圧力センサにおける不具合時の挙動と その危険源に関する考察

森山　哲[*]　蓬原　弘一[**]

The behavior of pressure transmitters upon failure and examination of its hazard

Tetsu MORIYAMA [*]　　Koichi FUTSUHARA [**]

要旨：安全関連パラメータを物理量から安全情報として抽出する原理を述べ、圧力伝送器を例にアナログ入力を警報信号や安全関連制御信号に変換するときの論理構造を述べる。

キーワード：アナログ入力・しきい値演算・ウィンドウズコンパレータ・制御システムの安全関連部

1　はじめに

機械や装置に組み込まれたセンサの一部は安全に極めて緊密になっており、国際規格では制御システムの安全関連部として扱われる。センサは、機械システム上で顕在する危険源だけではなく、機械や装置の様々なところに組み込まれて、運転操作とその制御性に関連し、安全確保の主要部を構成する場合がある。

機械やプラントの安全関連パラメータ、例えば、位置、速度、温度、圧力が予め設定された制限値を逸脱する場合、制御システムは停止操作出力やそのための警報を生成する。本論文では、原始情報である計測信号を安全関連部の安全情報として取り扱いできることを明らかにする。

2　使用上の注意

2.1　主要な物理量の処理過程

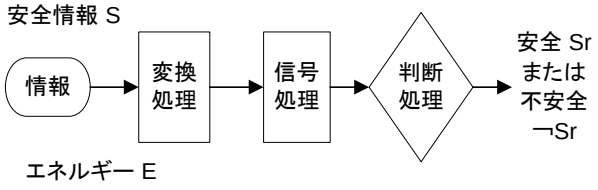


図1　安全の計測システム

図１は物理量の処理過程を示す。安全は情報として取り扱うことはすでに述べられている [1]。安全情報 S ならびに判断処理の結果としての安全または不安全の情報 Sr および¬Sr は２値で、Sr=1 を“安全”、Sr=0 を“安全でない”、¬Sr=1 を“危険”、¬Sr=0 を“安全”、とする。ここで¬は否定を表す。

2.2　直動変換と変調変換

計測情報を電気信号に変換する形態は、図２に示すように直動変換型構造と変調変換型構造に大別できる [4].

直動変換型構造のシステムは，情報の発生源自身がエネルギを幅射する。即ち，情報発生源とエネルギ発生源が共通である。

測定量を、それに比例する電圧または電流の変化に、直動的に変換する計測器の実用例として温度計と圧力計の一例を示す。

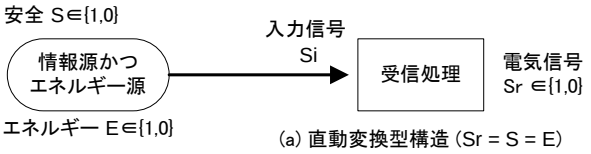
・熱電対は熱系から電気系への直接変換であり，物理現象であるゼーベック効果（熱起電力 mV）をエネルギ増幅に変換して利用している.

・水晶やサファイヤのような結晶誘電体に圧力をかけると電圧に変換される。

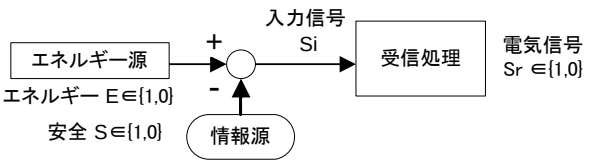
変調変換型構造のシステムは、検出対象を抽出するためにあらかじめエネルギを幅射しておき、トランスデューサは検出すべき情報をこの幅射エネルギの変調信号として抽出する。さらにエネルギの伝達

*長岡技術科学大学大学院/森山技術士事務所　〒236-0057　神奈川県横浜市金沢区能見台 3-26-7　tetsu-moriyama@muh.biglobe.ne.jp
**長岡技術科学大学大学院機械系　〒940-2188　新潟県長岡市上富岡町 1603-1　futsuha@mech.nagaokaut.ac.jp

経路を遮断することによって変調信号を得る方法と，エネルギの伝達経路を変える(曲げる)ことによって変調信号を得る方法とに分けることができる。 図２(b)において受信側のアナログ情報は負信号である。測定量で回路の導電性を制御して、それを電圧または電流に変える変調変換器の実用例には測温抵抗体、抵抗歪み計、ピエゾ抵抗効果圧力計、光導電セルがある。またレーダー式のレベル計も変調変換型構造のシステムである。本論文で取り扱う圧力伝送器は変調変換型構造である。



(a) 直動変換型構造 (Sr = S = E)



(b) 変調変換型構造 (Sr = S･E)

図2　直動変換型構造と変調変換型構造

3　安全確認のためのセンサ

3.1　安全情報伝達の論理式

安全情報抽出の原理によれば安全を示す情報はエネルギの発生によって伝達されなければならない。

図 2(a)に示す安全情報自体がエネルギ源である直動変換型において、情報源が安全であるか否かを示す情報として２値の論理変数 S∈{1,0}とし、伝達されるエネルギ E∈{1,0}の有無をそれぞれ〔1,0〕とすると信号処理機能で受信される入力 Si は

$$Si = S = E$$

と表すことができる。

図 2(b)に示す変調変換型においては、安全情報源がそれ自体ではエネルギを有しないので、安全を示す情報は外部から供給されるエネルギ源 E に重畳して伝達される。情報源が安全であるか否かを示す情報を２値の論理変数 S∈{1,0}とし、伝達されるエネルギ E∈{1,0}の有無をそれぞれ〔1,0〕とすると信号処理機能で受信される入力 Si は

$$Si = E \cdot S$$

と表すことができる。

3.2　非対称故障モードの論理式

図３に示した入力を２値信号 x∈{1,0}、出力を２値信号 y∈{1,0}とする２値の処理系 f(x)において、その動作状態を S*∈{1,0}、ただし S*=1 を正常な状態、S*=0 を故障状態とするとき、出力 y が

$$y = f(x) \cdot S^* \qquad \cdots\cdots (1)$$

で表されるとき、その処理系の特性を非対称故障モードと定義する [5]。

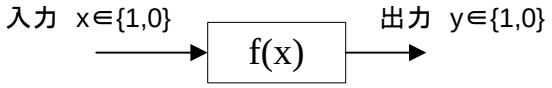


図3　2値の処理系

計測される情報がアナログ信号であるとき、安全を示すか否かを判断するために、図 4 のように安全の上限を決める要素と安全の下限を決める要素を作り、この機能を窓と呼ぶ。入力信号が圧力伝送器のアナログ信号 A(t)である場合、しきい値演算によって２値信号 x∈{1,0}を得ることができる。

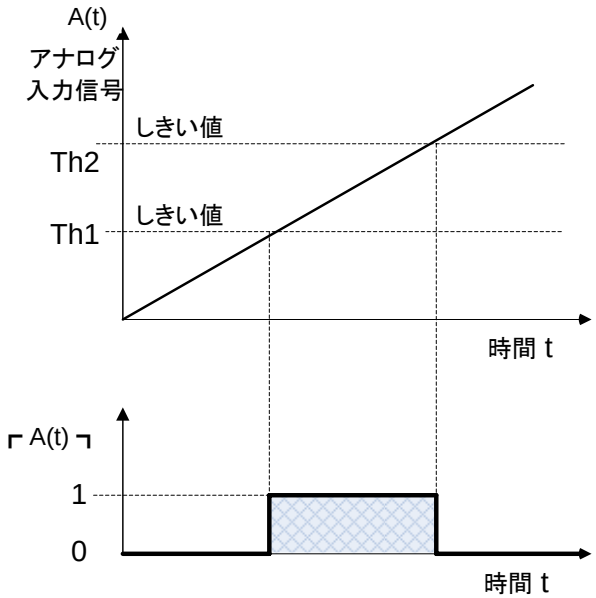


図4　幅を持つしきい値演算

すなわち上限値、下限値をもつアナログ計測値の安全性の判断は、しきい値を２つ使って“窓による判断機能”ウィンドウコンパレータで行うことが出来

る。図４の下限しきい値 Th1 と上限しきい値 Th2 はこのアナログ入力信号の安全を示す許容変動範囲である。安全出力とアナログ入力値 A(t)は

Sr = 1,　　Th1 ＜ A(t) ＜ Th2

Sr = 0.　　A(t) ≧ Th1 または　A(t) ≦ Th2

と表すことができる。論理式では Sr は下限のしきい値演算と上限のしきい値演算の論理積であるので(2)式で表すものとする。なおアナログ信号 A(t)に対する下限のしきい値演算を ⌐ A(t)、上限のしきい値演算を A(t) ¬、窓によるしきい値演算を ⌐ A(t) ¬ と表す[6]。

Sr = ⌐ A(t)・A(t) ¬ = ⌐ A(t) ¬　・・・・(2)

非対称故障モードのウィンドウズコンパレータの論理式は、ウィンドウズコンパレータを２値の処理系 ⌐ A(t) ¬ とし、その動作状態を w*∈{1,0}、ただし w*=1 を正常な状態、w*=0 を故障状態とするとき、(1)、(2)式より(3)式と表すことができる。

y = ⌐ A(t) ¬ ・w*　・・・・(3)

4　危険源

4.1　圧力センサの構造

図５に変調変換型である２線式圧力伝送器のブロック図をしめす。センサは測定原理により静電容量式、振動式、ピエゾ抵抗式がある。スマートタイプ伝送器は内蔵するプロセッサと周辺回路の自己診断が可能である。

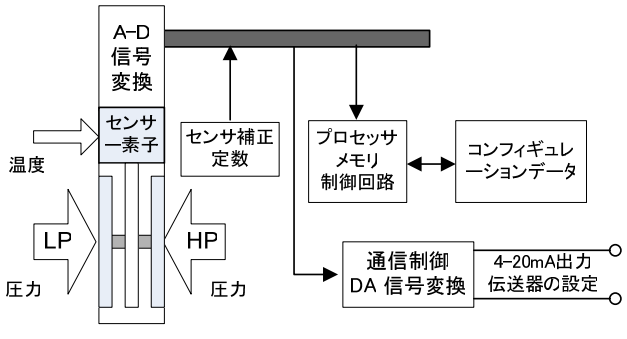


図5　圧力伝送器ブロック図（typ）

圧力伝送器は、正常に機能しているときに4-20mA の電流を測定値に比例して出力する。しかし伝送器が正常に機能していない場合は、4-20mA の範囲外の電流を伝送器出力として外部の受信側に伝達する。表１に 4-20mA 信号システムにおける故障モードの出力値の例を示した。故障モード信号の出力値のオーバーレンジ(107%以上)またはアンダーレンジ(-7%未満)の選択は、ソフトによる設定あるいは基盤上のジャンパーピンであらかじめ選択する構造である。

表１　4-20mA システムの故障モード出力値（例）

断線	-25%　　(0mA)
自己診断による	-7%未満　(2.9mA)
自己診断による	107%超　　(21.1mA)

4.2　故障モード

表２に圧力計測システムの導圧配管、圧力伝送器、警報設定器の故障モードの例を示す。システムが故障を検出できるものを“可”、出来ないものを“否”、条件によって可否が変わるものを“不定”としてある。

表２　圧力計測の故障モード

部位	モード	検出
導圧配管	詰まり	否
	漏れ	否
	破断	否
ブロックバルブ	漏れ	否
三方弁	漏れ	否
バリヤ・ダイアフラム	変形	否
	付着物	否
	水素透過	否
	脆化	否
センサ素子	故障*	不定
センサ校正データ	間違い	不定
	消失、書き換わり	不定
エレキモジュール	故障	不定
ソフト	エラー	否
配線（出力）	断線	可
	短絡	可
電源（24VDC）	故障	可
IV 変換抵抗 250Ω	断線	可
	短絡	可
警報設定器	故障	不定
同上出力リレー	断線、接触不良	不定
	短絡、溶着	不定

4.3 相反する危険源と安全側故障

圧力伝送器の不具合時には、安全関連部は安全側に働くように設計されなければならない。安全関連制御系では、警報回路や遮断回路を設けて圧力がしきい値を超えると装置を停止させる、あるいは縮退モードに移行させる。そのために表１に示したように伝送器の故障時の出力を選択する。これは回復不可能な故障モードの圧力伝送器が危険源にならないための方策である。この方式は、装置や機械の安全関連部で広く採用されているが、装置の運転状況によって故障時の安全側出力値方向がオーバーレンジ側（100%以上)、あるいはアンダーレンジ(0%未満）と変動する場合がある。これを相反する危険源という。この場合は伝送器の故障時の出力値を安全関連制御系の入力としてそのままでは適用できない。すなわち非対称故障モードが定まらない。そのため安全側故障に移行させるために、制御システムが保有している運転状態の情報をもとに安全関連制御系でアクチュエータの安全方向を定める。

機械やプラントの制御システムの安全関連部は、リスクアセスメントを行い、その結果従って表３に示すISO13848-1で分類される５通りのカテゴリのうちから適切なカテゴリを選択しその要求事項に従っていなければならない。

表３　カテゴリの概要

カテゴリ	要求事項
B	関連する規格に従い、基本的安全原則にしたがわなければならない。
1	十分吟味された構成部分及び十分吟味された安全原則を用いて設計，製造されなければならない。
2	安全機能が機械の制御システムによって適切な間隔でチェックされなければならない。
3	いずれの部分の単一の不具合（障害）も安全機能の喪失を招かない。合理的に実施可能な場合は常に単一 の不具合（障害）が検出される。
4	いずれの部分の単一の不具合（障害）も安全機能の喪失を招かない。かつ単一の不具合（障害）は， 安全機能に対する次の動作要求時，又はそれ以前に検出される。それが不可能な場合，不具合（障害）の蓄積が安全機能の喪失を招いてはならない。

5　むすび

安全性を確保するには、このための安全情報抽出の原理が存在し、また安全関連パラメータで要求される物理量を変換して安全情報とするためのしきい値演算とウィンドウズコンパレータの論理的構造を明らかにした。つぎに圧力伝送器の故障モードを考察し非対称故障モードとの整合性を示した。また国際規格 ISO13849-1が要求する安全の為の安全関連制御装置には５つのカテゴリが分類され、その要求に従うことが要求されていることを圧力伝送器の例にて示した。

参考文献

[1] 向殿政男編、蓬原弘一、“フォールト・トレラント・コンピューティング”、「安全性とフェールセーフ」丸善（株），1989-9 P199-202.

[2] 杉本・蓬原、安全の原理、機論56巻530号(1990-10)、P75-83

[3] ISO13849-1(JIS B 9705-1:2000) 機械類の安全性－制御システムの安全関連部－

[4] 岡村・寺尾、測定論I、岩波講座基礎工学11、1969

[5] 加藤・蓬原・向殿、フィードバックを含むフェールセーフシステムの一構成法、電子情報通信学会、時限研究会、S88-24 (1988-4)

[6] 白井稔人、蓬原弘一：保護装置の構成方法を表すための演算子の提案とその適用例、日本信頼性学会誌、Vol.24、No7(2002-10)l

（もりやま　てつ　/　ふつはら　こういち）