Study of Machine Safety Control

N. MIYAWAKI

Since the establishment of ISO12100 (machine safety basic concepts and design-related general principles) in 2004, machine makers in Japan have been paying great attention to design safety. Especially in the machine control field, safety protection control measures based on system risk assessment are required. In accordance with the popularity of safety control measures, safety machine control systems with a reliable and user-friendly safety PLC (programmable logic controller) have been widely used. "Machinery Safety" refers to the safety of machines including the control system. This document describes safety design measures, safeguards, complementary protective measures, and additional protection measures based on ISO12100. Furthermore, the applicable scope of safety PLC and applicable stop categories according to the international safety standard are described regarding fail-safe safety systems including safety PLC supporting such measures using JTEKT's safety PLC TOYOPUC-PCS as an example. Concrete fail-safe control systems using a safety PLC are also described.

***Key Words**: machine, inherent safety, functional safety, fail safe, safety PLC*

1. Introduction

Along with the increased consciousness for machine safety centered around Europe in recent years, a group of standards have been systematized around the EN292 (European Machine Safety Standard 1992) originated from the EU Directive for machinery, meanwhile the international safety standard ISO12100 (Machine Safety –Basic Concepts and Design-related General Principle) was established in 2004 as the global standard. In Japan, too, the industrial safety and health law was revised in April 2006 to stipulate a new requirement that in order to preemptively eliminate factors causing labor accidents, an assessment of risks attributable to the equipment should be implemented and corrective measures based thereon should be taken. As such, attention is now drawn to the safety design of machines and equipment. Specifically in the area of machine control technology, it is required to incorporate safety protection measures (hereinafter referred to as safety control measures) for each control category based on the risk assessment on the equipment. Side by side with promulgation of the safety control measures, the usage of safety PLCs (programmable logic controllers) have been spreading. Safety PLCs are also referred to as fail-safe PLCs in the sense that it is intended to enable the control system, even during a malfunction, to diagnose the malfunction by itself as well as to shift itself to a safety state in case of failure. Such a control system characterizes the safety control circuits. Here we will describe the fail-safe control used in the risk reduction measures and machine safety control.

2. Risk Assessment Procedures and Risk Reduction

Figure 1 shows the risk assessment and risk reduction procedures described in the international safety standard ISO12100.

3. Risk Reduction Measures

The risk reduction measures include the inherent safety design → followed by protective measures via safety protection → additional protective measures → and information for the users. These must be implemented in this order until the permissible risk level is achieved. The standard system of ISO12100 is shown in **Fig. 2**.

Specifically, the protective measures A→B→C→D are implemented in this order as the risk reduction procedures. These safety measures are supposed to add up to ultimately achieve a permissible risk level for a particular machine system.

Furthermore, the safety control system which mainly controls power supply/shutdown as well as starting/stopping the machine is indispensable in order to make safety design available. As far as the control devices are concerned, safety relays and safety PLCs have been adopted. Recently, those safety PLCs certified by the Electric/Electronic/Programmable Electronic System Standard (IEC61508-1~7)[2)] are assuming a significant position in the field of safety control.

Figure 3 shows an image of specific risk reduction procedures.

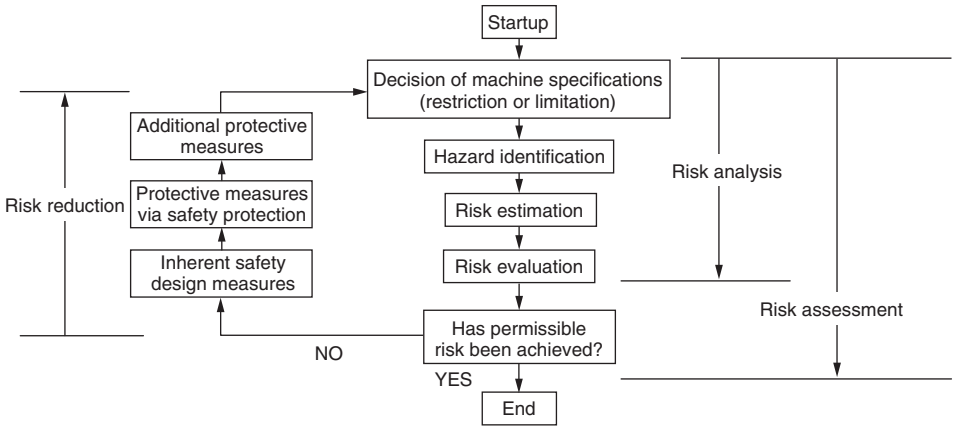

Fig. 1 Risk assessment and reduction procedures based on ISO12100

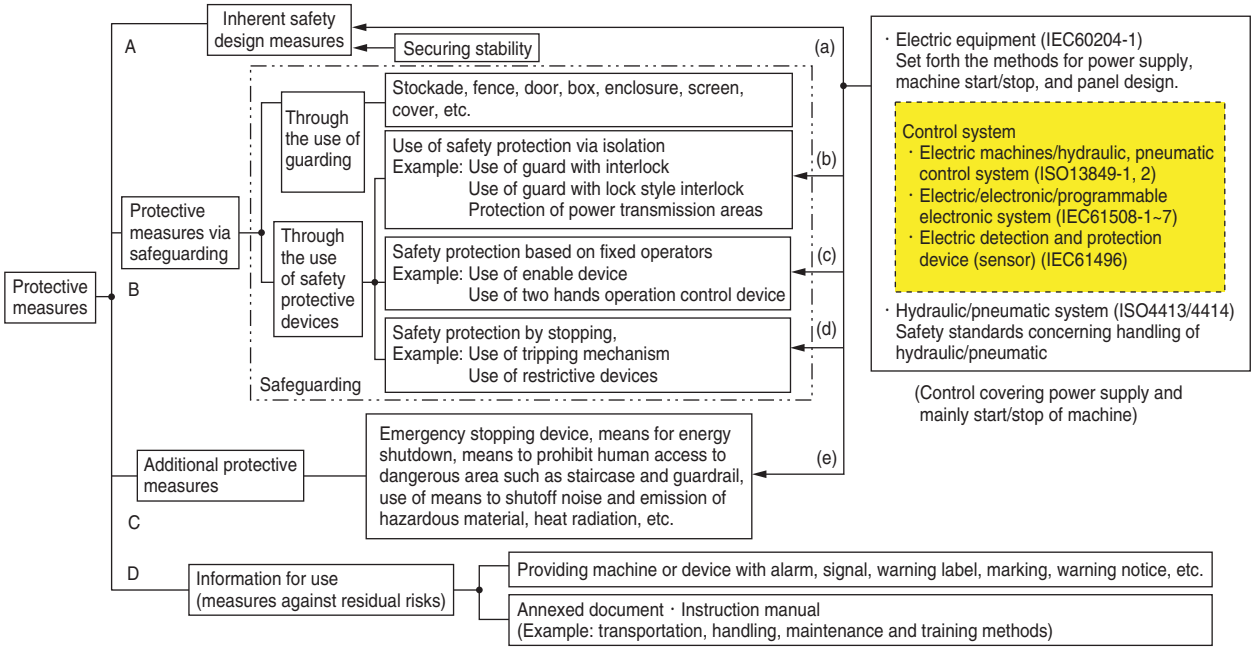

Fig. 2 Standard system of international safety standard ISO12100[1)]

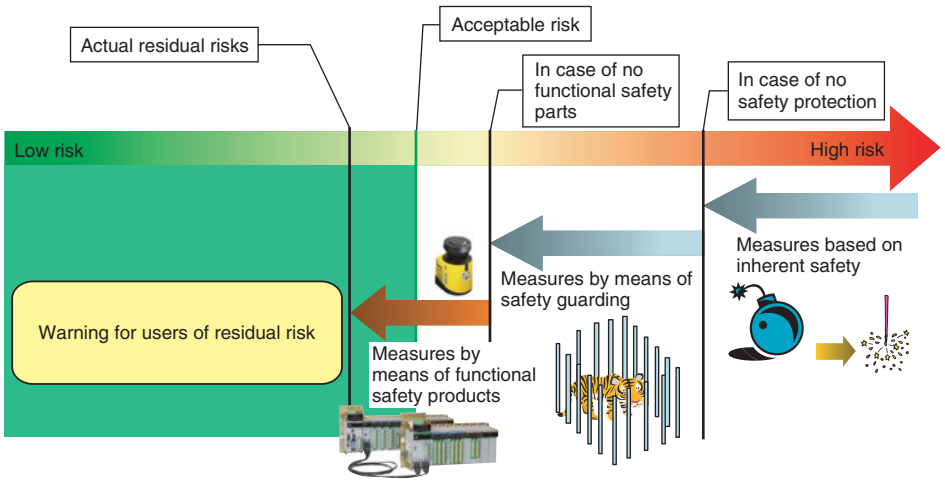

Fig. 3 Image of concrete risk reduction procedures

4. Safety Issues in Machine Control

Equipment with moving part(s) repeats a cycle of operation starting from the resting state to startup → preset action cycle → and back to the resting state again. The safety issues to be checked in this cycle are summarized in **Table 1**.

Table 1 Safety issues during machine operation cycle

Operation cycle	Objectives for safe operation
1) At start	No accident occurs due to startup No startup in hazardous condition (Example: Human exists in dangerous area)
2) During operation (continuous)	In case hazardous condition is brought about during operation (Example: Human moves into the hazardous area), the equipment shall be shutdown
3) In stop state	Make sure that no unintended startup should happen from resting state
4) Entire cycle	In case the safety control system is in hazardous condition (i.e. malfunctioning), the equipment shall be shutdown

In the event that the safety control system is in a hazardous condition (i.e. failed condition) during any step of the machine's operating cycle, it is liable that an accident can be caused immediately. In order to circumvent such hazardous conditions, the safety control devices are required to have a fail-safe capability. In the international safety standards, a SIL (safety index level) and categories are set forth as the safety capabilities of a control system in the Electric/Electronic/Programmable Electronic System Standard IEC61508 and ISO13849, respectively, so that safety capabilities can be assessed.

Normally, a programmable electronics system of SIL2 or category 3 or higher is structured with an architecture of 1oo2 (one-out-of-two) or better to realize this fail-safe capability. **Figure 4** shows the architecture of JTEKT's safety PLC, TOYOPUC-PCS.

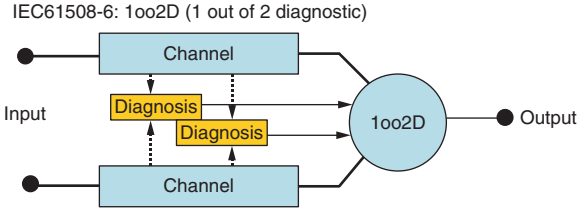

Fig. 4 TOYOPUC-PCS architecture based on IEC61508-6

The TOYOPUC-PCS incorporates an architecture which is comprised of two channels connected in parallel. If an abnormality is detected in the diagnostic test on either of these channels, or if the output conditions do not match, the system is promptly shifted to a safe state (normally, the state of OFF output).

5. Application Range of Safety PLC TOYOPUC-PCS

The SIL values of JTEKT's Safety PLC TOYOPUC-PCS in accordance with IEC61508 are as follows:

① Low demand mode: When the frequency of demanded activation of the safety related system is once a year or less, or twice as frequent as regular checks (proof checks) or less (**Table 2**)

Table 2 Low demand mode of operation

PFD	SIL
From $\geq 10^{-4}$ to $< 10^{-3}$	3
From $\geq 10^{-3}$ to $< 10^{-2}$	2
From $\geq 10^{-2}$ to $< 10^{-1}$	1

$PFD = 1.29 \times 10^{-4}$ (SIL3)

② High demand or continuous mode: When the frequency of demanded activation of the safety-related system is more than once a year, or more than twice as frequent as regular checks (proof checks) (**Table 3**)

Table 3 High demand or continuous mode of operation

PFH	SIL
From $\geq 10^{-8}$ to $< 10^{-7}$	3
From $\geq 10^{-7}$ to $< 10^{-6}$	2
From $\geq 10^{-6}$ to $< 10^{-5}$	1

$PFH = 1.56 \times 10^{-8}$ (SIL3)

In addition, the TOYOPUC-PCS has achieved category 4 of the EN954. This demonstrates that the TOYOPUC-PCS can cope with all applications in general industrial machinery.

Concerning the adaptability of this product to different machine stop categories, **Table 4** summarizes three stop categories classified in Clause 9.2.2 of EN60204-1 as well as the adaptability of this safety PLC to each stop category.

6. Fail-safe Control Measures in Machine Safety Control System

The safety PLC achieves fail-safe functionality through the architecture shown in **Fig. 4**. As an actual safety control system is composed of a sensor section, a logic

Table 4 Safety PLC and stop category of EN60204-1

Type of stop	Stop Category per EN60204-1 Clause 9.2.2	Description	Applicability of Safety PLC
Emergency stop	0	Immediate shutdown of power source for machine actuator	Applicable
Controlled stop	1	Power supplied until machine actuator stops, and thereafter the power is shutdown	Applicable
Controlled stop	2	Stop with power supplied to the machine actuator. Additional means/device required to meet ISO14118 (EN 1037) "Protection from unintended startup"	Not applicable by safety PLC alone

solver section and an actuator section per the IEC61508-6 (**Fig. 5**), it is necessary to achieve fail-safe functionality in the entirety of the system including the wiring and the circuits between these sections.

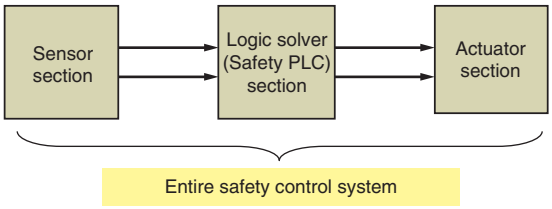

Fig. 5 Safety control system based on IEC61508-6

Specific description of the major fail-safe functions follows:

① Button Off Confirmation

It is desirable to allow the starting signal to be generated only after confirming both the action of closing a contact by a button press and that of canceling a contact by releasing a button (where welding is not occurring). (In this way, the possibility of an unintended start due to welding of the start button contact can be reduced.)

② Prevention of Restart

When the cycle is started by the start button, the operation is continued by the self-holding circuit. The self-holding is released when either the operator executes the stopping procedure or when the fail-safe function is activated due to failure so that machine may be prevented from restarting.

③ Normal Close Contact Point

To stop the machine by forcibly separating the contact point of a normal closed type switch directly utilizing the force used by the operator to press the emergency stop button, the force to open the safety fence door, or the force used to press the stroke end switch. (This allows the machine to be stopped in case there is a wire break in the safety circuit.)

④ Antivalent (Contradictory) Signal (for Categories 3 & 4)

The switching signals for the safety door are monitored by providing two switches with contradictory signals (positive and negative signals). (To reduce the possibility of failures due to common causes through the utilization of diversity of devices).

⑤ Detection of Inconsistency in Duplicated Signals (for Categories 3 & 4)

The contact point is duplicated so that any inconsistency between the two actions may be considered to indicate welding or improper contact, allowing the machine to stop and avoid a hazardous condition.

When a safety circuit is constructed through the use of the safety PLC, detection of inconsistencies in duplicated signals is conducted automatically.

⑥ Back Check

If the main circuit (a contact) is affected by welding in circuits such as the enable circuit contact for output, another pairing b contact (or supplementary b contact) will detect it and cause the machine to stop immediately or prevent the subsequent cycle from starting.

⑦ Test Pulse (applied to input/output modules of the safety PLC)

The input module is self-monitored by a test pulse (pulse of several hundred μs width). During this short period of time, the input channel (address) is suspended, while the checking of signals from the connected sensor is taken into consideration during the test pulse.

In the output module, the semi-conductor output module is self-monitored by a test pulse (several hundred μs width), provided it is required to make sure that the actuator on the output side is not affected by the test pulse.

⑧ Cross Short Check on a Duplicated Signal (Category 4)

In the event that a short circuit takes place in the wiring of the duplicated signal, it will be possible that the input signals have become identical signals. Therefore, in order to prevent any major failures, it is necessary to have a function to detect cross shorts in the wiring for duplicated signals. The safety PLC for Category 4 incorporates a function to detect cross shorts.

⑨ Transistor Output (Category 4)

While, in the case of a failure in the safety PLC for a transistor output module, the output is shut off by the output transistor, further shutdown of output through relay

is incorporated in order to reduce the probability of failure on the hazardous side due to failure by common causes. The purpose of this arrangement is to make sure that the output is shut down against one stress through two different devices, i.e. transistor and relay (implemented in the TOYOPUC-PCS).

7. Examples of Safety PLC Circuits

7. 1 Emergency Stop Button Circuit (Fig. 6)

The emergency stop button is equipped with a duplicated b contact point. The duplicate input signals are subjected to detection for duplicate signal inconsistency on the input side within a preset period of time. The output adopts a duplicate relay (contactor) with a supplementary b contact point being input via an input card for the purpose of checking for welding at start up. (For items ③, ⑤~⑨ in **Section 6** above)

7. 2 Safety Fence Door Monitoring Circuit (Fig. 7)

The door monitoring sensor incorporates duplicated a and b contact points. The duplicate input signals (contradictory modes) are subjected to detection for duplicate signal inconsistency on the input side within a preset period of time. The output adopts a duplicate relay (contactor) with a supplementary b contact point being input via an input card for the purpose of checking for welding at start up. (For items ③~⑨ in **Section 6** above.)

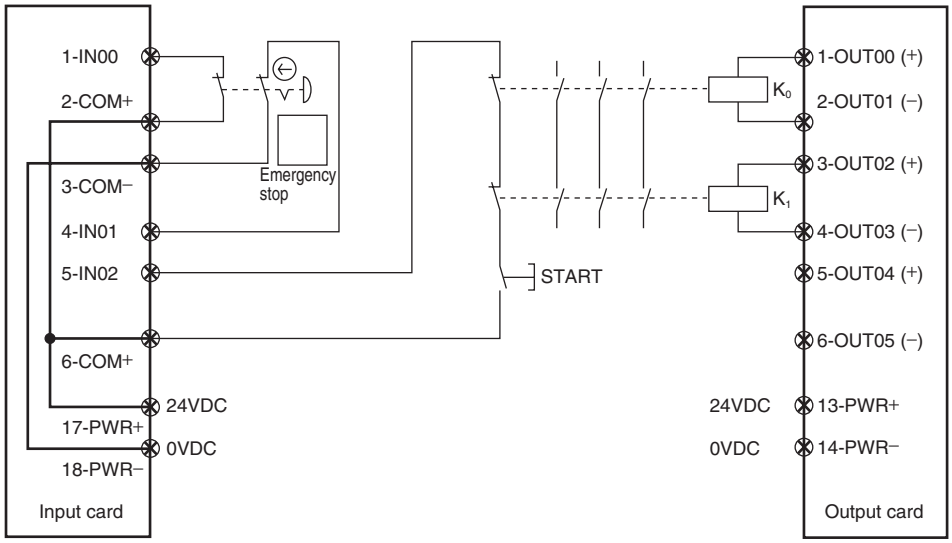

Fig. 6 Emergency stop button circuit

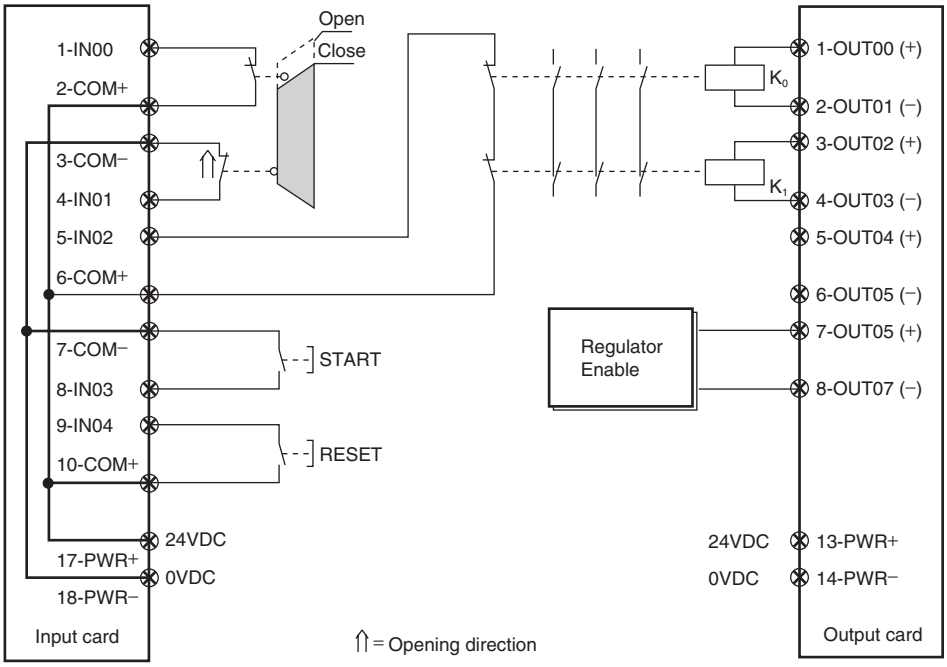

Fig. 7 Safety fence door monitoring circuit

8. Conclusion

JTEKT's development of the safety PLC, TOYOPUC-PCS, has contributed to the rapid spread of safety control systems incorporating safety PLCs, replacing the baseline safety relay control in primarily large scale facilities such as automobile production lines which have been expanding globally. However, this innovation utilizing safety PLCs is yet to be active in medium and small scale machines, which account for a large part of mechanical equipment due to the high costs of such large scale machinery[3]. In the future, the demand for more user-friendly and maintainable safety PLC is expected to increase along with the standardization of ISO12100. In order to meet this increased demand for safety PLCs that will assure the safety of operators in every manufacturing site, we will continue to develop new series of safety PLCs for a broad range of machines from large to small scale machines.

References

1) Dr. K. Futsuhara: The Safety based on the international safety standards. Nagaoka Technical Institute University. (2005.5) 3.
2) IEC61508-1~7: Functional safety of Electrical/ Electronic/Programmable electronic safety related systems Part 1 (1998) 65.
3) K. Niwa, N. Miyawaki: Measurements and Controls (2006.9) 34.

N. MIYAWAKI*

* *Mechatronics Control Design Department, Machine Tools & Mechatronics Division Headquarters*