

4. 安全確認型システムの基本要件

安全確認型と危険検出型は安全状態を対象とするか危険状態を対象とするかの違いだけで、「なあんだ簡単なことではないか」と思われがちですが、確定的な安全を保証する安全確認型のシステムを構築するためには、下記の要件を満足させる必要があります。

A. 「**確実な安全状態**」が存在すること

注) ここでいう「確実な安全状態」とは、「被災ゼロ」だけでなく、「被災の程度が社会一般通念に照らして十分に小さい状態」を含みます。

B. 「確実な安全状態」を示す代表特性が存在すること

C. 「確実な安全状態」を示す代表特性を安全情報（エネルギー）として伝えることができること

D. 安全情報（エネルギー）を用いて機械あるいは作業の運転開始・継続を許可するシステムであること

以下、A～Dについて、個々に説明していきます。

(1) 「**確実な安全状態**」が存在すること

「この状態であれば確実に(100%)安全である」という「**確実な安全状態**」が存在しなければ、確定的な安全を保証することはできません。

「1. 確定的安全と確率的安全」の冒頭で述べたように、世の中には地震・雷のように人間がそのエネルギーをコントロールできないものが存在するため、どのように安全対策を講じても確実に(100%)安全を保証することは不可能です。

しかし、生産現場は一般社会とは異なり、エネルギーだけでなく、原材料、設備、またそれらを取り扱う人をコントロール(管理)することで物づくりを行っています(コントロールできないければ物づくりは行えない)。すなわち、生産現場であれば、工夫することで意図的に「**確実な安全状態**」を作ることができるのです。

生産現場における「**確実な安全状態**」には次のものがあります。

①危険源ではあるが、危険状態になるための条件が除去されている状態

(以下「**停止安全状態**」と称します。)

- ・危険源へのエネルギー供給が遮断され、危険源の保有する位置・運動・圧力・電気エネルギーが解放されてゼロになった状態（「ゼロメカニカル・ステート」と呼ばれます）

②カバーや安全柵などで危険源への曝露が完全に防止されている状態

(以下「**隔離安全状態**」と称します。)

③危険源は存在するが、曝露しても被災しない状態(以下「**許容安全状態**」と称します。)

- ・危険源の持つエネルギーが小さい状態
- ・接触したら怪我するような尖った角などが無い（丸い、平滑）、あるいは、挟まれても怪我しないようにクッション材が施工された状態

(2)「確実な安全状態」を示す代表特性が存在すること

生産現場は機械を動かしたり止めたりしながら物作りを行っているので、生産のステップに応じて上記(1)①～③に述べた「確実な安全状態」を、例えば「準備ステップ：停止安全状態」→「運転ステップ：隔離安全状態」→「製品取り出しステップ：停止安全状態」→「ワーク交換ステップ：許容安全状態」・・・といのように切り替える必要があります。この場合に重要なことは、次の2つです。

- ①次のステップが「確実な安全状態」になったことを確認した後でないと(図 4-1(1) 青点線)、現在の「確実な安全状態」を解除することができないようにする(図 4-1(1) 青矢印)。
- ②どのステップでも「確実な安全状態」が確保されていることを常に確認するとともに、確認できなくなった場合は、直ちに「停止安全状態」に移行することで(図 4-1(2) 赤矢印)「確実な安全状態」を確保する。

ステップ 安全状態	定常状態			非常状態	定常状態	
	準備	運転	製品取出し	ワーク変更	準備	運転
停止	停止安全		停止安全		停止安全状態	
隔離		隔離安全				隔離安全
許容				許容安全		

図 4-1(1) 定常状態、非常状態における安全状態の切り代わりタイミング

ステップ 安全状態	定常状態		異常	定常状態	
	原料供給	運転	故障・修理	運転(再開)	製品取出し
停止	停止安全		停止安全		停止安全状態
隔離		隔離安全		隔離安全	
許容					

図 4-1(2) 異常状態発生時及び修復後における安全状態の切り代わりタイミング

上記①においては、「次のステップが『確実な安全状態になった』」ことを確認して情報として伝える」、②においては「どのステップでも『確実な安全状態が確保(保持)されている』」ことを常に確認しながら情報として伝える」ということが必要となります。

「状態になった」とか「状態が確保(保持)されている」ということは、ある条件が満足されているということで、「確認する(確認できる)」ためには、この状態をエネルギーや情報の形に変えて伝えることが必要です(図 4-1(1)(2)の矢印)。また、間違いのない安全情報として伝わるためには、これらのエネルギーや情報は受ける側が識別できるものでなければなりません。

そのためには、まず、「確実な安全状態」を特定の機器(またはデバイス)の具体的な状態に変換して表すことが必要となります。ある特定の機器(またはデバイス)が「確実な

安全状態」を示す状態、それがここでいう代表特性で、この特性はエネルギーや情報の形に変換されて伝達されることになります。

「停止安全状態」「隔離安全状態」「許容安全状態」を示す具体的な代表特性は、採用するシステム、デバイスにより異なります。下記にそれらの例を示します。

「停止安全状態（危険状態になるための条件が除去されている状態）」を示す代表特性

いずれもゼロメカニカル・ステートになっていることを示す特性です。

〔例 1〕

電源供給回路のメインスイッチの接点が開（Open）になった状態

or メイン回路の電磁リレーが開（Open）になった状態

or メイン電源のコンセントを取り外した状態

かつ 惰性回転部の回転計の値がゼロの状態

かつ コンデンサーの電圧計の値がゼロの状態（保有する電荷を測定する計器の値がゼロの状態）

〔例 2〕

圧縮空気供給配管のメインバルブを閉にした状態

かつ 圧縮空気の大気開放バルブを開にした状態

かつ 圧縮空気系統の圧力計の指示値がゼロの状態

「隔離安全状態（危険源への曝露が完全に防止されている状態）」の代表特性

〔例〕

危険源の安全カバーや安全柵の入口扉を閉じて施錠した状態（ただし、危険領域に人の体が入るスペースがないものとする）

「許容安全状態（危険源に曝露しても被災しない状態）」の代表特性

〔例〕

挟み込まれる前に回転体が止まるように、回転トルクを下げた状態

なお、接触しても怪我するような尖った角などがない（丸い、平滑）な状態は、確定的な安全状態そのものであり、安全状態を検出して伝える必要性はありません（当然ながら検出のための代表特性は不要）

(3) 「確実な安全状態」を示す代表特性を安全情報（エネルギー）として伝えることができること

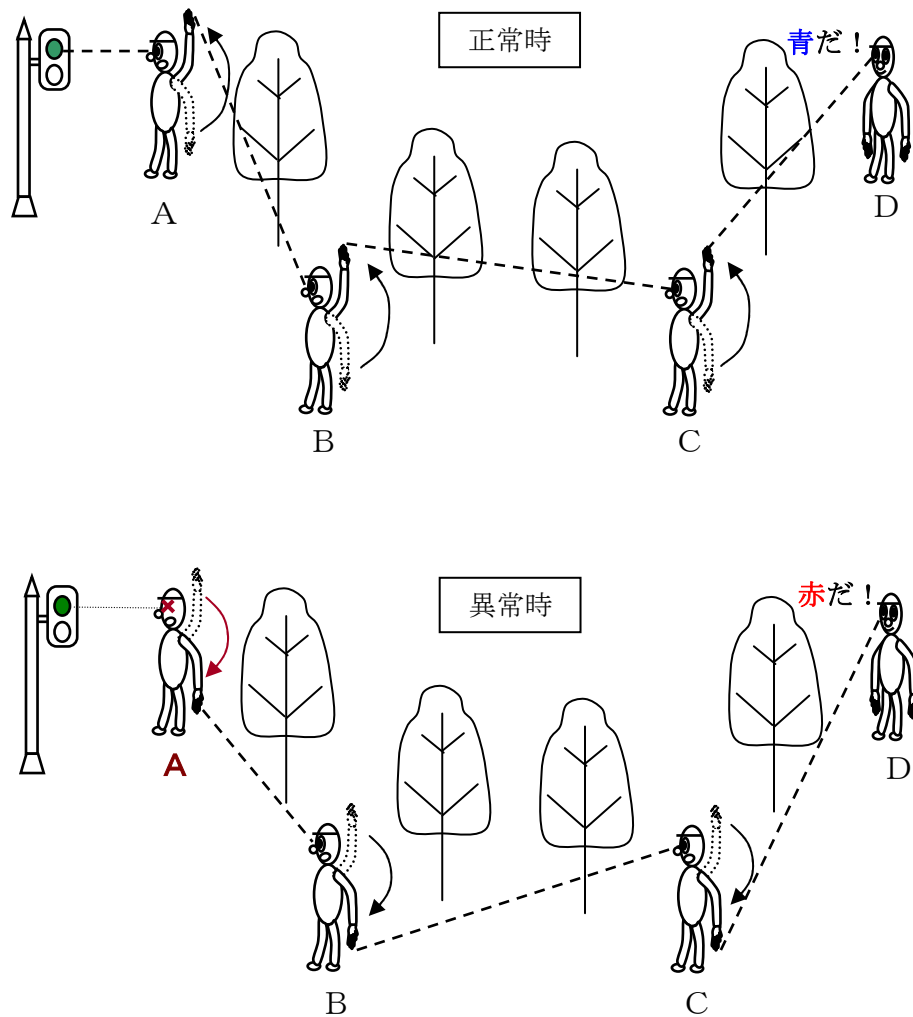
「確実な安全状態」を受ける側が検知して識別できるためには、代表特性をエネルギーまたは情報の形として伝達しなければなりません。この場合、エネルギーまたは情報のない場合を安全状態としたのでは、受ける側は本当の安全状態なのかそれとも故障したためにエネルギーまたは情報が来ないのかを識別することができません。すなわち安全情報は、

代表特性やそれを伝える機能が正常であることを常時確認しながらエネルギーまたは情報の形で伝えることが必要なのです。

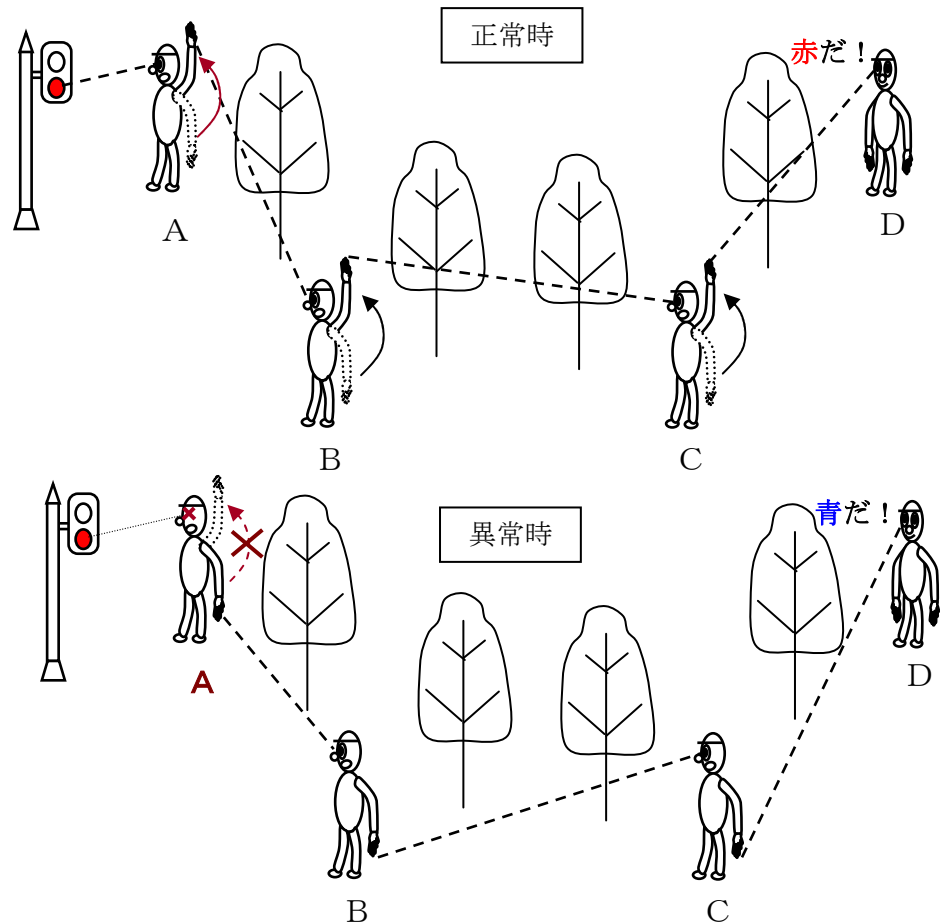
(危険検出型の場合は、「危険状態の証拠を確認」した時しかエネルギーまたは情報を伝えません。そのため、「危険状態の証拠を確認する」「危険情報を伝達する」という機能が正常であるかどうかは、危険状態になった時しか確認できません。すなわち危険情報が伝達されるかどうかは故障確率に依存しており確率的になります。)

[例]

下図のように、手を上げる（エネルギーを用いる）ことで青信号（安全情報）を伝えるやり方だと、例えばAの意識がなくなった（故障）した場合には手が下がります。すなわち手を上げていることは確かに意識がある（正常である）ことも伝えていきます。また、意識がなくなった（故障）した場合に手が下がると青信号（安全）なのに「赤（危険）」を伝えることになってしまいますが、これは安全側の誤りであり許されます。



これに対して下図のように、手を上げる（エネルギーを用いる）ことで赤信号（危険情報）を伝えるやり方だと、例えばAの意識がなくなった（故障）した場合には手を上げることができません。すなわち手を下げている状態は意識があるか（正常であるか）どうかを示していません。また、意識がなくなった（故障）した場合に手が下がり、赤信号（危険）なのに「青（安全）」を伝えることとなります。これは危険側の誤りであり絶対に許されません。



- (4) 安全情報（エネルギー）を用いて機械あるいは作業の運転開始・継続を許可するシステムであること

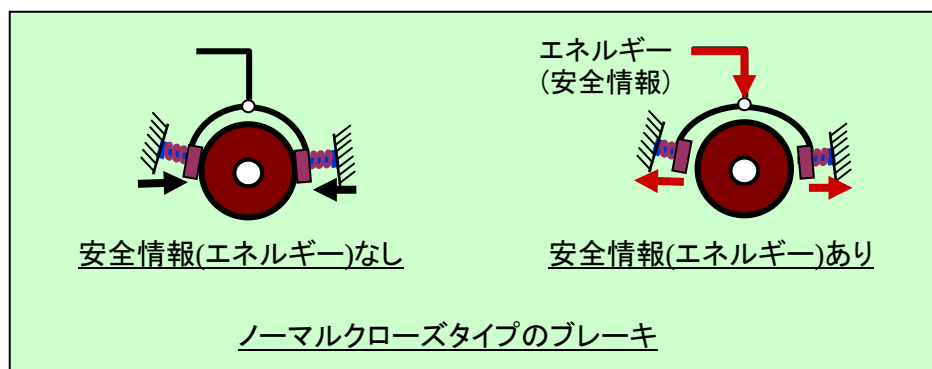
「安全情報（エネルギー）を用いて運転の開始を許可する」というのは、「安全情報を示すエネルギーで設備のブレーキ（ロック）を解除するとともに設備を駆動するためのエネルギーの供給路を開く（スイッチを入れる、バルブを開く）」ということ、「継続を許可する」というのは「安全情報を示すエネルギーでブレーキ（ロック）の解除状態と設備駆動エネルギーの供給路を開状態に保持する」ということです。このシステムであれば、安全情報が伝達されない時には（故障した場合を含む）、設備へのエネルギーが遮断されるとともにブレーキ（ロック）が作動するので直ちに停止状態、すなわち「確実な安全状態」へ移行します。

(駆動エネルギーが遮断されると瞬時に「確実な安全状態」へ移行するもの(例：電子レンジ)は、ブレーキ(ロック)は不要です。)

(危険検出型の場合は、「危険情報を示すエネルギーで設備を駆動するためのエネルギーの供給路を遮断(スイッチを切る、バルブを閉じる)するとともにエネルギーを供給して設備のブレーキ(ロック)を作動させる」ので、危険情報が伝達されない時には(故障した場合を含む)、設備が停止しない、すなわち「確実な安全状態」へ移行しません。)

[例]

下図のノーマルクロスタイプのブレーキは、常時バネ等でブレーキがかかった状態(ロック状態)にあり、安全を示す情報(エネルギー)でもってブレーキを解除する構造のため、安全情報(エネルギー)が供給されないときに直ちにブレーキが作動します。



これに対して下図のノーマルオープントタイプのブレーキは、常時バネ等でブレーキを解除した状態で危険を示す情報(エネルギー)でもってブレーキをさせる構造のため、危険情報(エネルギー)が供給されないときにブレーキが作動しません。

