安全規格 IEC61508 適合差圧伝送器 EJX

EJX Series of IEC61508 Safety Standard-compliant Differential Pressure Transmitters

園 田　　薫*1
SONODA Kaoru

石油等のプロセスオートメーションのプラントの操業において，事故を未然に防ぐことは重要な項目として長年に亘って取り組まれており，プロセスに直接取り付けられるフィールド機器をより安全なものとして提供することは，機器ベンダーにおいて大きな命題であった。当社は，この命題を開発の大きな柱として，長年に亘り，差圧伝送器を始めとするフィールド機器を提供してきた。一方，システムとして事故を未然に防ぐ仕組みである安全計装システムは，プラントで発生した過去の災害を反省した上で定められ，現在IEC規格として広く採用されている。本稿では，このIEC規格に適合した差圧伝送器EJXの特長や機能について述べる。

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 SIL 2-approved pressure transmitters with SIS functionality.

1. はじめに

安全操業は，あらゆる産業において，長年に亘って課せられてきた命題である。特に危険要素の多いプロセスオートメーションでは，幾多の悲惨な経験を基に，防爆システムを始めとする安全対策が採られてきた。本稿では，プロセスオートメーションの最後の命綱であるESD（Emergency Shut Down）システムを始めとする，安全計装で使用される差圧伝送器について紹介する（**図1**）。

2. 安全計装システム

石油・ガス，石油化学等のプロセスオートメーションでは，災害を未然に防いで，安全に操業することが最も重要な指針である。事故による人的，物的災害は当然として，自然環境に影響を与えないことも，プラント操業にとって重要である。長年の歴史の中で培った経験を踏まえてこれらの災害を未然に防ぐシステムとして考え出されたのが，ここに紹介する安全計装システムである。

現在，IEC規格として規定されており，産業全般での安全機能を定義したIEC61508と，プロセス産業用の安全計装システムを定義したIEC612511がある。

安全計装システムSIS（Safety Instrumented System）とは，IEC61511で以下のように定義されている。

“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）;

図1　安全伝送器EJXの外観

*1　IA事業部プロダクト事業センターフィールド機器 PMK部

表 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	>=$10^{-5}$to <10^{-4}	100000 to 10000
SIL 3	>=$10^{-4}$to <10^{-3}	10000 to 1000
SIL 2	>=$10^{-3}$to <10^{-2}	1000 to 100
SIL 1	>=$10^{-2}$to <10^{-1}	100 to 10

・Permit 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）. ”

3. SIL とフィールド機器に要求される機能

安全計装システムを構成する要素であるフィールド機器に要求される機能の検討を行う。そこで，IEC61508でのフィールド機器に対する基本的な要求を整理してみる。

始めに，安全計装でよく使用される SIL（Safety Integrity Level）の定義について述べる。安全計装では，プロセス自体が本来持っているリスクを如何に低減するかが，一番重要な目標であり，潜在的に含まれる危険要因を低減させることで，プロセス自体の安全性を高めるのが安全計装の使命である。そこで，PFD（Probability of Failure on Demand）を低減することでこれを実現している。SIL はこのPFDのレベルにより，**表1**のように定義され，SILが高いほど，より安全性の高いシステムが実現可能となる。

IEC 規格では，Low Demand Mode と High Demand Mode の二種類のモードがあり，それぞれSILが定義されている。さらに，IEC61508 では Low Demand Mode と High Demand Mode の二つのモードが以下のように定義されている。

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 excepted demand mode, ［IEC61508-2, 7.4.3.2.2 Note3］

安全計装システムを構成する機器は，Type A と Type B の2種類が定義されている（IEC61508-2, 7.4.3）。これらを簡単に説明すると，バルブ，リレー，スイッチ等の単純な機器は Type A，スマート伝送器や PLC 等の複雑な機器は Type B に分類される。Type A，Type B は，各々**表 2，3** に示すように，SIL がそれぞれ定義されている。この表の SIL を決定する要因である SFF（Safety Failure Fraction）について，差圧伝送器を例にとり説明する。

安全性の観点から考えると，機器の故障は Fail Safe と Fail Dangerous に大別できる。Fail Safe とは伝送器の内部のモジュールやサブシステム単位の故障で，これらに関しては，機器が持っている診断機能によって自動的に診断され安全サイドへ動かされる。CPU や ASIC の故障がこれに相当する。

一方，Fail Dangerous は，例えばCPU内部の演算プロセスについては，入力信号と出力信号の関係の偏差等を求めなければ，演算プロセスの誤りを見つけることができない。これは機器の安全性から考えると，非常に危険なことである。つまり，機器内部で異常が発生していても，伝送器は外部から見て正常に動いているように見えてしまう。このような場合，安全計装システムでは，この伝送器の信号を無視しなければいけないのであるが，異常が判らないため，そのまま使い続けることとなり，危険な事態を招くことになる。このため，この 2 つの故障モードを検出可能・不可能の要素に分け，安全上最も危険な Fail Dangerous Undetection の占める割合で SFF を決定している。以下に示すのが，IEC61508で定義されている計算方法で，これにより SFF を求める。

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

SFF ＝ Safety Failure Fraction
λ_{SD} ： Fail Safe Detected
λ_{SU} ： Fail Safe Undetected
λ_{DD} ： Fail Dangerous Detected
λ_{DU} ： Fail Dangerous Undetected

そして，SFFが，60%を超えればSIL1，90%超でSIL2となり，99%を超えればSIL3となる。IEC61508では，SIL1については自己宣言を認めており，SIL2 以降に関して

表 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

表 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

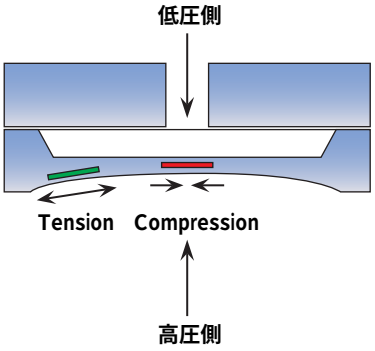

図2　シリコンレゾナントセンサ

は，第三者による認証を要求している。

表2，3に示す表は，冗長化とSILの関係を示しており，例えば，SFF が 90% 超の場合，伝送器 1 台で SIL2 となる。同様に，2台でSIL3，3台使用するとSIL4となる。最近の石油・ガス・石油化学での安全計装採用の動きが高まるなか，より危険性の少ない高いSILへの期待が高まってきている。そのため，それに対応するSIL2以上の認証を持ったフィールド機器への需要が増えてきている。**表3**からも判るように，高いSILで使用するにはSIL2認証を持っているかいないかが大きな分かれ目となる。例えば，SIL4の安全計装を求められた場合，SIL2の伝送器を採用する必要があり，今後多くのフィールド機器で，SIL2以上の認証を持った機器が登場してくることが期待されている。

4.　EJX 設計コンセプトと特長

EJX では，IEC61508，IEC61511で要求されているSIL2の機能に合致すべく，EJAの機能をベースに開発を行った。以下に，その詳細を述べる。

4.1 安全設計コンセプト

EJXの高信頼性は，シリコンレゾナントセンサの採用と高信頼性回路設計，先進の診断機能の採用により実現されている。このため，IEC61508 の SIL2 の要求を満たすための特別な設計を行うことなく，標準設計のまま SIL2 認証への適合を実現している。

4.2 高信頼性設計シリコンレゾナントセンサ

EJ，EJA，EJX と 3 代に亘る DPharp シリーズは，圧力を振動数で検出するシリコンレゾナントセンサを採用している。このシリコンレゾナントセンサは圧縮，引っ張りの2つの振動式センサにより構成されており（**図2**），このことにより，どちらかのセンサが故障した際，出力がされない仕組みとなっている。このため，安全設計上要求されるセンサの故障による Fail Dangerous Undetected 要因を，原理的に減らしている。

4.3 高信頼電子回路と診断機能

回路内部の CPU，ASIC 等のブロック単位での故障モードに関しては，EJXの診断機能でSIL2の要件を満たしているが，CPU，ASIC 内部の演算機能の信頼性に関しては，SIL2の要件を満足していない。このため，これらの要素の診断機能として，リバースキャリキュレーション機能を採用し，Fail Dangerous Undetected を削減した。

次に，リバースキャリキュレーション機能の詳細を説明する。EJX内部のソフトウエアで行われている演算処理を，**図 3** に示すように 4 つのブロックに分割し，各々のブロックの入力信号と出力信号の整合性を検証している。各ブロックの検証結果に異常があった場合には，診断結果に異常ありとして出力する。これにより，特別な回路構成を付加することなく，標準の差圧伝送器と同じ回路で SIL2 の要求を満足した。

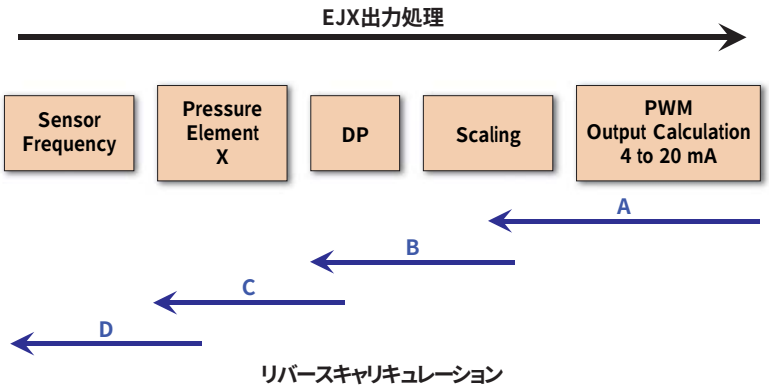

図3　リバースキャリキュレーション機能

図 4　TÜV 認証

4.4　TÜV 認証

IECの要求に基づいて，TÜVによる評価を受け認証を取得した。認証に当たっては，IEC61508のハードウエアの要求だけではなく，ソフトウエアに関しても評価をされている。特にソフトウエアに関しては，SIL3の要求に対して，満足をする評価を得た。その結果，**図 4** に示すような内容で TÜV の認証を得ている。

TÜV 認証の内容は，

Single Use for SIL2
Dual Use for SIL3
Life cycle> ＝ 50years

であり，これは，現在差圧伝送器に求められている SIL を十分に満足している内容である。TÜVの認証は型式認証の形態を採っており，EJXであれば，同じソフトウエアを搭載している全てのモデルに対して与えられる。認証期間は 5 年間で，継続は可能である。IEC61508 の規格が変更になった場合には，認証期間が過ぎた時点で，新しい規格に則った評価を受ける必要がある。この認証には設計プロセス，生産場所の評価を受けているので，生産場所の変更等が生じた場合には新しい生産場所の監査を受ける必要がある。

4.5 フィールドにおける実績

安全計装用伝送器にとって重要なものが，フィールドでの実績である。実際の安全計装設計に使用する重要な指数である PFD は，実際のフィールドでの故障実績を加味して求めた MTBF が大きな要素を占める。EJX はシリコンレゾナントセンサを採用している‘ DPharp ’シリーズの最新製品で，基本的な設計はEJAの考えを踏襲し，発展させたものであり，多くの診断機能を付加したものである。そのため，当然 DPharp シリーズのフィールドでの信頼性実績が裏付けとなり，**図 5** に示すような高い PFD を実現している。

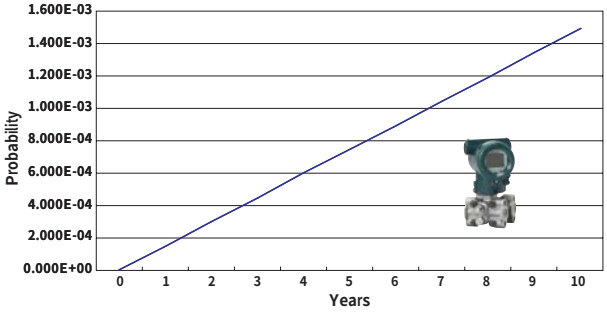

図 5　PFD データ

5. お わ り に

今回，EJXが安全計装用に特別なハードウエアの設計変更をすることなく，標準品としてSIL2/3の認証を得られたのは，シリコンレゾナントセンサを冗長化して使用している点と，多くの診断機能を搭載した堅牢な電子回路の組み合わせた設計に依るところが大きい。また，当社の設計システムの良さや生産システムの信頼性の高さが評価された結果である。このことは，EJXだけではなく，横河のフィールド機器に関してTÜV認証を得る潜在能力があるということである。通常のプロセスオートメーションと同様に圧力伝送器だけではなく，温度伝送器，流量計，レベル計等へのアプリケーションの要求もあり，安全計装では，今後，他の機器への展開を進めていく。現在，フィールドバス協会で，安全計装規格の策定が進められており，当社もこの活動に貢献すると共に，今後の安全計装の重要な要素として開発を推進していく所存である。

参考文献

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