Fuji Electric's Approach to Machinery Safety and Functional Safety —Total Safety—

Akihiko Kohanawa
Masami Hasegawa

1. Introduction

Serious accidents involving machinery and industrial plants have occurred one after another recently, and society's concern for improving safety and security has heightened. To establish safety and security requires a wide range of applied technology, such as the prediction of sources of harm, preventative maintenance for equipment, plant security, electronic recording of system data and so on. Meanwhile, new techniques for ensuring safety at the equipment design and system design stage have been standardized systematically in the form of machinery safety and functional safety.

This paper presents an overview of new techniques for establishing safety that are presently being incorporated into equipment and systems at manufacturing plants, and also introduces Fuji Electric's approach to safety.

2. Domestic and Foreign Trends for Safety Standards

2.1 Status of safety standards

In Europe, safety standards are widely utilized to regulate basic safety-related concepts and design principles. Under these circumstances, the ISO/IEC Guide 51 has been distributed[(1)], the international standard ISO 12100 (Safety of machinery − Basic concepts, general principles for design) has been issued, and as the culmination of this standard, the safety standard pyramid shown in Fig. 1 has been established. Further enhancement of the safety standards for individual machines and systems is expected in the future.

Fig.1 ISO/IEC safety standard pyramid

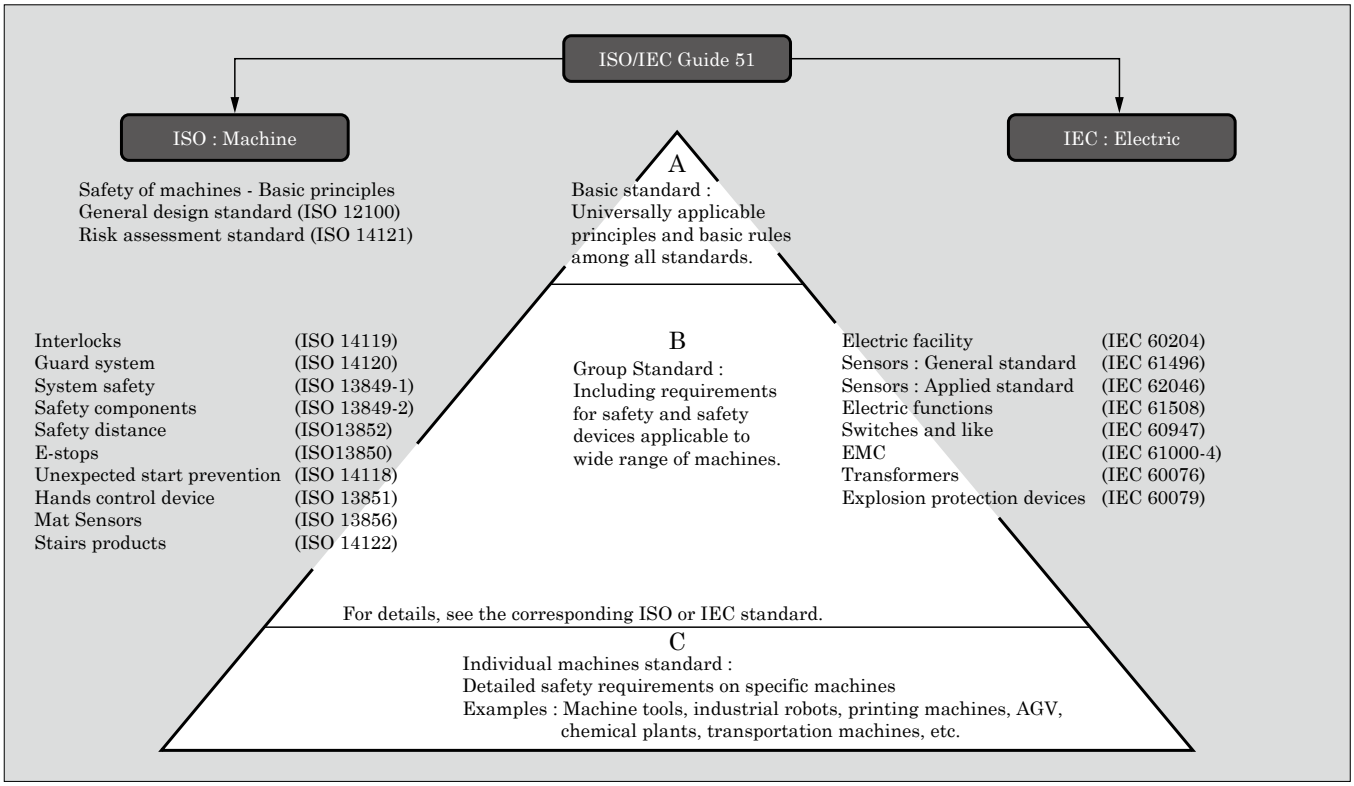


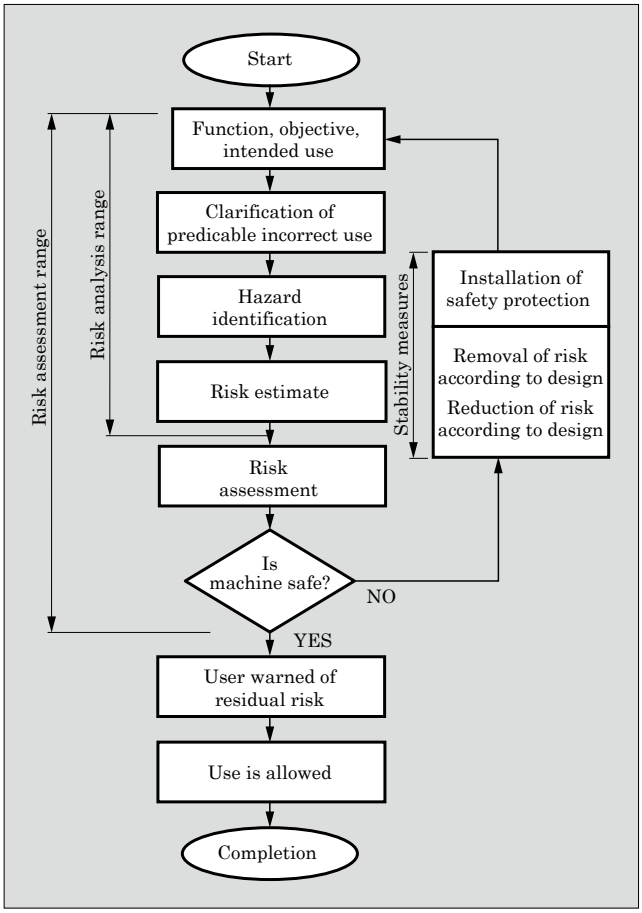
Fig.2 Amended labor safety and sanitation law

11 points of the amended labor safety and sanitation law

1	Implementation of long-term doctor interview and guidance to worker
2	Notice to worker of results of special medical examination
3	Implementation of survey of risk and harmful effect, and required measures
4	Exemption from plan notification for authorized business
5	Prospective eligibility requirements for safety managers
6	Strengthening of safety and sanitation system
7	Implementation of coordination among work by general contractors in the manufacturing industry
8	Issuance of written order for work such as cleaning a chemical facility
9	Improved display and document issuance system for chemical substances and the like
10	Establishment of report for expose to hazardous substances
11	Prospects for licensing and skill training

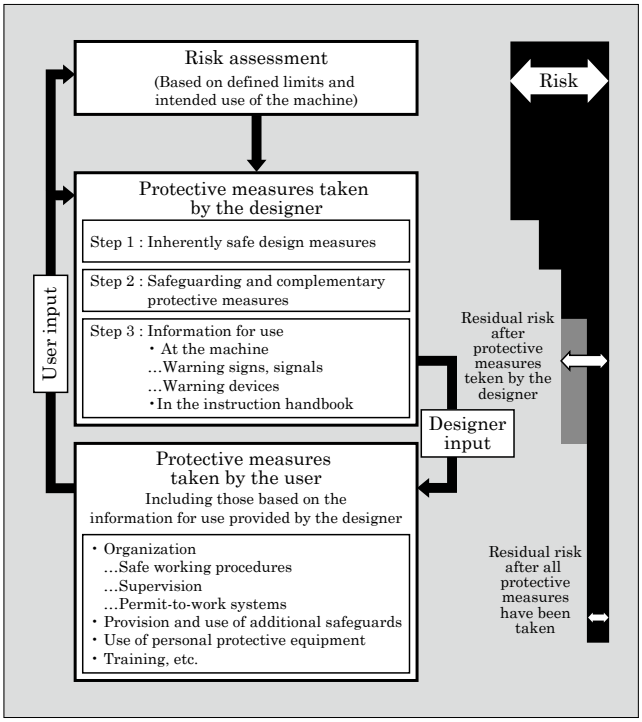
For all business offices where a safety manager is obligatory

Fig.3 Risk assessment and safety measures



In Japan, pursuant to the WTO/TBT agreement, the international standard system of Fig. 1 is accepted, and with nearly the same scheme, JIS were also established. Concurrent with these events, in April 2006 the Japanese "Labor safety and sanitation law" was

Fig.4 ISO 12100 basic concept



amended and the "Assessment of risk and hazards and implementation of required measures" was signed into law. As a result, a risk assessment must be performed when newly installing or modifying machinery or equipment, or when changing a work method or procedure (see Fig. 2).

In Japan, management responsibility has been strengthened and has come to be symbolized by the belief in "safety through onsite management." The new risk assessment concept (ISO 14121) uses the procedure shown in Fig. 3 to investigate thoroughly processes in which hazards develop into accidents, and was established as a means for breaking the relationship between hazards and accidents. In other words, the new international safety standard trend can be called "safety through hazard management."

2.2 Risk reduction process from the designer's perspective

ISO 12100/JIS B9700 prescribes, as general design principles for safety equipment and systems, a cycle for mutually feeding back "protective measures taken by the designer" and "protective measures taken by the user." As shown in Fig. 4, the method of reducing residual risk by focusing mainly on inherently safe design according to the risk assessment is understood to "build safety into equipment." In other words, the basic assumption is that "machines breakdown, and people make mistakes." This process requires a high level of technical capability in order to identify hazards, apply appropriate countermeasures and so on, and at Fuji Electric, assessors having such technical capability are being trained.

3. Concept of Total Safety

At present-day manufacturing sites, the mechanical equipment, driving mechanisms for such equipment, overall controllers and instrumentation including reaction processes, and the like are laid out in complex arrangements. Moreover, safety systems are formed as portions of usual standard systems. Accordingly, when constructing a safety system for an entire manufacturing site, the safety system must be applied with an understanding of diverse safety standards, and this is not a trivial task. Moreover, in the past, the Labor Safety and Sanitation Department oversaw this type of safety system for manufacturing sites, and with the application of new safety standards was seen as a future challenge. As shown in Fig. 5, Fuji Electric aims to provide safety solutions by integrating all types of machinery safety, safety-related control and functional safety, and consulting with the customer. This is the concept of total safety.

4. Approach to Machinery Safety

When constructing a safety system in the FA (factory automation) field, in systems where hazardous situations arise with the operation of mechanical equipment, the basic principle is "preventive safety." Specifically, the focus is on methods for directly guarding against the intrusion of hazards from mechanical equipment and on application of the electrical equipment of machines (IEC 60204/JIS B9960-1) safety standard. Figure 6 shows target items of the electrical equipment of machines safety standard.

4.1 Standards relating to the safety of mechanical equipment systems

There are three high level standards relating to the safety of mechanical equipment systems: ISO 13849-1, IEC 60204-1 and IEC 61508.

(1) ISO 13849-1

General design principles of portions relating to the safety of mechanical equipment systems are classified according to the severity of the harm and the safety category. In the 2006 version, stochastic factors such as the mean time to dangerous failure were added to qualitative categories, and the PL (performance levels) method was adopted. There are five PL, ranging from "a" (low) to "e" (high).

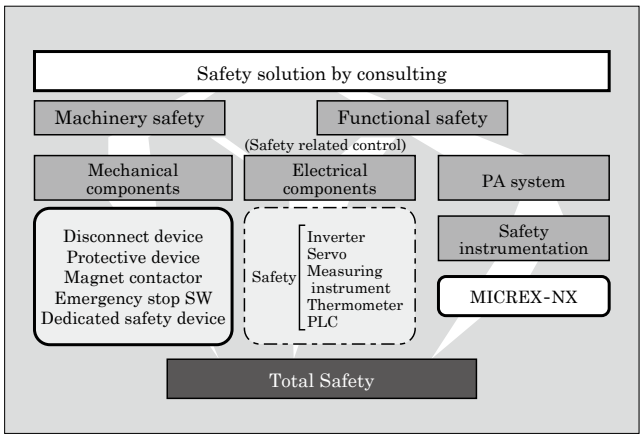
(2) IEC 60204-1

This is a standard for machine control panels, and indicates the interrelationship between requirements of individual parts and the types of parts shown in Fig. 6. Mechanical system safety, with the exception of standards for intrinsic machines, must conform to this standard.

(3) IEC 61508

In order to maintain mechanical equipment is a safe condition, this standard regulates product safety for E/E/PE (electrical/electronic/programmable electronic systems) devices equipped with "functions" and is applicable to inverters, electronic control equipment and PLCs. Based on this standard, individual standards are being enacted for the abovementioned devices.

Fig.5 Total safety concept



4.2 Safety of electrical equipment for machines

Figure 7 shows an example of a safety system for a machine control panel. The parts configuring the control panel shown in this figure must satisfy the safety requirements listed in Table 1. Particular attention must be paid to electrical parts of the main circuit and electrical parts related to emergency shutdown, for which compliance with standards was previously exempt, but is now required.

Fig.6 Targeted items of safety standards for electrical equipment of machines

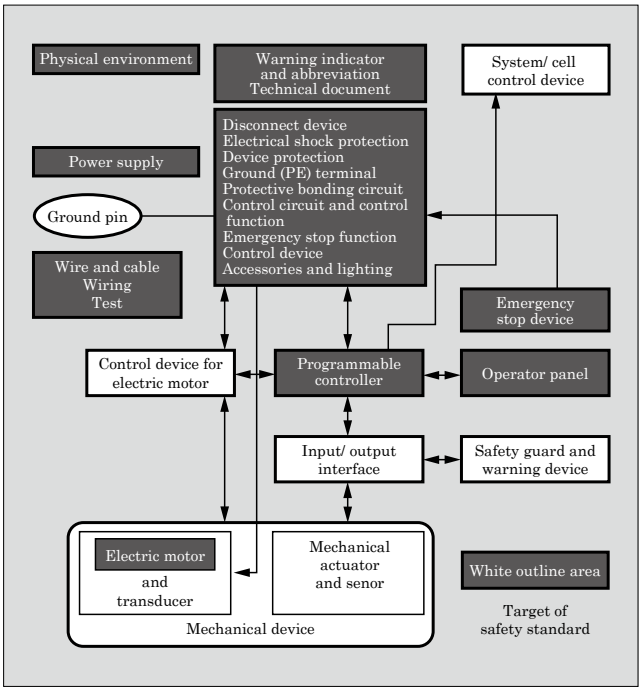
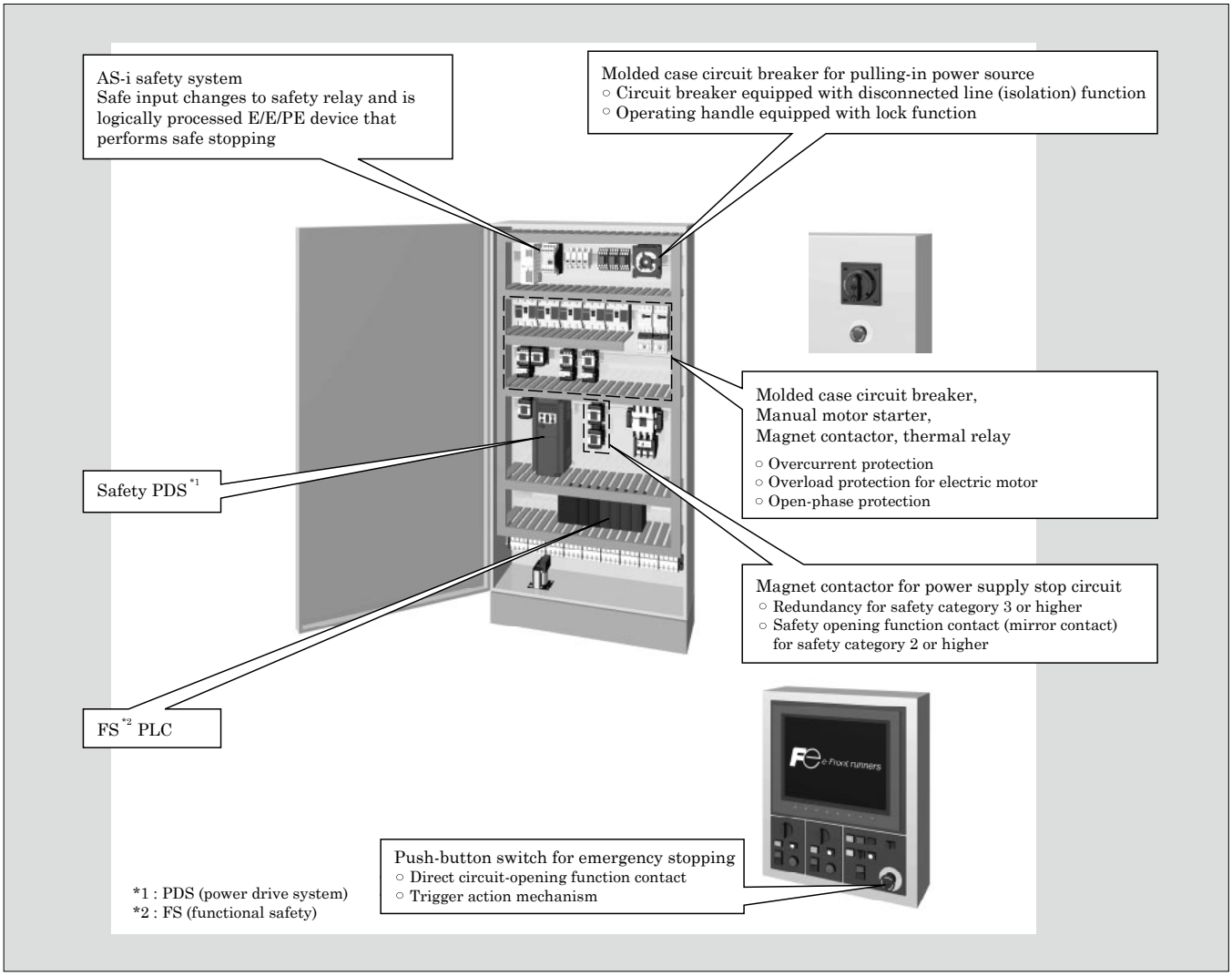


Fig.7 Safety system for control board



In order to comply with these requirements, Fuji Electric is preparing a lineup of products that incorporate safety functions in standard products.

5. Approach to Functional Safety

When constructing a safety instrumented loop in PA (process automation), the use of many measuring devices (pressure transmitters), safety controllers, and safety I/O modules are needed. These devices shall be developed in accordance with a functional safety standard (IEC 61508), and shall be certified for safety by a third-party certifying authority. Fuji Electric incorporates "functional safety" and sells the FCX-AⅡ/CⅡ series of pressure transmitters, and the MICREX-NX as safety controllers and safety I/O modules.

An example of a safety instrumented system realized with the MICREX-NX is introduced below.

5.1 Standards relating to safety instrumented systems

Two standards relate to safety instrumented systems, IEC 61508 and IEC 61511. The difference between these two standards is that IEC 61508 pertains to the manufacturers and suppliers of devices, while IEC 61511 pertains to the designers, integrators and users of the system. Conformance to IEC 61511 is required when installing a safety instrumented system.

Additionally, the entire safety lifecycle (specification, design and implementation, installation and commissioning, operation and maintenance, and changes after commissions) of the system is also prescribed in detail as shown in Fig. 8. In Japan, a standard corresponding to IEC 61508 has already been established with JIS, and a standard corresponding to IEC 61511 was established with JIS in February 2008.

5.2 Safety instrumented system

An SIS (safety instrumented system) is a critical system that reduces risk during a plant failure to within an allowable range, and ensures a high level of safety for human life, the environment and equipment. Previously in Japan, the use of a relay circuit as a SIS was typical, but in Europe, an SIS that uses a controller and conforms to new safety standards came into

Table 1 Requested safety items for electrical equipment of machines, and support

IEC 60204-1, JIS B 9960-1 requests	Products that comply with safety standards	Comments
Section 4.2, Equipment selection	Fuji global standard certified products Molded case circuit breaker, magnet contactor, push-button switch, etc.	—
Section 5.3, Power supply disconnect function	G-Twin breaker, ELB External operating panel	Isolation compliance IEC 60947-2 compliance
Section 6.2, Direct circuit break function	Finger protection structure (installed in various devices)	Protection level IP20
Section 7.2, Overcurrent protection	G-Twin breaker, ELB Manual motor starter	Cooperation among overcurrent protection devices
Section 7.3, Overload protection for electric motor	Manual motor starter Magnet contactor, thermal relay	Cooperation among over load/ protection devices
Section 9.2, Control function	If category 0 stop is used in emergency stop function, must be configured from hardwired electromechanical components only	Due to IEC revision (Oct. 2005, JIS under being revised), hardware clause was eliminated and use of electrical, electronic, programmable electronic devices became possible.
Section 9.4, Control function for time of failure	Magnet contactor	Safety opening function contact (mirror contact) IEC 60947-5-1 Appendix F
Section 10.7, Device for emergency stopping	Command switch for emergency stopping	Direct circuit-opening function contact IEC 60947-5-1 Appendix K compliant IEC 60947-5-5 compliant Safety trigger action function ISO 13850 compliant
Section 12.3, Enclosure protection rank	Command switch: IP65 External operating handle: IP54 (Molded case circuit breaker)	Requested protection level for general-purpose industrial enclosure IP32, IP43, IP54

Note) Category 0: stopping by shutting-down mechanical actuator directly

Fig.8 Overall safety lifecycle

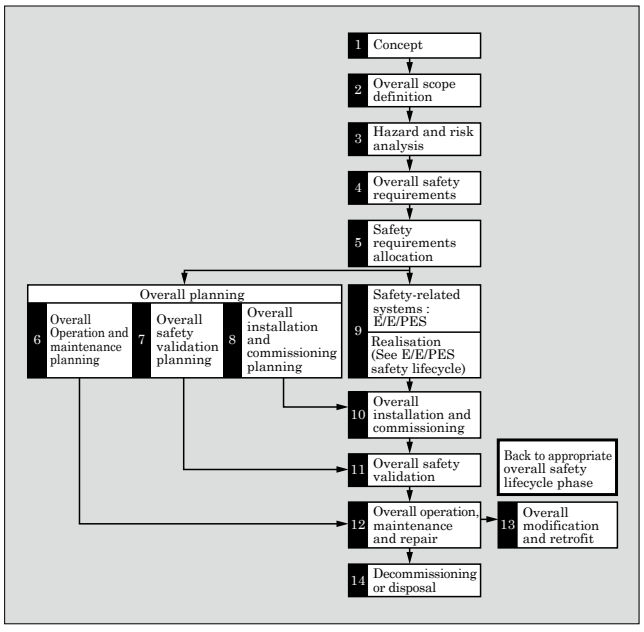


Fig.9 TÜV certificate

widespread use.

(1) Hardware and software

(a) Safety controller

An SIS realized with the MICREX-NX is described below. The MICREX-NX is a controller that conforms to IEC 61508, and has acquired SIL (safety integrity level) 3 certification (see Fig. 9) from TÜV (Technischer Überwachungs-Verein). Three types of CPUs (AS412, AS414 and AS417) having different processing capabilities are available for use with the MICREX-NX, enabling systems to be configured in many variations, from single setup to completely redundant setup configurations. As a result, the MICREX-NX has flexibility and scalability for selecting a system according to the size and use of a customer system (see Table 2). The realization of SIL 3 with a single CPU (single setup) is an important feature and is made possible by an architecture that implements two program logic blocks in a single CPU, enabling the soundness of the CPU to be checked from computational results (see Fig. 10). The first program is generated by a designer, and the second program is a reverse-operation program generated automatically by the system when the first program is compiled and converted into an executable form. Built into the CPU is a diagnos-

Table 2 Flexible system configuration

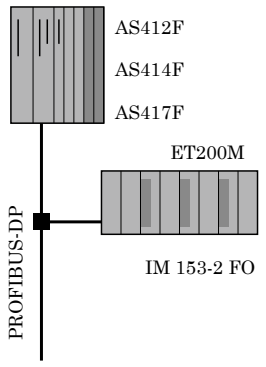
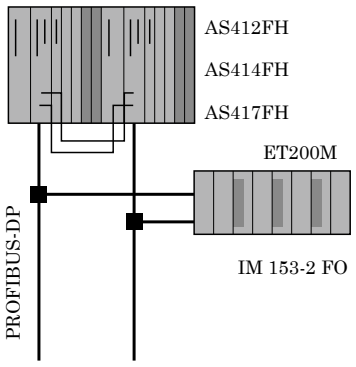
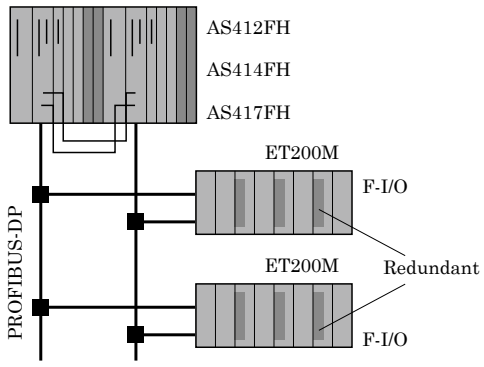
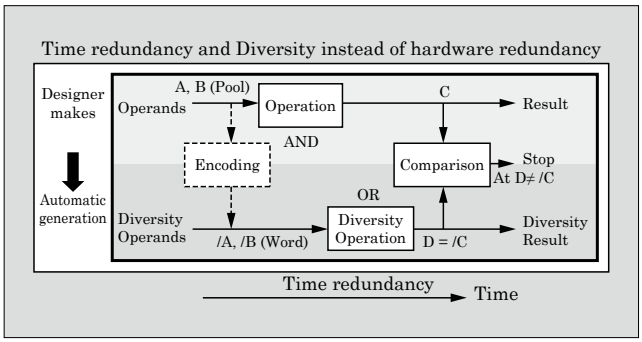
Single set-up	Redundant set-up with syngle I/O modules	Completely redundant set-up
		
A single set-up achieves SIL3	Redundant CPU and redundant bus Components can be exchanged without system stopping.	Redundant CPU and redundant bus and redundant fail safe I/O Components can be exchanged without system stopping.

Fig.10 Checking the soundness of the CPU



tic function that issues instructions for the system to operate in a stable direction when a failure is detected at the time of turning on power or during system operation. The detection of failures, broken wires and the like in the connected I/O module is also possible.

(b) Safety I/O

Table 3 lists the types of safety I/O modules. Each I/O module has acquired SIL 3 certification. Redundant circuitry within each I/O module validates the input and output signals of dual sensors, and a diagnostics circuit performs cross-checking to increase the level of safety.

(c) Safety communications

Safety communications between the safety controller and a safety I/O module is realized by using the PROFIsafe profile based on the PROFIBUS-DP[2]. PROFIsafe is the first communications system that conforms to IEC 61508, conforms to the SIL 3 safety level, and is applicable to a wide range of FA and PA fields. Using the PROFIsafe profile, a PROFIsafe telegram, as shown in Fig. 11, appends control data, counter data and CRC (cyclic redundancy check) data after safety I/O signal data to prevent the dropout of safety communications data.

(d) Engineering

The engineering of a safety control program is implemented using dedicated failsafe function blocks (FBs) (50 types). These FBs have received TÜV certification.

Required FBs are placed on the engineering screen, connected by mouse operations, and then are compiled and converted into a failsafe user program. During the engineering work, a password is requested whenever the screen is opened or data is loaded, and only appointed designers are able to design and modify the software. Thus, security considerations are taken into account so that a safety program is not modified unintentionally.

(2) Safety Matrix

The MICREX-NX is provided with a software program called “Safety Matrix.” This Safety Matrix basically has three functions (see Fig. 12). The first is an automatic programming function for the safety circuit. On the Safety Matrix, signals for abnormal conditions are defined on the horizontal axis, and output signals to devices for which safe operation is desired are defined on the vertical axis. A safety program can be generated easily by defining associations at points of intersection. The second is a function for directly displaying on an operating panel the Safety Matrix information generated by engineering. This enables accurate and timely responses to failure events (what type of failure occurred and what stopped?). The third is a function that enables data linkage with “exSILentia” by exida.com LLC[3]. exSILentia is a software program used to compute the PFD (probability of failure on demand) for each SIS operation request, and to perform SIL analysis and other assessments. Data generated by exSILentia can be imported into the Safety Matrix to increase the engineering efficiency further. Also, the Safety Matrix can partially support the safety lifecycle management prescribed by IEC 61511, and is ap-

Table 3 Safety I/O

Components	Number of input/output and safety level	Voltages and currents	Installation environment
Digital input (DI 24)	24 input : SIL2 AK4 12 input : SIL3 AK6	24 V DC	Temperature Horizontal installation : from 0 to 40 ˚C Vertical installation : from 0 to 60 ˚C Contaminant concentration SO_2 : < 0.5 ppm H_2S : < 0.1 ppm
Digital input (DI 8 NAMUR)	8 input : SIL2 AK4 4 input : SIL3 AK6	24 V DC	
Digital output (DO 10)	10 input : SIL2 AK5 or SIL3 AK6	24 V DC 2A	
Analog input (AI 6)	6 input : SIL2 AK4 6 input : SIL3 AK6	4 to 20 mA	

Fig.11 PROFIsafe communication telegram

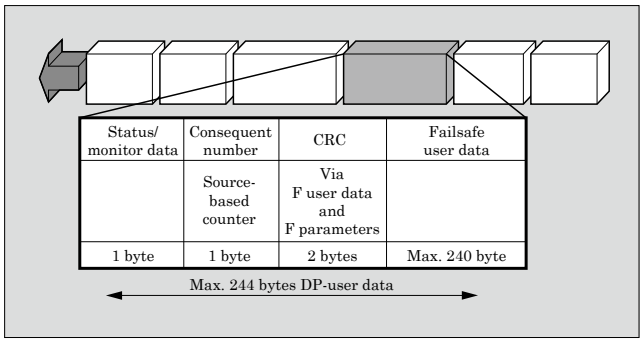


Fig.12 Function of Safety Matrix (for engineering)

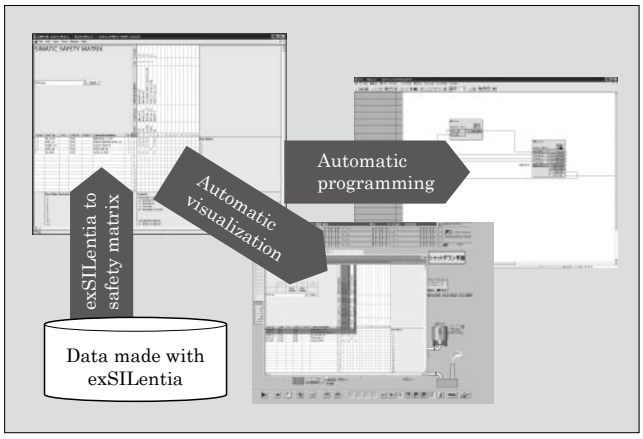


Fig.13 Function of Safety Matrix (for lifecycle management)

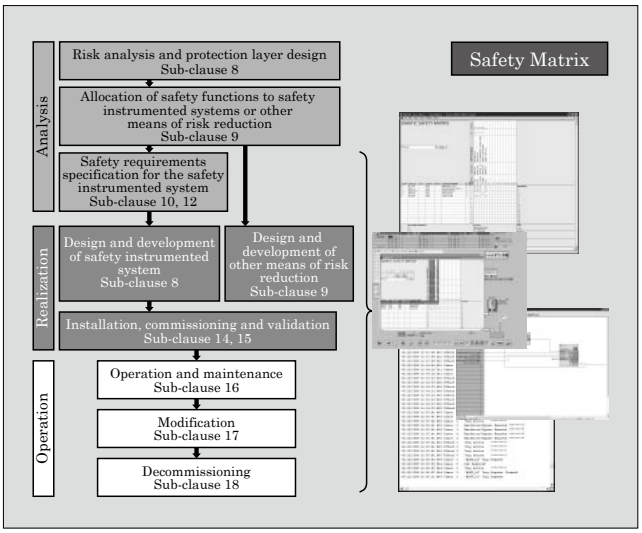
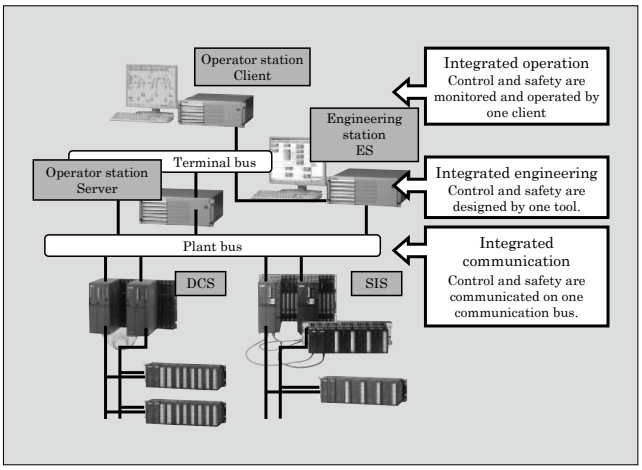


Fig.14 Integrated safety and control



plicable to a wide range of processes, from engineering to management (see Fig. 13).

(3) SIS and DCS integration

As shown in Fig. 14, monitoring of the SIS measuring state and software engineering are implemented using the same equipment as with DCS (distributed control system).

(a) Operating and monitoring

Monitoring of the SIS measuring state is implemented with DCS operator station clients. The use of the same clients as DCS has the following advantages.

- ○ Even during an emergency, monitoring and operation can performed reliably.
- ○ The SIS operating state and the state of the control system can be verified on the same screen, and the plant status can be assessed accurately.

(b) Engineering

SIS engineering work is performed using the same ES (engineering station) as with DCS. The engineering work can be performed using the CFC (continuous function chart) normally used with DCS, and in the same environment and with the same procedure. In other words, since there is no need to choose between two different types of engineering for use, the engineering work can be carried

out more efficiently. Also, even in the case where signals are exchanged with the DCS side, the use of a dedicated interface FB makes it possible to construct an SIS without having to be aware of system differences.

6. Postscript

Fuji Electric's approaches to machinery safety and function safety, which aim for total safety, have been described. Safety consists not only of machinery safety and function safety, and safety that comprehensively incorporates both into a plant or equipment must be considered. In the future, as "Total Safety" solutions, Fuji Electric intends to continue to provide safety that is stable and conforms to international standards.

References

(1) IEC
http://www.iec.ch/ (Reference: December 21, 2007)
(2) Japan PROFIBUS Organization
http://www.profibus.jp/index.htm (Reference: December 21, 2007)
(3) exida.com LLC
http://www.exida.com/ (Reference: December 21, 2007)