５．安全確認型の構造

「４．安全確認型システムの基本要件」で“４つの要件”が必要であることを述べましたが、これだけでは理解しにくいと思います。

実際に現場で使用されている安全システムの多くは、「確実な安全状態」として「隔離安全状態」と「停止安全状態」を用いています。

・隔離安全状態…「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（Ｈ＝１＆Ｅ＝０）」

・停止安全状態…「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（Ｈ＝０）」

具体的には、安全状態を検知するためのデバイスとしてリミットスイッチまたは光センサを使用して安全回路（インタロック）を組んでいます。

そこで、ここではこのシステムを例にあげて、

① 通常のインタロックシステムではなぜだめなのか（どういう点が問題なのか）

② どうすれば①の問題は解決されるのか

③ ①②を踏まえ、どういう構造にしたら確定的に安全が確保されるのか（なぜ安全確認型システムとして“４つの要件”が必要なのか）

ということを説明したいと思います。説明は下記の順序で行います。

5.1. 「隔離安全状態」と「停止安全状態」を用いたインタロックシステム

5.2. 従来のインタロックシステム

5.2.1. リミットスイッチを使用したインタロックシステム

5.2.2. 光センサを使用したインタロックシステム

5.3. 従来のインタロックシステムの問題点

5.3.1. 問題点 1…機械そのものがエネルギーを保持している場合

5.3.2. 問題点 2…センサの故障

5.3.3. 問題点 3…判断システムの故障

5.4. 確定的安全の確保

5.4.1. 確定的安全を確保するための条件

5.4.2. 具体的な方策

5.5. 安全確認型とは

なお、以下に説明する技術内容は、国際安全規格　ISO 12100-1,2(JIS B 9700-1,2)に規定されているものでもあります。国際安全規格は、安全な機械を作るための「基本的な考え方」と「具体的な技術」を規定した膨大な体系で、確定的安全も確率的安全も含んでいます。安全確認型は規格の膨大な技術内容のうち、ガードといった安全防護、特にインタロックを用いた安全防護が確定的な安全を保証するためにはどうあるべきかについての論理(特に「安全情報の論理」)であるといえます。国際安全規格に述べられている技術とその思想を適切に解釈するためにも安全確認型の論理を理解することが必要である、と私は考えています。

石原立憲 Copyright Reserved

5.1 「隔離安全状態」と「停止安全状態」を用いたインタロックシステム

「隔離安全状態」を常時保つことができれば「確実な安全状態」を維持することができます。しかし現実の生産現場では、工程条件の変更など作業の都合上、隔離状態を解除して機械の可動部など危険源に近づく必要が生じます。この時、カバーや安全柵の一部に開口部(例えば入口扉)を設けて、そこから危険源に近づくことになります[1)]。このように隔離状態を解除して危険源に近づく場合には、一般に危険源への駆動エネルギー[2)]供給を遮断して（危険源が人にケガを与える能力を除去して）「停止安全状態」を作ってから危険源に近づくようにすれば安全を確保することができます。すなわち、なんらかの手法を用いて「隔離安全状態」と「停止安全状態」のいずれかの状態を常時確保することができれば「確実な安全状態」を確保することができます。

人は意識しないと物事を決めたとおりに実行できないし、意識は長続きしません。そのため「『隔離安全状態』と『停止安全状態』のいずれかの状態を確保する」ということは、人に任せるのでなく、なんらかの仕組みで行う必要があります。この仕組みをインタロックと呼び、例示すると図 5-1(a)(b)のようになります。

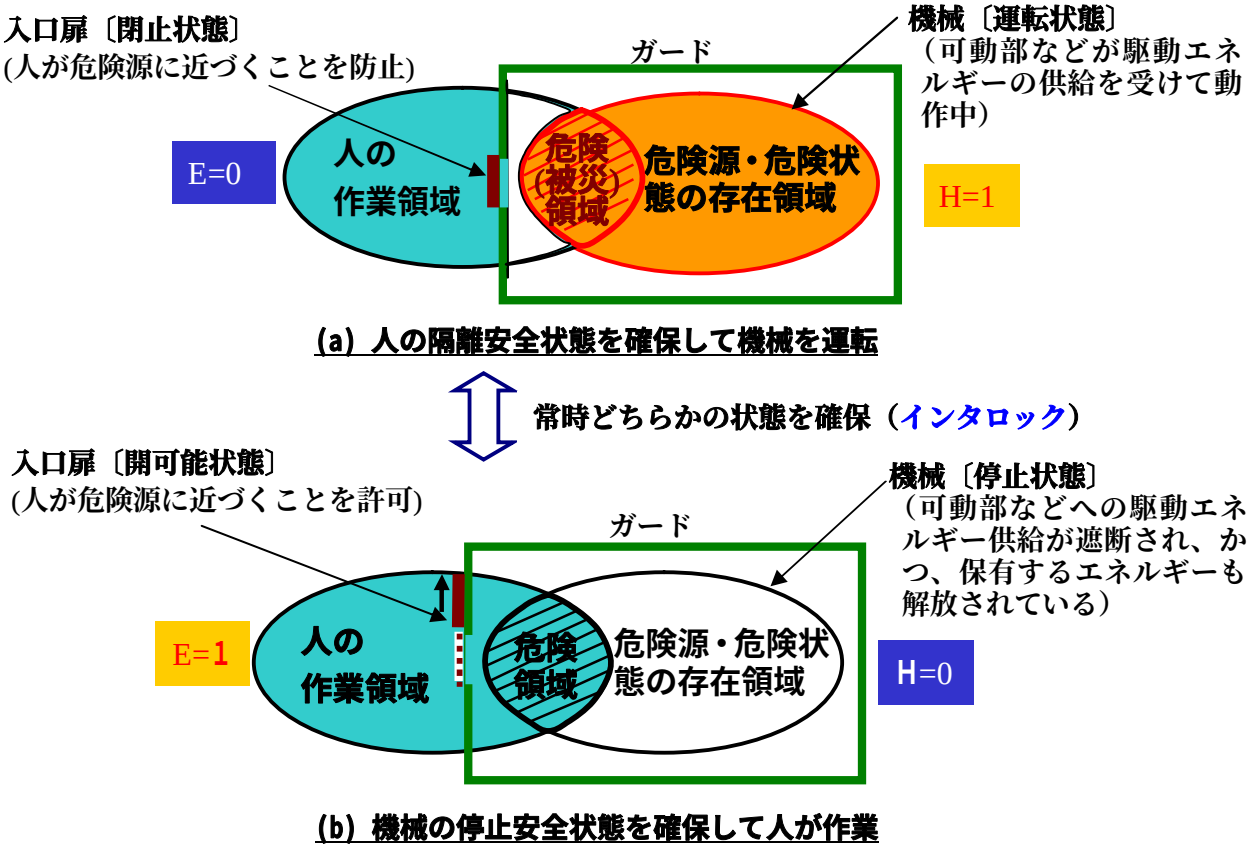


図 5-1　「隔離安全状態」と「停止安全状態」のインタロック

---

1) ここでは話を単純にするため、ガードで囲われた危険区域内には体の一部（例えば腕）しか入らないものとします（人がすっぽり入るスペースはないので、人が危険区域内に入った状態で扉を閉めることはできない、つまり入口扉が閉じた状態は隔離安全が作られた状態であると考えます）。

2) 機械を稼働させる、すなわち危険な状態にさせるエネルギーを指す。安全情報を伝達するためのエネルギー(本稿では情報伝達エネルギーと称す)とは異なります。エネルギーによる安全情報の伝達については「4.安全確認型システムの基本要件」をご参照ください。

石原立憲 Copyright Reserved

図 5-1 をブロック線図で表すと図 5-2 のようになります。

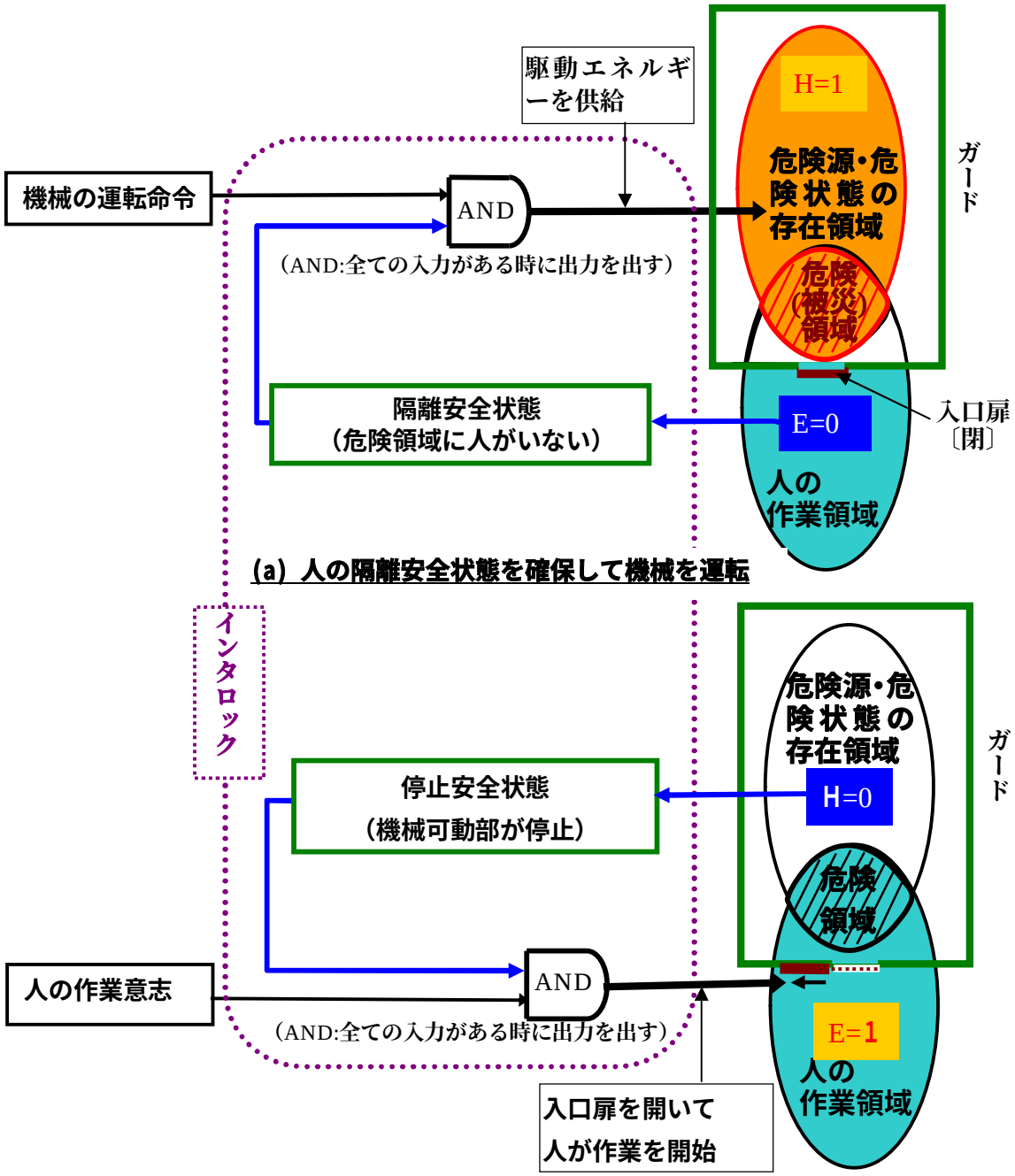


図 5-2　「隔離安全状態」と「停止安全状態」のインタロック

石原立憲 Copyright Reserved

5.2 従来のインタロックシステム

図 5-1、5-2 のような「隔離安全状態」と「停止安全状態」のいずれかの状態を常時作ることで安全状態を確保するシステムにおいては、一般にはカバーや安全柵の入口から人の体が入ろうとする状態（危険源に近づこうとする状態）をなんらかの手段で検知して、この情報を用いて機械の駆動エネルギーを遮断する（電磁接触器を切る、圧縮空気配管のバルブを閉じるなど）という安全方策が用いられます。この場合、よく用いられる安全方策には以下の２つがあります。

5.2.1. リミットスイッチを使用したインタロックシステム

入口扉にリミットスイッチを設置して、人が扉を開く（人の体が入口から入ろうとする）とリミットスイッチがＯＦＦとなり運転回路が遮断されて機械の運転が停止します（扉が閉まっている時にはリミットスイッチがＯＮとなり運転回路が操作できます）。

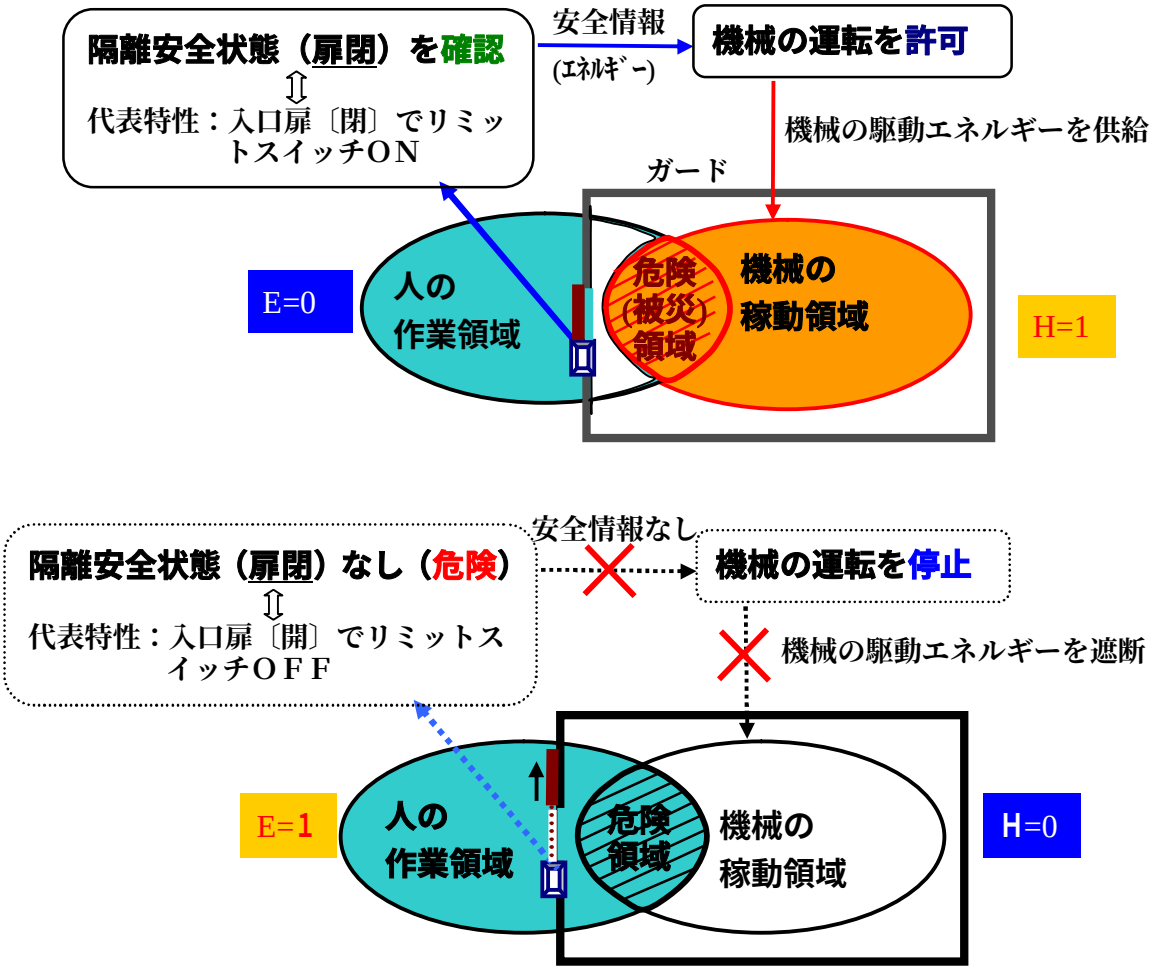


図 5-3　リミットスイッチを使用した「隔離安全状態」と「停止安全状態」のインタロック

石原立憲 Copyright Reserved

5.2.2 光センサを使用したインタロックシステム

入口に光センサを設置して、光センサが人を検知（人の体が入口を通るのを検知）した時に運転回路が遮断されて機械の運転が停止します（光センサが人の体を検知しない時には運転回路が操作できます）

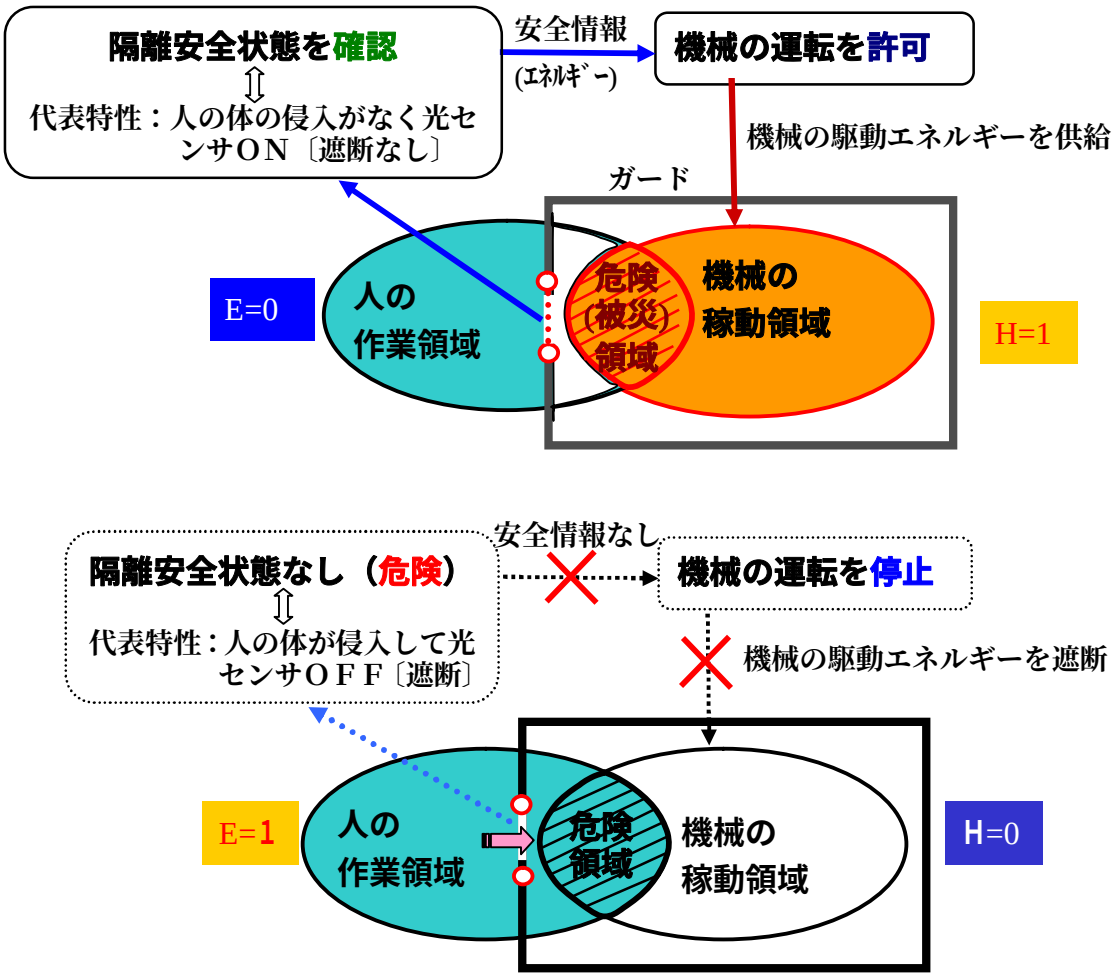


図 5-4　光センサを使用した「隔離安全状態」と「停止安全状態」のインタロック

石原立憲 Copyright Reserved

5.3 従来のインタロックシステムの問題点

図 5-3、5-4 を見る限り、一見問題のない安全なシステムに見えますが、これらの方式には以下の 5.3.1～5.3.3 に示すように「『隔離安全状態』あるいは『停止安全状態』のいずれかを常に確保する」ということができない場合があります。

5.3.1. 問題点 1…機械そのものがエネルギーを保持している場合

惰性回転のある機械のように機械そのものがエネルギー(例えば運動エネルギーとして、ポテンシャルエネルギーとして、電荷としてあるいは圧力として)を保持している場合、図 5-5 のようにリミットスイッチや光センサがＯＦＦになって駆動エネルギー供給を遮断しても直ちに停止状態にはなりません。この惰性回転中に入口から人が体を入れると被災します。

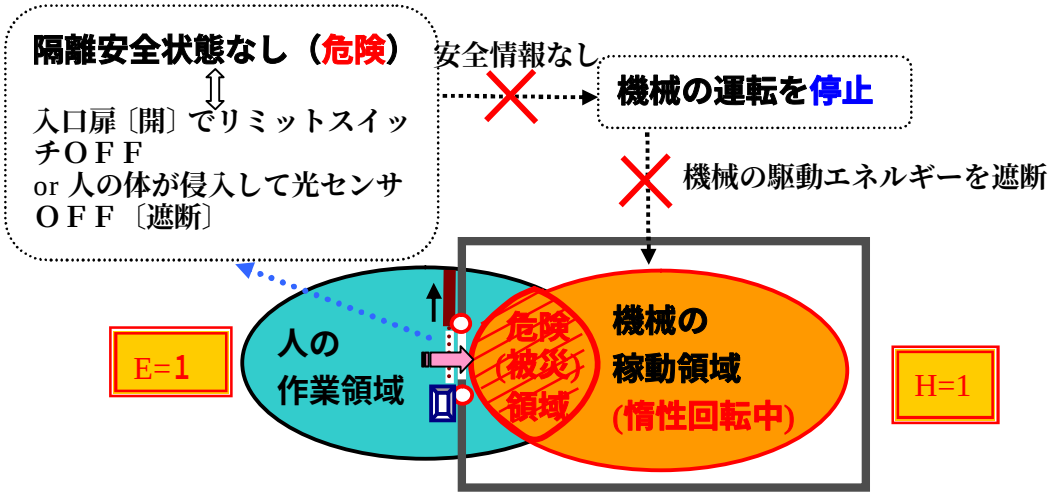


図 5-5　「停止安全状態」の未確立〔惰性回転系〕

これは停止安全状態（ゼロ・メカニカルステート）になっていないのに隔離安全状態を解除して危険区域に人が入れるということで、図 5-6 に示すブロック線図において、(a)の 「人の隔離安全状態を確保して機械を運転する」という手段はできているが、(b) の「機械の停止安全状態を確保して人が作業する」という手段が確立されてないことに起因しています。

石原立憲 Copyright Reserved

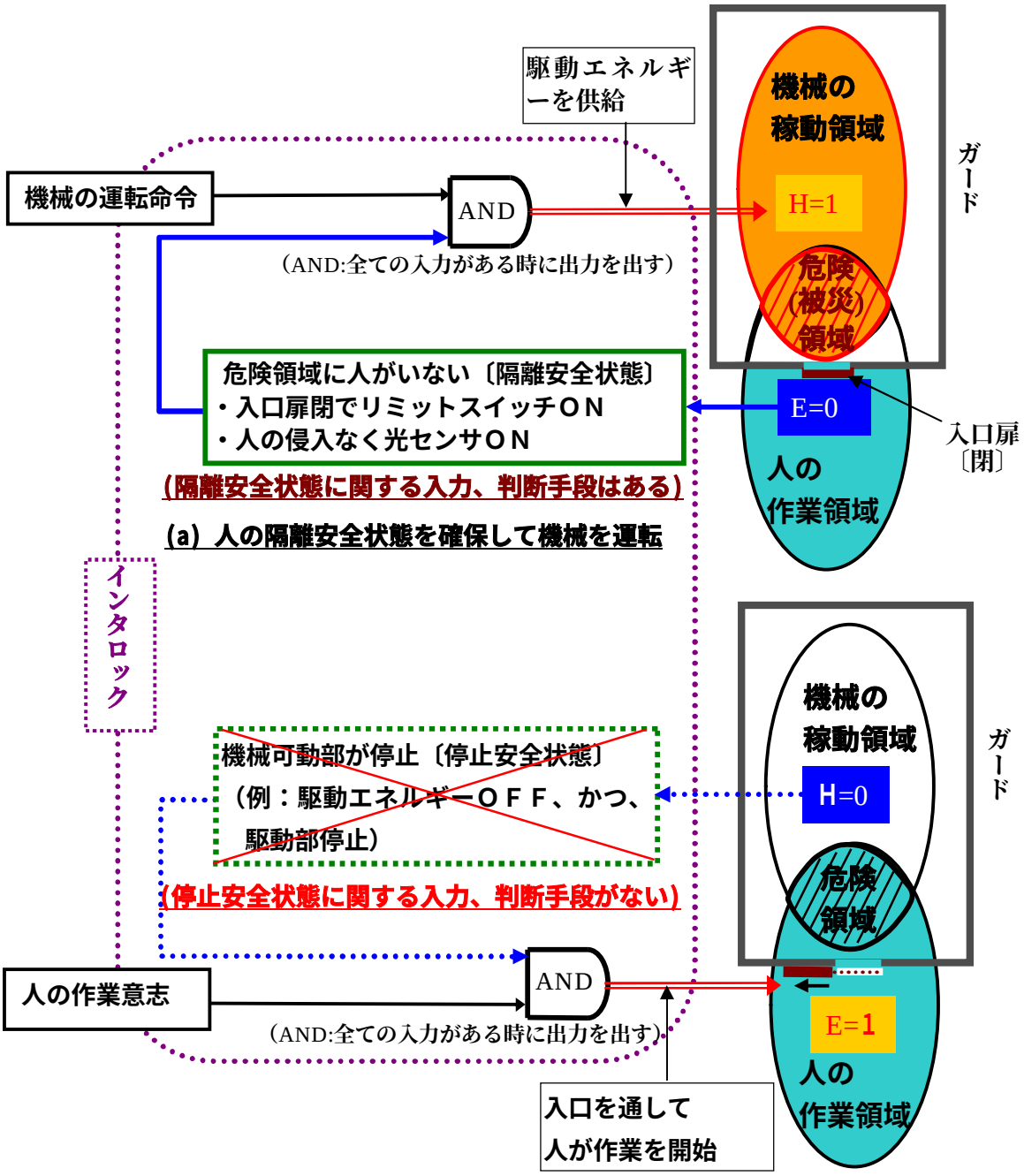


図 5-6　「隔離安全状態」のみの（「停止安全状態」のない）ブロック線図

石原立憲 Copyright Reserved

5.3.2. 問題点 2…センサの故障

リミットスイッチの接点が溶着（故障）すると安全情報が出続けるので、入口扉を開いても機械が停止しません。また、忙しい時には機械が停止しないようにリミットスイッチを道具やガムテープなどで ON 状態に固定して無効化されることもあります。

また、光センサの場合は、外部からの光が入る（誤作動する）と人の体が光センサを遮っても安全情報が出続けるので機械が停止しないことがあります。

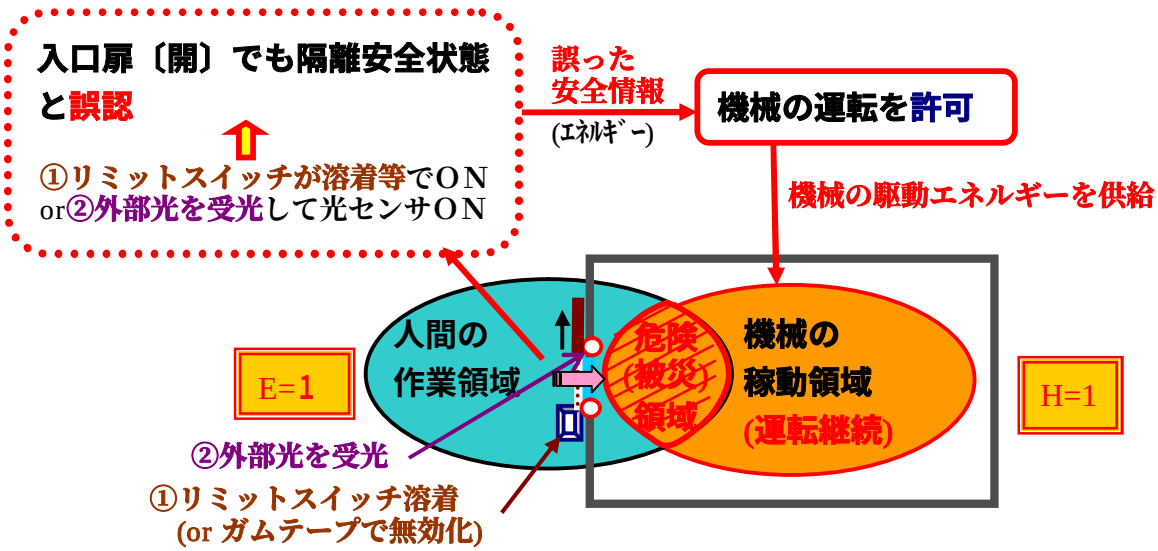


図 5-7　「停止安全状態」の非確立〔センサの故障・異常〕

これは〔隔離安全状態〕や〔停止安全状態〕を検知するセンサに故障や誤作動が生じても機械の運転や人が危険領域に入ることが許可されるということで、安全情報を検知する部品（デバイス）が故障や誤作動（故意の無効化を含む）を起こした場合には安全が確保されないシステムになってしまっていることを示しています。

石原立憲 Copyright Reserved

5.3.3. 問題点 3…判断システムの故障

安全情報を受けて機械の駆動エネルギーを供給したり停止したりする判断システム(コントロールシステム）が故障すると、図 5-8 のように安全情報の「あり」、「なし」に関係なく機械の運転が停止しない場合があります。

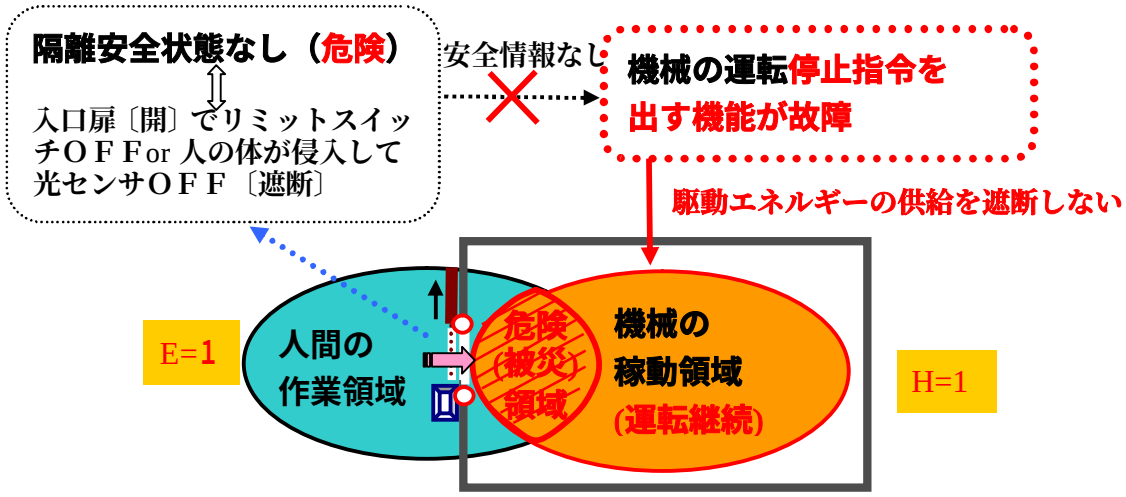


図 5-8　「停止安全状態」の非確立〔判断システムの故障〕

これは入力された情報を判断して機械の運転や人が危険領域に入ることを許可する判断システム（図 5-2、5-6 では【ＡＮＤ】部分）に故障や誤作動が生じたときに、機械の運転や人が被災領域に入ることが許可される場合があるということで、安全情報を判断する部品（デバイス）が故障や誤作動（故意の無効化を含む）を起こした場合には安全が確保されないシステムになってしまっていることを示しています。

5.3.1～5.3.3 のいずれも「停止安全状態が確保されてないのに隔離安全状態が解除される」場合がある、すなわち安全の確保が確率的であるというところに問題があります。

「ほんの少し問題があるだけではないか、ちょっと気をつければ被災を回避できるはずだ。」と思うかもしれませんが、人は安全システムで自分が守られていると思っている（信じている）かぎり、異常を見つけても異常と認識できないものです。そのため異常が生じても正常（安全）と思い込んで行動するので、安全システムの不備や故障による災害はヒヤリハットにならず重大災害になる可能性が高いのです。
また、現場作業者は時間に追われると、安全装置が働かないように細工（安全装置の無効化）をして作業を進めるようになりますが、この時には気が焦るために普段やらないミスを犯して災害に巻き込まれます。この手の災害事例が多いのは、日本だけでなく世界共通ですが、このような災害が起こった時に、起こした本人の不注意・業務違反として処理しながら「ゼロ災を目指せ！」と叱咤激励する従来の日本のやり方を続けている限り、ゼロ災害、特に重大災害の

石原立憲 Copyright Reserved

撲滅を図ることは不可能です。

5.4. 確定的安全の確保

5.4.1. 確定的安全を確保するための条件

ではどうすればよいのでしょう。安全システムを構成する部品（デバイス）の故障や誤作動も含めて、「隔離安全状態」あるいは「停止安全状態」のいずれかを常に確保しなければなりません。そのためには、安全システムは次の①～③に示す条件を満足する必要があります。

①停止安全状態が確保され、かつ、その状態が確認・維持されている条件下でなければ、人の体が危険区域に入ることを許可（隔離安全状態を解除）してはならない。

【対策】

「機械の可動部が確実に停止した状態（停止安全状態）を示す情報」を用いて、入口扉のロックを解除するとともに、ロックを解除したら（開錠したら）機械に駆動エネルギーを供給できないようにします。

なお、ここでいう「停止安全状態」とは、下記ａ．～ｃ．がすべて満足された状態をいいます。（内容がしつこいように見えますが、単独だと〔　〕内に記した問題をクリアできないためです。）

ａ．駆動部へのエネルギー供給が遮断されている（例えば「電源スイッチＯＦＦで電流計の値がゼロ」）

〔 電源スイッチをＯＦＦにしてもスイッチが溶着や短絡を起こすと実際には電流が遮断されない。〕

〔 電流計が断線すると実際には電流が流れていても電流指示値はゼロとなる。〕

ｂ．可動部が停止している（例えば「可動部の回転数がゼロ」）

ｃ．可動部がロックされている（例えば「可動部をブレーキでロック」）

〔 可動部をロックしておかないと、ちょっとした外部からの力で止まっていた機械が動くことがある。〕

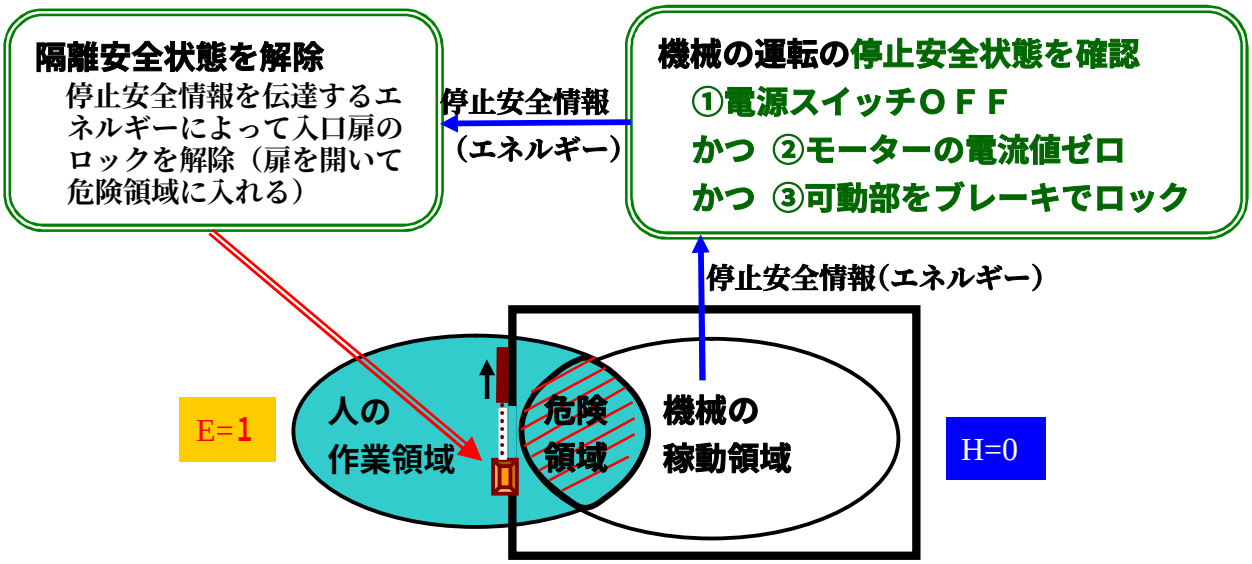


図 5-9　「停止安全状態の確認」による「隔離安全状態」の解除

石原立憲 Copyright Reserved

②隔離安全状態が確保され、かつ、その状態が確認・維持されている条件下でなければ、機械の運転を許可（停止安全状態を解除）してはならない。

【対策】

機械の可動部をロックできるようにブレーキを設置します(「４．安全確認型システムの基本要件」の P6 に記載している「ノーマルクローズタイプのブレーキ」を参照方)。

また、入口の扉にもロック機構を設け、入口扉を閉めてロックがかかった状態〔隔離安全状態〕を示す情報（例えば、センサ等で検知した信号）を伝達するエネルギーを用いて、機械可動部のブレーキのロック解除と駆動エネルギーの供給を許可するようにします。

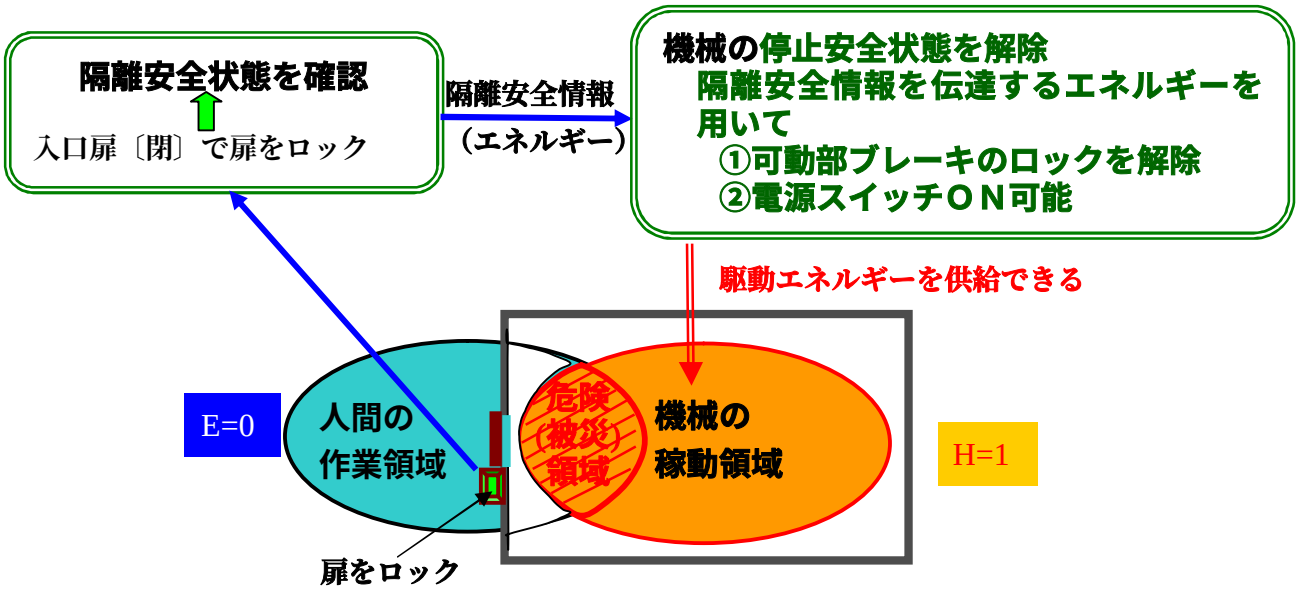
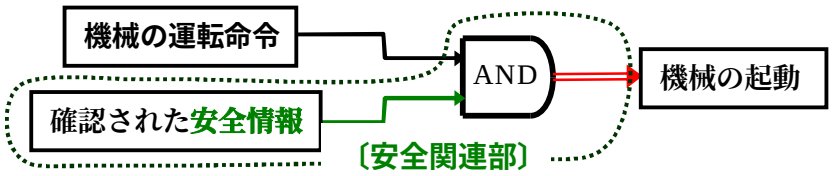


図 5-10　「隔離安全状態の確認」による「停止安全状態」の解除

③「隔離安全状態や停止安全状態を『確認する』という手段」および「機械の運転や人の体が危険区域に入ることを『許可する』という手段」が故障や誤作動を起こした場合にも、隔離安全状態あるいは停止安全状態のいずれかが確保されなければならない〔フェールセーフ〕。また、これらの手段は、故意の無効化を防止するものでなければならない。安全に関する情報を取り扱う経路（電気の場合は回路）をフェールセーフにするためには、下記の条件を満足させることが必要。

ａ．安全に関する情報を取り扱う経路（電気の場合は回路）は、他の情報を取り扱う経路と分離・独立させる。



石原立憲 Copyright Reserved

回路図で示すと下図のようになる。

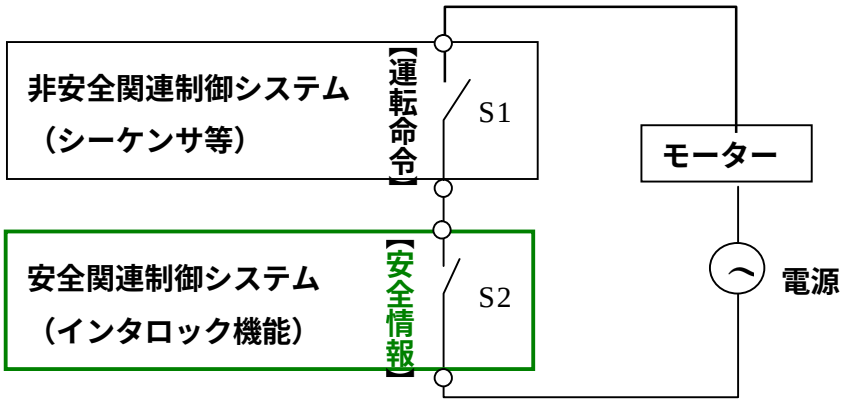


図 5-11 安全関連部と非安全関連部の分離

b．「隔離安全状態」「停止安全状態」を示す情報には高いエネルギー状態を用いる。
例えば、一定以上の「電流」または「電圧」がある場合を安全状態とする。（「電流」または「電圧」が一定以下というのは故障も含めて安全状態でない場合を示す。）

c．用いられるセンサやコントロールシステムが故障や誤作動を起こした場合には出力（エネルギー）が出ないようにする。
【この c.の条件を満たすには、非対称故障モードを有するコンポーネントの使用、構成要素間のポジティブな結合、ダイナミックな信号処理などが用いられますが、説明が複雑になるので省略します。関心のある方は、安全機器メーカーのカタログ等を見てください。】

石原立憲 Copyright Reserved

5.4.2. 具体的な方策

上記①～③の条件を満足する具体的な方策として、ソレノイド付安全スイッチを用いたシステムを下記(図 5-12a、b)に示します。この例は、P3 に示した「図 5-2　「隔離安全状態」と「停止安全状態」のインタロック」を具体的に表わしたものです。

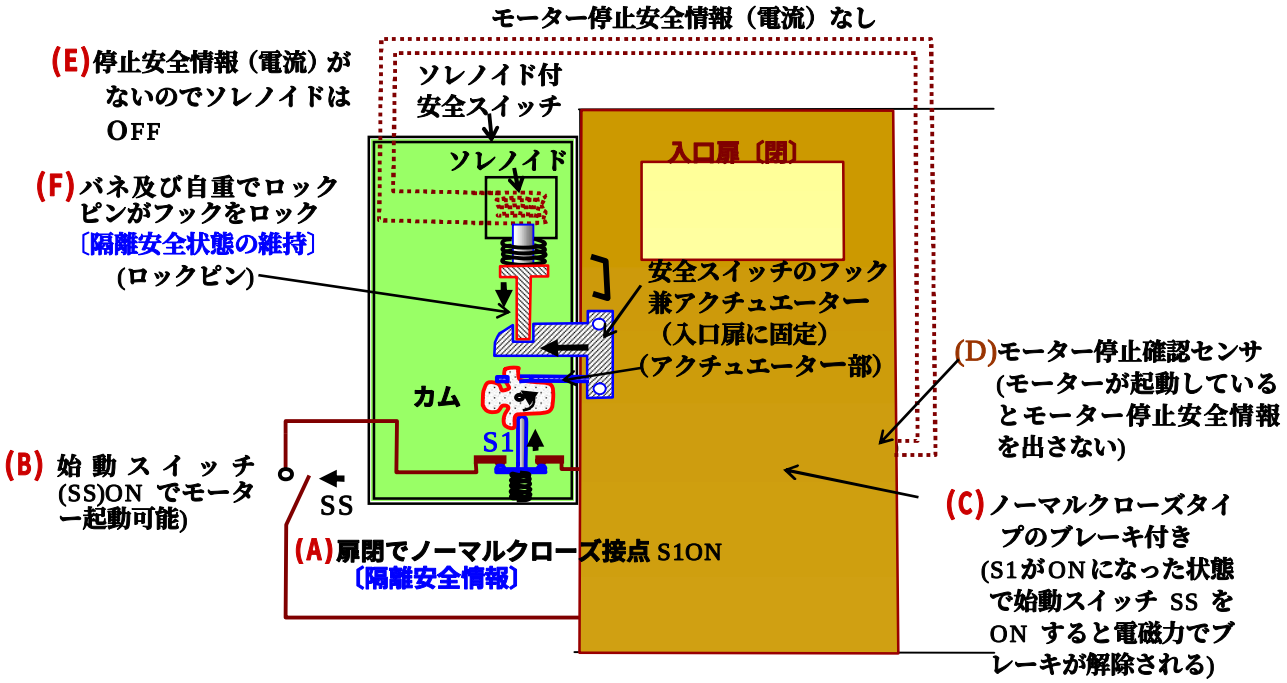


図 5-12a ソレノイド付安全スイッチを用いた仕組み
〔「隔離安全状態の確認」による「停止安全状態」の解除〕

【図 5-12a の説明】

- 回転するモーター等(危険源)が存在する危険領域の入口扉を閉める（隔離安全状態が成立する）と、扉に固定された安全スイッチのフック兼アクチュエーターのアクチュエーター部が安全スイッチのカムを回すので、バネの力でノーマルクローズ接点 S1(隔離安全情報)が ON となります(図中（A）)。
- ノーマルクローズ接点 S1 が ON の状態で始動スイッチ SS を ON すると(図中（B）)、電磁力でノーマルクローズタイプのブレーキが解除され(図中(C))モーターの起動が可能になります。
- モーターが起動すると、モーター停止確認センサからの停止安全情報(この場合は直流電流)がなくなるので(図中(D))、安全スイッチのソレノイドは OFF となります(図中(E))。これによりバネ及び自重でロックピンがフックをロックするので(図中(F)扉を開くことはできません（隔離安全状態の維持）[3]。

3)ロックピンが確かにフックをロックしているという隔離安全が維持されている情報を検知してモーター起動の条件に追加することも必要ですが、これを入れた回路図は複雑になるので、ここでは追加していません。

石原立憲 Copyright Reserved

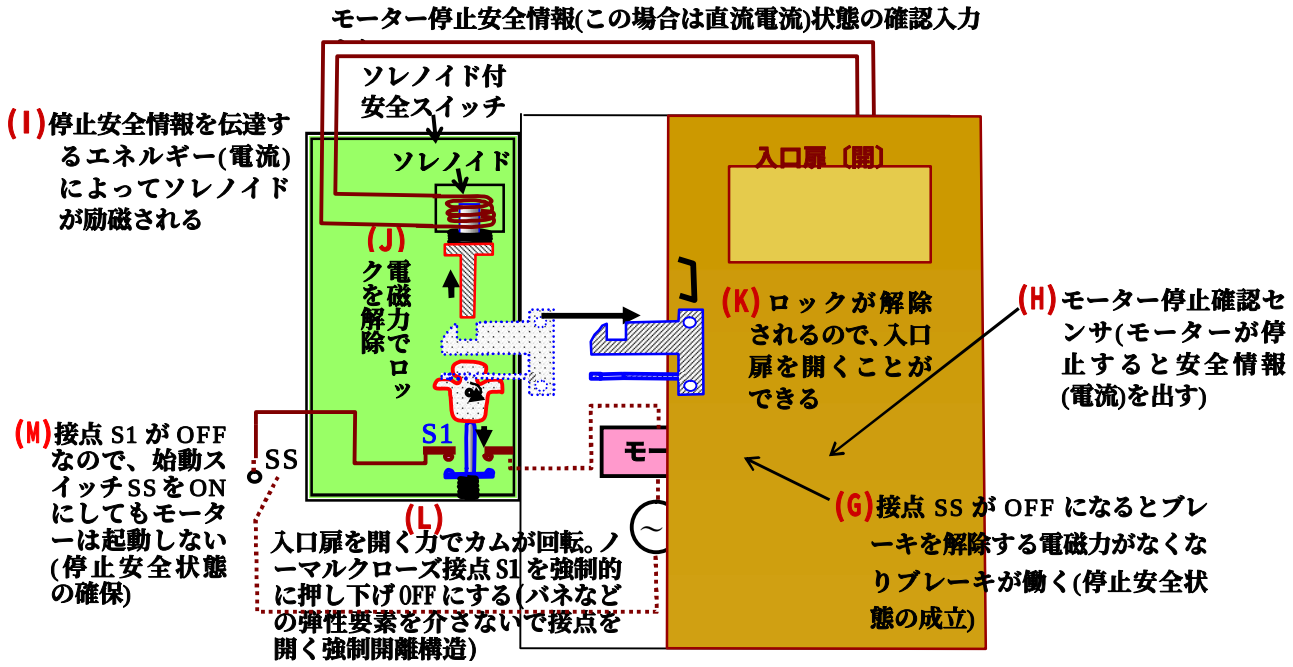


図 5-12 b ソレノイド付安全スイッチを用いた仕組み
〔「停止安全状態の確認」による「隔離安全状態」の解除〕

【図 5-12 b の説明】

・始動スイッチを OFF(接点 SS OFF)にすると、モーターのブレーキを解除する電磁力がなくなるのでブレーキが働き(図中(G))、モーターが停止(停止安全状態が成立)します。

・モーターが停止すると、モーター停止確認センサが停止安全情報(電流)を出すので(図中(H))、安全スイッチのソレノイドが励磁されます(図中(I))。

・ソレノイドの電磁力によってロックピンが引き上げられてロックが解除され(図中(J))、入口扉を開くことができるようになります(図中(K))。

・危険領域の入口扉が開くと、扉に固定された安全スイッチのフック兼アクチュエーターのアクチュエーター部が、安全スイッチのカムを回してノーマルクローズ接点 S1 を強制的に押し下げ OFF にします(図中(L))。

・接点 S1 が開いているので、始動スイッチ SS を ON にしてもモーターを起動させることはできません(図中(M))。またブレーキは働いたままです(図(G))。

5.5. 安全確認型とは

確定的安全状態を作り出すためには、「5.4.1. 確定的安全を確保するための条件」の①～③に示す条件を満足する必要がありますが、要約すると下記のシステムということになります。

「確実な安全状態が存在しており、その状態が維持されていることを示す安全情報（エネルギー）が確認されるときだけ機械の運転または人の作業を許可するシステム」

・「安全情報（エネルギー）が確認される」ということは、「隔離安全状態あるいは停止安全状態のいずれかの安全状態にある」ことを示す。

石原立憲 Copyright Reserved

・「安全情報（エネルギー）が確認される」ということは、「安全状態を検知する、あるいは判断するシステムが正常に機能している」ということを示す。
・「安全情報（エネルギー）が確認できない(安全状態を確認する手段、または機械の運転や人の作業を許可する手段が故障(故意の無効化を含む)している)」場合であっても、「隔離安全状態あるいは停止安全状態のいずれかが常に保持されている(隔離安全状態および停止安全状態の両方が同時に解除されることがない)」。

これが安全確認型システムの定義**「人と機械の共存システムにおいて、人の安全が確認されているときだけ、その機械装置やシステムの運転開始または継続を許可する構成を持つタイプ」**の意味です。

(これに対して、危険検出型システムの定義は「人と機械の共存システムにおいて、人の危険が確認されたときだけ、その機械装置やシステムの運転開始または継続を禁止する構成を持つタイプ」と定義されます。)

また、安全確認型の構造を作るための条件を要約すると下記のようになります。

①「隔離安全（Ｅ＝０）」「停止安全（Ｈ＝０）」といった確定的安全状態を組み合わせる〔「インタロック構造」をとる〕ことにより常に確定的安全状態を確保する。

②「安全情報を検知・伝達する」「伝達された安全情報で運転を許可する」という機能における安全情報には、高いエネルギー状態を用いることで、安全情報だけでなく機能が正常であることを伝える。

③上記②の機能が故障したら、安全情報が高エネルギーの状態からに低い状態（エネルギーゼロの状態）になり、これにより直ちに危険源へのエネルギー供給が遮断されて停止安全へ移行するといった「フェールセーフ機能」を有する。また、惰性回転のように危険源が残存エネルギーを保有する場合は、残存エネルギーがなくなるまで扉が閉のままロックされて隔離安全が保持される。
（瞬時に「停止安全」に移行して曝露しても被災しない場合は、扉のロック機能は不要）

石原立憲 Copyright Reserved