuyoshi MIYAWAKI	JTEKT CORPORATION
	Kenichi IKEGAMI	JTEKT CORPORATION
	Kazumawa OSAWA	YASKAWA Electric Corporation
	Makoto TOKO	TOSHIBA CORPORATION, Social Infrastructure Systems Company
	Yasuhito TAKAMUKI	IDEC CORPORATION
	Masatoshi TSURUOKA	OMRON Corporation
	Tsuyoshi MATSUMOTO	OMRON Corporation
	Hiroo KANAMARU	Mitsubishi Electric Corporation
	Yoji YAMADA	Nissin Electric Co., Ltd.
(Secretariat)	Kunihiko EGAWA	The Japan Electrical Manufacturers' Association (JEMA)
	Tomoya ABE	The Japan Electrical Manufacturers' Association (JEMA)

To get the latest version of this document...

The latest version of this document is available by downloading electronic data. Downloadable as a charge-free open publication from the online store on the JEMA website as follows:

JEMA website URL : <http://www.jema-net.or.jp/>

For inquiries and more information on the contents of this document, please contact...

Engineering Section, Engineering Department, the Japan Electrical Manufacturers' Association (JEMA)

TEL: 03-3556-5884 / FAX 03-3556-5892

<p>© 2011 The Japan Electrical Manufacturers' Association. All Rights Reserved. The reproduction, reprint, etc. without permission are prohibited by the Copyright Act.</p>

Published on June 20, 2011

Publishing office

17-4, Ichiban-cho, Chiyoda Ward, Tokyo 102-0082

The Japan Electrical Manufacturers' Association (JEMA)

Tech. 11-01