EJX SERIES OF IEC61508 SAFETY STANDARD-COMPLIANT DIFFERENTIAL PRESSURE TRANSMITTERS

SONODA Kaoru *1

Safe plant operation has long been a prime requirement for process automation in oil, gas, petrochemical, and other industries. Since it is an important mission for field device vendors to provide even safer products to customers, Yokogawa has been developing field devices with enhanced safety functions. Safety instrumented systems (SIS) constitute one systematic means for safe plant operation. The specifications of such systems have been incorporated into the IEC 61508 standard and the standard has been adopted by many plants. This paper introduces the new EJX series of TÜV SIL2-approved pressure transmitters with SIS functionality.

INTRODUCTION

Safe plant operation has long been pursued in all industries. Specifically, in the process automation industry which involves many hazardous elements, safety measures including explosion-protected systems have been adopted based on numerous tragic experiences. This paper introduces a differential pressure transmitter series for safety instrumented systems including Emergency Shut-Down (ESD) systems which constitute the last lifeline for process automation (Figure 1).

SAFETY INSTRUMENTED SYSTEM

In process automation in oil, gas, petrochemical and other industries, it is crucial that plants are operated safely by previously preventing disasters. Plant operation must also not impact the natural environment, nor cause human and physical disasters in the case of accidents. The safety instrumented system introduced in this paper was developed to previously prevent such disasters based on experience built up over a long years.

As safety instrumented system standards, there are presently IEC61508 which defines safety functions in general industries, and IEC61511 which defines safety instrumented systems for process industries, both of which are set up as IEC standards.

In IEC61511, Safety Instrumented System (SIS) is defined as shown below.

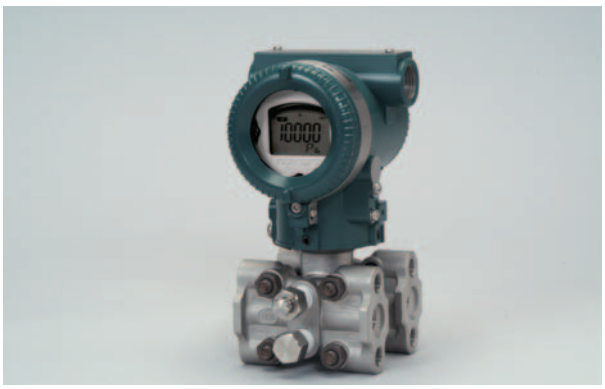

Figure 1 External View of EJX Series Safe Differential Pressure Transmitters

*1 Product Business Center, IA Business Division

Table 1 Safety Integrity Level (Low Demand Mode)

Safety Integrity Level	Probability of failure on demand, average (Low Demand mode of operation)	Risk Reduction Factor
SIL 4	$\geq 10^{-5}$ to $<10^{-4}$	100000 to 10000
SIL 3	$\geq 10^{-4}$ to $<10^{-3}$	10000 to 1000
SIL 2	$\geq 10^{-3}$ to $<10^{-2}$	1000 to 100
SIL 1	$\geq 10^{-2}$ to $<10^{-1}$	100 to 10

"A SIS is defined as a system composed of sensors, logic solvers and final control elements designed for the purpose of:

- Automatically taking an industrial process to a safe state when specified conditions are violated (shutdown function);
- Permitting a process to move forward in a safe manner when specified conditions allow (permissive function); or
- Taking action to migrate the consequences of an industrial hazard (mitigation function)."

SAFETY INTEGRITY LEVEL (SIL) AND FUNCTIONS REQUIRED FOR FIELD INSTRUMENTS

The functions required for field instruments, which are the elements composing the safety instrumented system, are examined below, in consideration of the basic requirements for field instruments in IEC61508.

First, what is the definition of Safety Integrity Level (SIL) frequently used in safety instrumented systems. In safety instrumented systems, the most important target is how to reduce risks inherent to the process itself. Therefore, it is the safety instrumented systems' mission to enhance the safety of the process itself by reducing potential inherent risk factors. This is done by reducing the Probability of Failure on Demand (PFD). SIL is defined as shown in Table 1 depending on the PFD levels. A higher SIL means that a safer system can be achieved.

The IEC standard includes two types of modes, Low Demand Mode and High Demand Mode, and SIL is defined for each mode. IEC61508 defines these two modes as shown below.

"The frequency of demands for operation made on a safety-related system is no greater than one per year and no greater than twice the proof test frequency, [IEC61508-4, 3.5.12]

If the ratio of diagnostic test rate to demand rate exceeds 100, then the subsystem can be treated as low demand mode, [IEC61508-2, 7.4.3.2.5 Note 2]

The diagnostic test interval will need to be considered directly in the reliability model if it is not at least an order of magnitude less than the expected demand mode. [IEC61508-2, 7.4.3.2.2 Note 3]"

Two types, Type A and Type B, are defined for equipment composing safety instrumented systems (IEC61508-2, 7.4.3), which are as follows. Simple equipment including valves, relays, switches, etc. is classified as Type A, and complicated equipment including "smart" transmitters and PLCs, etc. is classified as Type B. For Type A and Type B, SILs are defined respectively as shown in Tables 2 and 3. The Safety Failure Fraction (SFF), which is a factor for determining the SILs in these tables, will be described taking the differential pressure transmitter as an example.

In terms of safety, equipment failures can be roughly divided into two categories: Fail Safe and Fail Dangerous. Fail Safe failures mean those at the level of modules and subsystems inside the transmitter. For these failures, the system can be migrated to the safe side through automatic diagnoses by the diagnostic functions of the equipment. Failures in CPUs and ASICs correspond to this type of failure mode.

On the other hand, Fail Dangerous failures mean, for example, that an error in operational processes inside a CPU cannot be found unless deviations in the relation between input and output signals is determined. Such a situation is very dangerous for the safety of the equipment. In other words, even if an abnormality occurs inside the transmitter, it appears to be working normally when viewed from the outside. In such a case, although the safety instrumented system must ignore the signal from this transmitter, the transmitter continues to be used without stopping because the abnormality cannot be detected, leading the system to a hazardous situation. For this reason, the above two failure modes are divided into detectable and undetectable elements, and SFF is determined on the rate of Fail Dangerous Undetected, the most dangerous element for safety. The calculation methods defined in IEC61508 are shown below, and SFF is determined using these.

$$SFF = (\lambda_{SD} + \lambda_{SU} + \lambda_{DD})/(\lambda_{SD} + \lambda_{SU} + \lambda_{DD} + \lambda_{DU})$$

where: SFF = Safety Failure Fraction

λ_{SD} : Fail Safe Detected

λ_{SU} : Fail Safe Undetected

λ_{DD} : Fail Dangerous Detected

λ_{DU} : Fail Dangerous Undetected

If SFF exceeds 60%, 90% or 99%, SIL 1, SIL 2 or SIL 3 is obtained respectively. IEC61508 permits self-declaration for SIL 1 but requires the third-party certification for SIL 2 and higher.

Tables 2 and 3 indicate the relationship between redundancy and SIL. For example, if SFF exceeds 90%, SIL 2 is obtained using one transmitter. Similarly, SIL 3 is obtained using two transmitters and SIL 4, using three transmitters. As safety instrumented systems are increasingly adopted in the oil, gas, and

Table 2 Type A Subsystem

SFF	Hardware Fault Tolerance		
	0	1	2
0%	SIL1	SIL2	SIL3
>60%	SIL2	SIL3	SIL4
>90%	SIL3	SIL4	SIL4
>99%	SIL4	SIL4	SIL4

Table 3 Type B Subsystem

SFF	Hardware Fault Tolerance		
	0	1	2
0%	NA	SIL1	SIL2
>60%	SIL1	SIL2	SIL3
>90%	SIL2	SIL3	SIL4
>99%	SIL3	SIL4	SIL4

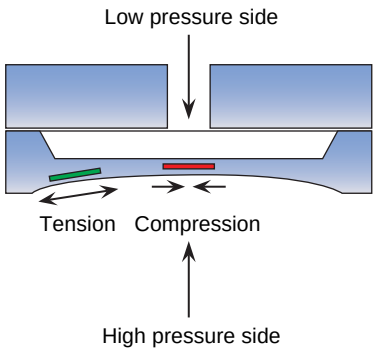

Figure 2 Silicon Resonant Sensor

petrochemical industries, there is a growing expectation of higher SIL where risk is lower. For this reason, the demand for field instruments having the certification of SIL 2 or more is increasing. As Table 3 shows, whether SIL 2 certification is acquired or not is the important turning point for using equipment or instruments at higher SIL. For instance, if a safety instrumented system at SIL 4 is requested, transmitters of SIL 2 must be used, and thus equipment having certification for SIL 2 or more is expected to appear in the near future in a number of field instruments.

DESIGN CONCEPT FOR AND FEATURES OF EJX SERIES TRANSMITTERS

EJX series transmitter has been developed based on the functions of EJA series transmitters to meet with SIL 2 functions required in the IEC61508 and IEC61511. The developed transmitters are described below.

Safety Design Concept

High reliability in the EJX series transmitters is achieved by adopting a silicon resonant sensor and by employing highly reliable circuits and advanced diagnostic functions in the design. Accordingly, compliance with SIL 2 certification is achieved only with standard design without implementing specialized design for satisfying the SIL 2 requirements of IEC61508.

High Reliability Design Silicon Resonant Sensor

DPharp series transmitters over three generations of EJ, EJA, and EJX series have adopted the silicon resonant sensor, which detects pressure from the number of vibrations. This silicon resonant sensor is composed of two vibration-type sensors for compression and tension (Figure 2). This structure means that no output is obtained when either sensor fails. This theoretically decreases the factors for Fail Dangerous Undetected failures due to sensor failures, required for safety design.

Highly Reliable Electronic Circuits and Diagnostic Functions

Although the diagnostic functions of EJX series transmitters comply with the factors for SIL 2 in failure modes for every block such as CPUs, ASICs inside the circuits, they do not satisfy the factors for SIL 2 in reliability for functions of calculation operations inside the CPUs and ASICs. For this reason, the reverse calculation function is used as the diagnostic function for these elements to reduce Fail Dangerous Undetected failures.

Next, the reverse calculation function is described. Calculation processing carried out inside the EJX series transmitters is divided into four blocks as shown in Figure 3 and the matching of input with output in each block is verified. If an abnormality is found as a result of verification for each group, it is output that an abnormality is present in the diagnosis result. This satisfies the requirement of SIL 2 with the same circuit as the standard differential pressure transmitter without adding a special circuit configuration.

TÜV Certification

EJX series differential pressure transmitters were evaluated by TÜV based on the requirement of the IEC standards and successfully acquired certification. When acquiring certification, the transmitters are evaluated not only for the IEC 61508 requirement of hardware but also for software. Specifically for software, the transmitters were shown to satisfy the requirement for SIL 3. As a result, certification by TÜV, as shown in Figure 4,

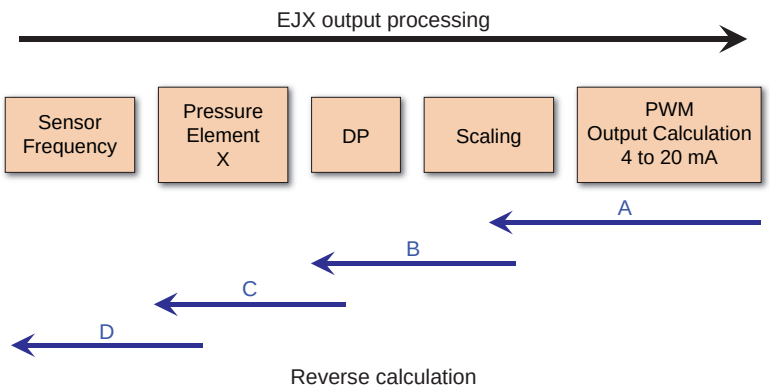

Figure 3 Reverse Calculation Function

Figure 4 TÜV Certificate

has been acquired.

The contents of TÜV certification are as follows:

Single Use for SIL 2
Dual Use for SIL 3
Life cycle ≥ 50 years.

This sufficiently satisfies SIL presently required for differential pressure transmitters. TÜV certification employs the form of type certification, that is, if EJX series transmitters acquire certification, then certification is given to all transmitter models which incorporate the same software. The certified period is 5 years but can be extended. If the IEC61508 standard is modified, the transmitters must be re-evaluated complying with the new standard when the certification period expires. Since the TÜV certification includes evaluation of design processes and manufacturing locations, if manufacturing locations and the like are changed, then the new manufacturing locations must be audited.

Operation Records in the Field

Another important issue for safety instrumentation transmitters is the operation records in the field. In PFD, which is an important index used for actual safety instrumented system designs, Mean Time Between Failures (MTBF) determined by taking the actual field failure records into account, is an important factor. The EJX series transmitters are the latest products in the DPharp series, which adopts the silicon resonant sensor. They are produced by following and developing the EJA series concept in the basic design and adding many diagnostic functions. For this reason, they have achieved a high PFD as shown in Figure 5 because the reliability of DPharp series transmitters has, of course, been proven in the field.

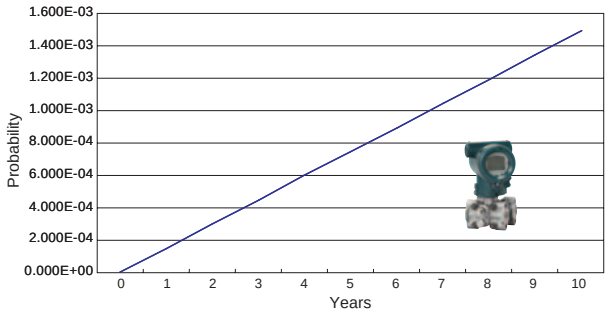

Figure 5 PFD Data

CONCLUSION

The fact that the EJX series transmitters acquired SIL 2/3 certification this time as standard products without changing hardware design specific to safe instrumented systems is largely due to the use of the silicon resonant sensor in a redundant manner and the combined design of the sensor with robust electronic circuits equipped by many diagnostic functions. This result was obtained thanks to the good design system and highly reliable production system of Yokogawa. Thus, Yokogawa has the potential to acquire the TÜV certification not only for the EJX series transmitters but also for its field instruments. For safety instrumented systems, since the above concept applies not only to pressure transmitters but also to temperature transmitters, flowmeters, level gauges, and so forth in general process automation, Yokogawa will continue to develop other subsystems and instruments in safety instrumented systems. Presently, the field-bus association is drawing up safety instrumented system standards, and Yokogawa will promote their development as important elements of future safety instrumented systems as well as contribute to such activities. ◆

REFERENCES

(1) Safety Equipment Reliability Handbook (http://www.exida.com)
(2) Sales/Marketing of EJX certified pressure transmitter (Yokogawa Electric Corporation TI 01C25A01-04E)
(3) IEC61508 Part 1-7: 2000
(4) IEC61511 Part 1-4: 2004

* "EJX" and "DPharp" are the registered trademarks of Yokogawa Electric Corporation.