Specific Research Reports of the National Institute
of Industrial Safety, NIIS-SRR-NO.16 (1996)
UDC 62-783:164:331.054

7. 自動倉庫における危険領域防護システムの論理的考察

深谷 潔*, 粂川 壮一*, 梅崎 重夫*

7. Logical Study on Danger Zone Guard System in Automated Warehouses

by Kiyoshi FUKAYA*, Soichi KUMEKAWA* and Sigeo UMEZAKI*

Abstract; Safety measures were analyzed logically from the standpoint of protection against a danger zone. In this analysis an accident is represented logically by coexistence of a man and a machine. Consequently basic principle of safety measures is a spatial or temporal separation of a man and a machine. Spatial separation means a division of the space into a danger zone in which machinery moves and a safety zone in which men exist. Temporal separation means stop of machinery during men's existence in the danger zone. To control separation, an interlock structure is needed. There are two type of interlock. One is an interlock to human and another is an interlock to machine. If there is no time delay in control system, either interlock can realize the separation. But there is a time delay in any control system and it must be compensated in control structure. There are two methods of compensation. One is "the confirmation precedence method" in which both type of interlock structure are applied, that is, a human entrance into the danger zone is permitted after confirming stop of the machine and start of machine operation is permitted after nobody's existence in the danger zone. Another is "the prediction method" in which a human approach to the danger zone is predicted and a machine is stopped. This method is an enhancement of an interlock to machine and control is based not only on the human existence in the danger zone but also on the prediction of human existence. Therefore certainty of the prediction and of control, especially stop control of machine, is needed.

In an automatic warehouse the prediction methods can not be applied, because an emergency stop of a stacker crane may cause other accidents such as fall of loads. Furthermore, aged workers in Japan have the tendency to avoid a stop of a machine, and they often overcome the safety device to enter the danger zone without stopping the machine. Consequently the confirmation precedence method should be applied. To prevent men from entering the danger zone, the safe guards must surround thoroughly the danger zone including the opening for loads and it was moved to 2nd floor level out of human space. To permit a man to enter the danger zone a door with lock was used and a man must wait the unlock of the door until the stacker crane stops.

The guard system against danger zone with entrance door lock is necessary for the machinery in which emergency stop is not preferable.

Keywords; Safety measures , Danger zone, Aged worker, Automated warehouse

1. はじめに

危険な機械に対する防護の形態として従来広く用いられているのは，機械の危険部に対するカバーか，人間が接近するなど危険なときには機械を停止するというものである。「他の形態があるのか？」と言われるくらい，安全対策としては当然の形態と考えられてきた。

後者の形態においては，非常停止装置を設置し作業者

*機械システム安全研究部 Mechanical and System Safety Research Division

が異常を検知したときに機械を停止させたり，機械の動作領域などの危険領域の手前に光線式安全装置や安全マット等の安全装置を設置し，作業者が危険領域に入ろうとするときそれを検知して機械を停止させたりしている。安全装置があるから安全が保たれると単純に考える人もいるが，現実には安全装置がありながら事故となる例は少なくない。その理由は，1つには安全装置の故障などの設備的要因にあり，1つには次に述べる人間側の要因にある。例えば，特に高齢者に顕著に見られることであるが，作業者が仕事に対する責任感が強く機械を停止することを嫌がる傾向があり，そのため，異常の処理を機械を停止しないでしようとしたり，安全装置を迂回して危険領域に進入することなどが挙げられる。

このように，「危ないときには機械を停止する（以下，安全停止* 方式と呼ぶ。）」という形態では，安全装置より賢く，作業に対する意欲の高い中高齢作業者等の熟練作業者の不安全行動には必ずしも対処できない。そのため，もっと直接的に作業者の行動を規制する安全対策が必要となる。そのような形態として，「作業者の危険領域への進入は，機械が停止する等の安全が確認されて初めて可能になる（以下，進入防止方式と呼ぶ。）」という方式が考えられる。

従来，安全を論理的に追究する研究がなされてきたが，これは安全停止方式の観点からの論理構造の研究[1)2)3)]や，それを実現するための技術であるフェールセーフについての研究で，進入防止方式の論理的意味については十分な追究がなされていない。そのため，本研究においては，機械の安全防護の基本について論理的に考察し，進入防止方式の必要性を明らかにし，自動倉庫を例にとり具体的な安全対策の論理的構造について述べる。

また，これらの論理的研究は，作業者の能力によらず事故を防止できる設備的な安全対策を行うための基本的要件を明らかにするためのものであり，また，それができない場合でも作業者に依存すべき箇所をできる限り限定し，その箇所を明確にすることで作業者の負担を軽減しようとしていると思われる。そのため，論理的研究においては，本来は年齢などの人間的要因は直接の関係はない。二次的に，到達距離に基づく安全ガードの要件の決定[5)]，作業者に依存する部分や，安全対策を行った場合の作業性などの問題では人間特性が関係する。これらのうち，高齢者の行動特性と機械の安全防護の形態の関連について考察する。

*安全停止従来は緊急停止とも呼ばれていたが，異常時に安全装置によって緊急に機械を停止させること。産業用ロボットに関するISO規格[4)]等ではこの用語が使用されているので，それに習った。

2. 事故と安全対策の論理モデル

2.1 事故防止の基本構造

一般に機械による事故は，動作中の機械と人間の接触によって発生すると考えられるが，これは人間と機械が同一時刻，同一位置に存在することとモデル化できる。これを論理式で表せば，

$$H(t,x)\cdot M(t,x)=1 \qquad \exists\, t,\ x \tag{1}$$

となる。ただし，・は論理積を示し，$H(t,x)$ は人間が時刻 t，位置 x にいることを示す論理変数であり，1が存在，0が不在を示す。また，$M(t,x)$ は機械が時刻 t，場所 x で動作していることを示す論理変数であり，1が動作，0が停止ないし不在を示す。また，$\exists$ は存在を示す。従って，(1) 式は，ある時刻にある場所において $H\cdot M=1$ となることを示している。

事故が発生しないためには，(1) 式を否定した，

$$H(t,x)\cdot M(t,x)=0 \qquad \forall\, t,\ x \tag{2}$$

でなければならない。ここで，$\forall$ はすべてということを示し，従って (2) 式はあらゆる時刻にあらゆる場所で $H\cdot M=0$ となることを意味する。事故防止のための安全対策は何らかの意味でこの式を成り立たせる条件を作り出すものと考えられる。

2.2 領域への拡張

2.1 節においては，論理変数は時間及び空間の一点において定義されている。しかし，安全対策は (2) 式が成り立つように制御を行うものであるが，空間の各点において論理値を制御することは非常に手間がかかり実現が困難である。現実には，空間を領域分割し，その領域単位で論理値の制御を行うことが多い。そのため，論理変数を領域を対象とするものに拡張する。この場合，位置を示す変数 x の代わりに領域を示す変数 X で置き換えることが自然である。ただし，そこでは式が意味するものは若干異なってくる。例えば，

$$M(t,X)=1$$

は，領域 X で機械が稼働状態にあることを意味するが，領域 X 内のあらゆる場所で機械が稼働しているというわけではない。機械の大きさが X より小さい場合には領域 X 内に機械が占有していない空間が存在することは明らかである。従って，この式は

$$\exists x_0 \in X,\quad M(t,x_0)=1$$

と解釈することが自然である。すなわち，領域 Xに属するある x_0 において $M=1$ である。一方，

$$M(t,X)=0$$

については，

$$\forall x_0 \in X, \quad M(t,x_0)=0$$

と解釈することが妥当である。すなわち，領域 X に属するあらゆる x_0 において $M=0$ である。このように，定義するものとすれば，

$$M(t,X)\cdot H(t,X)=0 \quad \forall t,x \qquad (2')$$

であれば，(2) 式が成り立つ。以後，(2) 式の代わりに (2') 式を用いる。

なお，同様に時間的区間 T に対しても $M(T,X)$ などが定義できる。

2.3 時間または空間的な領域の分離

ところで，安全対策を考える場合には，機械は動作していて（ただし，緊急時に停止してもよい），どこかに人間がいるということが前提である。これを論理式で示すと，

$$M(t,x)=1 \quad \exists t,\ x \qquad (3.1)$$
$$H(t,x)=1 \quad \forall t,\ \exists x \qquad (3.2)$$

となる。(3.1) 式は，機械が停止することもあるという条件で運転されていることを意味し，(3.2) 式は人間が必ずどこかにいるということを意味する。

この条件の下で (2') 式を満たす状態を考える。

まず，機械が動作している場合について検討する。時刻を t_0 とし，機械が動作している領域を X とすると，

$$M(t_0,X)=1 \qquad (4.1)$$
$$M(t_0,X^C)=0 \qquad (4.2)$$

となるので，(2') 式を満たすためには，

$$H(t_0,X)=0 \qquad (4.3)$$

でなければならない。一方，(3.2) 式より，

$$H(t_0,X^C)=1 \qquad (4.4)$$

である。ただし，X^C は X 以外の領域を示す。

(4.1)〜(4.4) 式は事故防止の条件 (2') 式を満たす 1 つの状態であるが，これらの式は，機械の運転中のある時刻 t_0 について見れば，人間と機械は別の領域にいなければならないことを示す。このように，人間と機械が別の領域に属する場合には事故にはならないが，機械の動作する危険領域と人間がいてもよい人間領域に分けることが，安全対策の基本である。この空間分離による安全防護の方法を「隔離の原則」と呼ぶことにする。

作業の種類によっては，人間が機械の動作領域に入ることがあるが，次にこの場合について検討する。時刻を t_1とし，このときの状態を式で表すと，

$$H(t_1,X)=1 \qquad (5.1)$$
$$H(t_1,X^C)=0 \qquad (5.2)$$

となるが，(2') 式を満たすためには，

$$M(t_1,X)=0 \qquad (5.3)$$

すなわち，機械を停止することが必要である。一方，(4.1) 式に示すように，t_1 とは別の時刻 t_0 についてみれば，$M=1$ である。(5.1) 式と (4.1) 式の関係は，機械の動作領域 X において見れば，人間と機械は時間的に分離されていなければならない，すなわち，交代で作業しなければならないということを意味する。この時間分離による安全防護の方法を「停止の原則」と呼ぶことにする。

以上の考察から，人間と機械が同一時刻同一位置にいてはいけないという (2') 式の意味するものは，人間と機械を空間的あるいは時間的に分離しなければならないということであることが明らかになった。この空間分離，時間分離は，必ずしも全く別のものではなく，安全対策の別の側面である。このうち，空間分離は機械を運転す

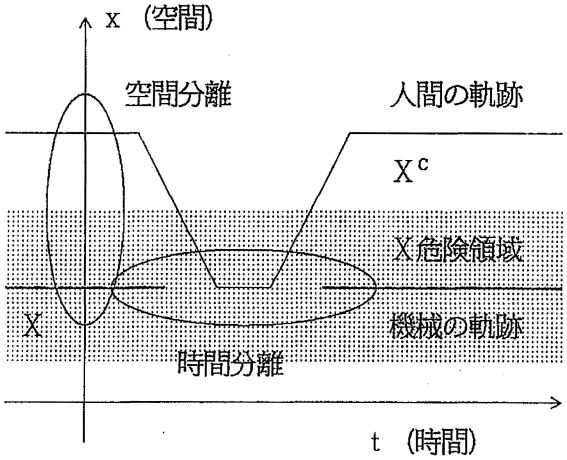


Fig. 1 Spatial separation and temporal separation.
時間分離と空間分離

Table 1　Examples of various form of interlock.
各種のインターロックの形態の例

		制御対象	
		人間	機械
制御主体	人間	危険回避行動	非常停止
	機械	安全ガード 自動ガード*	安全停止

* 機械の動作開始時に人間を危険領域から排除するガード

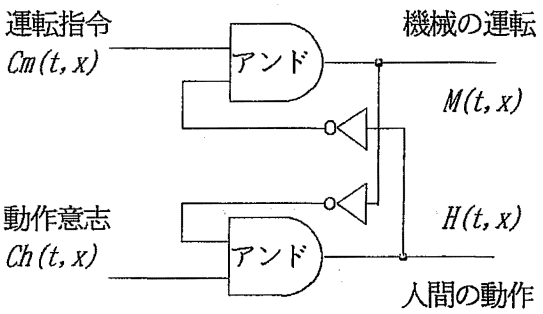


Fig. 2　Mutual interlock.
相互インターロック

る場合の正常状態*であり，時間分離は機械の動作領域で人間が作業を行う場合の安全状態**である。機械の運転のためには，自動運転モードのほかに，保守点検や修理等の人間の作業のモードが必要であり，空間分離と時間分離は，それぞれの場合における安全防護の形態である。また，時間分離は，空間分離が破れたときの防護になっている。この関係については，具体例に基づき詳述する。

2.4 インターロック構造

2.3 節では 2 つの安全な状態について考察したが，本節では，この状態を如何に実現するか，すなわち，どのように制御を行うかについて考察する。

(2') 式を実現するには 2 つの形態が考えられる。すなわち，人間の状態 H を見て機械 M を制御する「機械に対するインターロック」の形態と，機械の状態 M を見て人間の行動 H を制限する「人間に対するインターロック」の形態である。これらは，次の 2 つの論理式で表される[6]。

$$M(t,X) = \overline{H}(t,X) \cdot Cm(t,X) \tag{6}$$

$$H(t,X) = \overline{M}(t,X) \cdot Ch(t,X) \tag{7}$$

ただし，$\overline{\ }$は否定を示し，Cm, Ch はそれぞれ機械に対する運転指令または人間の動作意志を示す論理変数である。ここで，否定のついた $\overline{H}$ は人がいないという機械の運転 M に対する正常状態を意味し，一方 $\overline{M}$ は，機械が停止しているという人間の行動 H に対する安全状態を意味する。すなわち，(6) 式は正常を，また (7) 式は安全を確認しつつ作業を行うことを示す。

この論理式，例えば (6) 式は，人間がいない $(\overline{H}=1)$ から指令 $(Cm=1)$ に基づき機械を運転する $(M=1)$，或いは，スタッカクレーンのような移動機械においては，人間がいないからそこに移動する $(M=1)$ 等の制御や，逆に，人が来た $(\overline{H}=0)$ から機械を停止する $(M=0)$ 等の制御を意味する。

インターロックは，制御の対象と誰が制御を行うかによって **Table 1** に示す 4 つの形態に分けられる。

このうち，人間が制御する形態は，人間の注意力に依存するものであり，正常時には (6) 式又は (7) 式を満たすがこれらの式から逸脱する失敗もするので，事故は免れえない。(6) 式及び (7) 式は，人間と機械が相互に相手の状態を見て行動あるいは運転状態を制御する相互インターロックの形態である。これを **Fig. 2** に示す。

現実の安全システムは，この相互インターロックの形態を示す。しかし，理想化されたこのモデルの範囲内では，相互ではなくこの (6) 式または (7) 式のいずれか一方のインターロックの制御のみで，(2') 式を満たすことができる。それにもかかわらず，相互インターロックの形態とするのは，後述するように制御の遅れが存在し，どちらか一方のみでは (2') 式を満たせないためである。

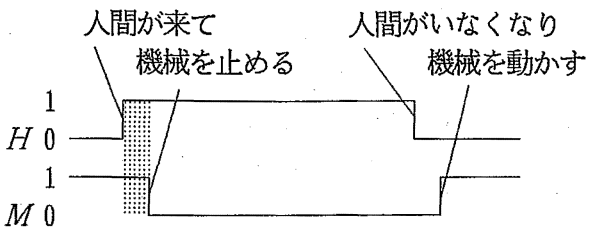
2.5 制御における時間遅れ

(6) 式及び (7) 式は，(2') 式を満たす制御方式を論理式で表したものであるが，これは理想的状況におけるものであり，現実の制御においては，修正が必要である。まず，修正しないでこれらの式をそのまま制御に適用した場合の結果について以下に示す。

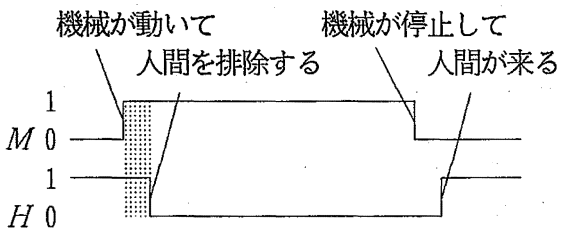
人間の状態 H を見て機械の運転状態 M を制御しようとする場合，一般には，M を直接操作することはできず，M に対する指令を変更することで行う。このことは (6) 式に基づく制御において，M が制御の結果ではなく制御の目標値であることを意味する。そのことを示すため M に目標値であることを示す ^ を付けると，この制御は，次のようになる。

---

* 正常　危険な機械を運転しているが事故のない状態
**安全　危険な機械が停止していて機械の動力による事故の起こりえない状態
　従来筆者らはそれぞれ合目的安全，無条件安全と呼んでいた[2]が，安全に関連する用語の厳密な定義づけを試みていて，このような用語の区別を行っている。



Hを監視して，Mを制御する(9) の場合



Mを監視して，Hを制御する(10)の場合

Fig. 3 Timing chart of interlock control.
インターロック制御のタイミングチャート

$$\widehat{M}(t,X) = \overline{H}(t,X) \cdot Cm(t,X) \qquad (6')$$

H についても同様に次のようになる。

$$\widehat{H}(t,X) = \overline{M}(t,X) \cdot Ch(t,X) \qquad (7')$$

ところで，制御においては一般に目標値と出力の関係は，時間遅れやゲイン (比例係数) で関係付けられる。ここで M が論理変数であることを考えると，ゲインは意味がなく時間遅れのみが意味を持つと考えられる。従って，これを Δt の時間遅れとして表現すると，

$$M(t+\Delta t, X) = \widehat{M}(t,X) \qquad (8)$$

となる。従って，H と M の関係は，(6') と (8) 式から，

$$M(t+\Delta t, X) = \overline{H}(t,X) \cdot Cm(t,X) \qquad (9)$$

となる。H についても同様な議論が成り立ち，

$$H(t+\Delta t, X) = \overline{H}(t,X) \cdot Ch(t,X) \qquad (10)$$

となる。$Cm = Ch = 1$ として，H と M のタイミングチャートを書くと，**Fig. 3** となる。いずれの場合も，監視対象が 0 から 1 になるときに $H \cdot M = 1$ (図の網線部) になり，式 (2') を満たさない。

2.6 制御方式の修正

時間遅れを考慮した場合には，制御方式 (6') または (7') のいずれも，安全条件 (2') を満たさない。これは，時間遅れのために (6) 式及び (7) 式が実現できないためである。(6) 式及び (7) 式は，(2') 式より論理的に導かれた式であり，(2') 式を満たす制御はこのいずれかしかないので，これを基にして時間遅れの影響を考慮して修正することが必要である。

時間遅れを考えたときに (2') 式を満たせなくなるのは，状態が変化するときである。**Fig. 3** のタイミングチャートを見ると，(2') 式を満たす 2 つの状態 ($H=1,\ M=0$) と ($H=0,\ M=1$) の間の遷移において，いずれの制御方式においても監視対象が 0 から 1 へに変化するときに問題が生じていることがわかる。従って，この部分を回避すればよいことがわかる。この修正の方法は，2 通り考えられる。

その第 1 の方法は，(9) と (10) を組み合わせる方法である。(9) と (10) は人間と機械について対称的であり，補い合うことができる。すなわち，状態 ($H=1,\ M=0$) から ($H=0,\ M=1$) への制御は，(9) 式により，状態 ($H=1,\ M=1$) から ($H=1,\ M=0$) への制御は，(10) 式によることにすればよい。これを **Fig. 4** に示す。この方式を，安全状態の確認が終了してから行動するという意味で，確認先行型と呼ぶことにする。

第 2 の方法は，時間遅れを実効的になくせばよいという考え方によるもので，現在の状態に基づいて制御を行うのではなく，少なくとも遅れの分だけ先行して状態の予測を行い，それに基づいて制御するというものである。これを予測方式と呼ぶことにしよう。ここで，遅れ時間を Δt, 予測時間を $\Delta t'$ とすると，

$$\Delta t' \geqq \Delta t$$

であることが必要である。これを，式で示すと，

$$\widehat{M}(t,X) = \overline{H}(t+\Delta t', X) \cdot Cm(t,X) \quad \Delta t' \geqq \Delta t \qquad (6'')$$

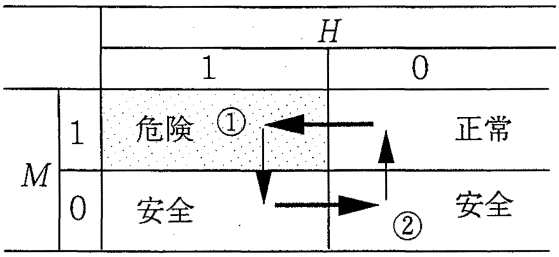
$$\widehat{H}(t,X) = \overline{M}(t+\Delta t', X) \cdot Ch(t,X) \quad \Delta t' \geqq \Delta t \qquad (7'')$$

となり，式 (8) から，

$$M(t,X) = \overline{H}(t+\Delta t'', X) \quad \Delta t'' \geqq 0 \qquad (9'')$$

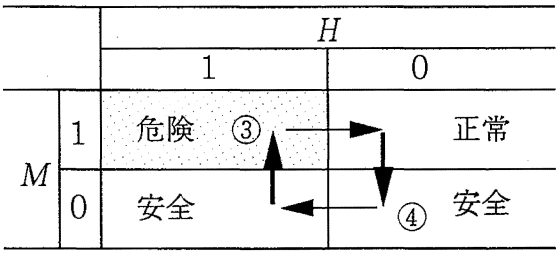
となる。ただし，Cm はこの議論において変える必要がないので 1 とし，また，$\Delta t' - \Delta t$ は $\Delta t''$ とおいた。同様に H についても，

$$H(t,X) = \overline{M}(t+\Delta t'', X) \quad \Delta t'' \geqq 0 \qquad (10'')$$



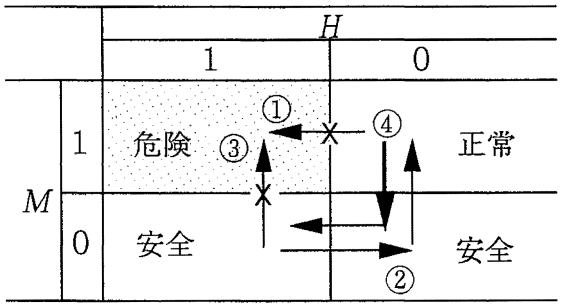
$M(t+\Delta t,X)=\overline{H}(t,X)\cdot Cm(t,X)$　①②

(a)制御方式(9)の場合



$H(t+\Delta t,X)=\overline{M}(t,X)\cdot Ch(t,X)$　③④

(b)制御方式(10)の場合



$M(t+\Delta t,X)=\overline{H}(t,X)\cdot Cm(t,X)$　②

$H(t+\Delta t,X)=\overline{M}(t,X)\cdot Ch(t,X)$　④

(c)制御方式(9)+(10)の場合

Fig. 4　State transition in the truth table.
真理値表上で示す状態の遷移

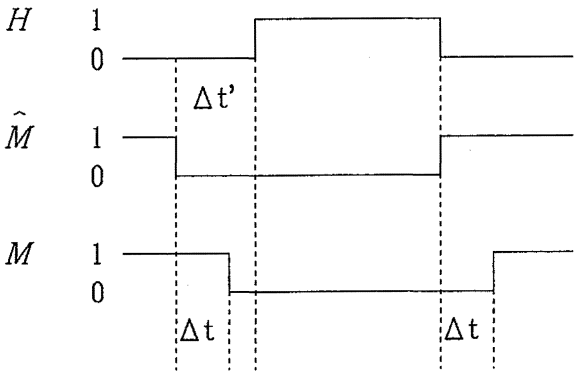


Fig. 5　Timing chart of prediction.
予測のタイミングチャート

となる。(6") 式, (9") 式を **Fig. 5** のタイミングチャートに示す。

ここで注意しなければならないのは，この予測は監視対象が 0 から 1 に変化する場合にのみ行うということである。なぜなら，条件 (2') が満たされなくなるのは 0 から 1 に変化するときだけだからである。実際に制御において使用する場合にも，異常発生時の安全停止には，この立ち上がり側のみが意味を持つ。また，人間も「機械が来たから避ける。」ではなく「機械が来るから避ける。」というかたちで，実は予測に基づいて行動していると考えられる。

なお，(6") から (10") までの式も立ち上がり側についてのみ成り立つ。

予測方式においては，予測と制御結果，特に安全停止の結果の確実性が前提となる。この点で，前提とすべきものがより少ない確認先行方式の方が好ましい。

2.7 境界を通しての領域の制御

領域を制御するのに領域全体を直接制御する場合もあるが，境界を通して制御することが多い。この論理的意味について次に述べる。

人間や機械等の物質は，何もないところから出現することもないし，空中に消滅することもない。ある領域内部での物質の量の増減は，境界を物質が通過することで起こる。すなわち，領域内部の量の変化分は境界を通過する量と等しい。従って，領域内部の状態は，初期状態と境界を通しての変動で規定できる。

例えば，領域内部の人数の変化はその領域の境界を通過する人数によって規定される。これを式で示すと，

$$\Delta \mathrm{H}(t,A) = \mathrm{H}(t,\partial A)$$

となる。ただし，$\mathrm{H}(t,A)$ は時刻 t における領域 A 内の人数で，Δ はその時間変化を示し，$\mathrm{H}(t,\partial A)$ は時刻 t における領域 A の境界 ∂A における人数を示す。

従って，人間がいないという状態を維持するためには，境界での人間の存在を排除すればよい。これは例えば，境界に柵を設けることで可能となる。また，境界を監視していれば，人間がいないという状態が維持されているかどうか分かる。この場合，初期条件として，領域内部に人間がいないということが必要である。このことを論理式で示すと，

$$\overline{H}(t,A) = \overline{H}(t_0,A)\cdot\overline{H}(t,\partial A) \qquad (11)$$

なお，予測方式では，時間を空間に置き換えて，領域 A に人が居ないことを監視するためには、領域 A を含

Table 2 Form of area guard applied to the automated warehouse.
自動倉庫に適用した領域防護の形態

	運転モード	安全対策の原理	開発した領域防護の形態	危険領域	管理レベル	参照節
(a–1)	運転	隔離の原則	搬入搬出口の柵	全可動範囲	1	3.2
(b–2)	停止	停止の原則	扉インターロック	全可動範囲	2	3.3
(b–1–1)	運転→停止	進入防止　確認先行	ロック式扉	全可動範囲	2	3.3
(b–3)	停止→運転	停止の原則	警報付き起動装置	全可動範囲	2	6 章
(a–2)	運転	隔離の原則	位置設定式暴走検出装置 ピッキングシステム	走行路一部 棚一部	3	3.5 4 章 2 節
(b–1–2)	運転→停止	安全停止　予測	走行用挟まれ防止装置 長ストロークバンパ	スタッカクレーン 前面	3	4 章 4.3 節 3.5

むより大きな監視領域 B を設け、その境界を監視している。予測方式については、従来から多くの研究がなされている。詳細は、例えば文献 3) を参照されたい。

3. 自動倉庫における領域防護

3.1 領域防護の形態

危険領域 X において，安全条件 (2') を満たす制御を領域防護と呼ぶ。ここで，領域 X のみが危険領域であることを前提とする。

このとき，領域 X における領域防護は，幾つかの段階に分けられる。まず最初は，

$$M(t,X)=1, \quad H(t,X^C)=1$$

を前提にして，

(a–1) 危険領域に人間を入れない。　$H(t,X)=0$

(a–2) 危険領域から機械を出さない。$M(t,X^C)=0$

という「隔離の原則」に基づく対策を行う。その実現方法については，後述する。

作業によっては隔離が不可能なものもあり，また隔離が失敗することもある。そのような場合には，人間の領域 X への進入に対して，

(b-1) 危険領域に人間が入る前に，機械を停止する。

$$M(t_1,X)=0, \quad H(t_2,X)=1 \qquad (t_1 \leqq t_2)$$

(b-2) 危険領域に人間がいる間機械を停止させ続ける。

$$M(t,X)=0, \quad H(t,X)=1$$

(b-3) 危険領域から人間が出たあと，機械の運転を許す。

という「停止の原則」に基づく対策を行う。

(b-1) の実現方法は，さらに

(b-1-1) 機械が停止したことを確認して人間の接近を許可する進入防止方式と，

(b-1-2) 人間の接近を領域の外側で検知し，その到着以前に機械を停止させる安全停止方式

に分けられる。これは，それぞれ確認先行方式，予測方式の実現形態である。

また，(b-3) については，(11) 式で示したように，初期状態として，人がいないという正常性の確認が必要となる。

自動倉庫においてこれらを適用したものを **Table 2** に示す。

3.2 最大動作領域の防護

機械及び荷物・ワーク等の全動作領域（以下，これを最大動作領域と呼ぶ。）を D とすると，この D は，

$$D=\{x|M(t,x)=1\}$$

のように定義できる。D において機械が動いているとき，

$$M(t,D)=1 \quad \exists t$$

であり，最大動作領域外 D^C に対して定義から

$$M(t,D^C)=0 \quad \forall t$$

である。すなわち，最大動作領域 D を危険領域とする場合には，前節の領域防護の条件 (a-2) は自動的に満たされる。従って，「隔離の原則」に基づく安全対策として (a-1) を達成すれば良く，これは防護柵を設けることで実現できる。この防護柵は危険領域の全周囲にめぐらすことが必要である。さもないと，2.7 節で示した境界での

人間の不在 $\partial D = 0$ が保証できず，ひいては $\overline{H} = 0$ が保証できない。

通常，自動倉庫においては，荷物の搬入搬出のために開口部があるが，本研究においては原則として開口部は作らないようにした。開口部を作らないためにこの部分にも柵を設け，荷物の搬入搬出は人間の存在空間外の柵を越えた高さで行うようにした (第 4 章 4.5 参照)。これによって，人間の進入による事故を心配することなく自動運転が可能になった。

3.3 最大動作領域への入退出管理

本研究の自動倉庫の安全対策においては，開口部をなくしたが，保全・トラブル処理等のために人間が入らなければならない場合がある。この場合には，隔離の原則が適用できず停止の原則を適用しなければならない。

人間の出入りのために柵に出入り口を設けた。この出入り口の管理には既に述べたように，進入防止方式と安全停止方式がある。従来の安全停止方式では出入り口を開口とし出入りをセンサで監視するか，出入り口を扉にし，扉を開けると安全停止がかかるという方式を用いる。

自動倉庫では後述するように安全停止方式は適さないので，本研究では進入防止方式を採用した。出入り口は **Photo 1** に示すように扉とし，この扉は，通常はロックしておき，スタッカクレーンが停止したことを確認したときに限りこのロックを解除できる方式とした。

作業者は，危険領域に入る必要があるときには，機械の停止の操作を行う。停止確認センサで機械の停止を確認して初めて解錠が許可される。このとき，解錠の操作を行えば，ロックが解除されて扉を開くことができ，危険領域に進入できる。

このロックは通常はバネで錠が押されているが，停止の確認信号によってソレノイドで解錠するものである。このような構成とすることで，停止確認センサ等の故障時にはロックがかかったままとなるフェールセーフなものとすることができる。

扉が開いているときには，人間がいないという保証が得られないので，機械の起動があってはならない。そのため，扉が閉まっているということを確認するインターロックを用いた。これは前述のロック装置に組み込まれていて，扉を閉めて，かつ，ロックされることで，扉が閉まったという信号が生成され，これによって起動が許可される。

ただし，既に述べたように扉が閉まったということは必ずしも危険領域に人がいないということを意味しない。そのためには，(11) 式に示すように初期状態としての正常確認も必要である。その具体的手段については，5 章及び 6 章に述べた。

Photo 1　Guard for entrance to a danger zone.
危険領域の入口の防護

この進入防止方式という形態は日本ではあまりなじみがなかったが，欧州では常識となっており，そのためのロック装置も販売されている。また，これらの装置は規格化されている[7]。

3.4 自動倉庫における進入防止方式の必要性

本システムでは最終的には採用しなかったが，荷物の搬入搬出口が開口部となる場合についても検討した。この場合の防護は，開口部において人間の接近を検出してスタッカクレーンを停止するという安全停止方式の形態になる。

この形態では，スタッカクレーンの急停止を要することになるが，これは自動倉庫においては本質的な欠点となる。すなわち，スタッカクレーンは背の高い構造体であるが，その推進・停止の駆動力はレールのある底部に加わるため，荷が上方にあるときには大きなモーメントが働く。従って，急停止を行うと構造体に無理な力がかかり，また，急停止させれば荷物がずれたり落ちたりするおそれがある。さらに，大型の機械であり慣性も大きいので，急に止めるためには能動的なブレーキが必要で

あるが，これはフェールセーフ化が困難である。これらの理由で，急停止させることは，例えできるとしても好ましくない。

自動倉庫に限らず，急停止させることが作業上や安全上問題となるシステムにおいては，開口部を残して人間の危険領域への進入を許す安全停止方式ではなく，進入防止方式を基本とするべきであろう。

また，荷物の搬入搬出口において人間を検知するためには技術的に困難な課題がある。すなわち，人間と荷物の識別である。搬入搬出口は荷物を出入りさせるための口であり，ここを荷物が通過するときにこれを異常と見なして停止することは避けねばならず，一方，人間が通過するときには停止させる必要がある。通常，開口部を監視するのに光線式安全装置を用いて開口部に物体がないことを検出することが多いが，この方法では人間と荷物の区別がつかない。

人間の存在，特徴のある特性を有する荷物の存在，人間を含めた物体の存在，物体の不在を検知する手段は一般に知られているが，ここで必要なものは人間の不在であり，これを検知するフェールセーフな手段は知られていない[8]。一般に，フェールセーフに何かあるものの不在を検出するためには，透過型センサでエネルギーを空間に投射し，それを受けている経路にその物体が入ることでエネルギーの吸収が起き，エネルギーの受信ができなくなる。これで選別するためには，人間のみが遮断し，他の物体の場合には遮断されないエネルギー形態を用いる必要があるが，このようなものは知られていない。

人間の存在を検知するためには，「人間に発信機を持たせる」，「特定の色の着衣を使用する」，「体温を検知する」等の手段が考えられる。しかしこれらの手段は，第三者が進入したり，着衣により体の表面が隠される等の検知方式自身の限界や，検知機の故障による検知の失敗があり得るので，安全支援装置でしかない。

開口部に人間か荷物のいずれか一方しか存在しないという条件が成り立つときに限り，物体の存在と荷物の存在から人間の不在を知ることができる。

しかしながら，自動倉庫の場合には，パレットに荷物と一緒に人間も乗ることができるので，この条件を当てはめることはできない。

3.5 最大動作領域内作業

人間が機械に接近してかつ機械を運転しながら作業を行うことが必要な場合がある。この場合にも，安全対策は隔離の原則と停止の原則によるが，危険領域を最大動作領域 D とする制御では，対応できない。そのため，危険領域を最大動作領域 D の一部に限定して対策を考えることになる。

Photo 2 The position setting type protective device for runaway and the long stroke bumper.
位置設定式暴走検出装置と長ストロークバンパー

一般に作業全体はいくつかの段階に分けられ，それぞれの段階では機械の動く範囲は最大動作領域より小さいことが多い。従って，適切に時間を限れば限定された動作範囲について検討できる。これを式で示すと，

$$M(T, X) = 1$$
$$M(T, X^C) = 0$$

となる。この場合も，隔離の原則を適用するためには，機械がこの範囲から出ないという対策と人間が入らないという対策が必要である。また，停止の原則についても同様である。

領域を制限した場合の安全対策としては，例えば，動作領域を 2 つに分けて，一方の領域に機械がある間は，他の領域を人間に開放するといった方式が考えられる。産業用ロボットにおいて筆者らが開発したシャトル方式[9]はこの一例である。この場合，領域防護には機械がその領域から出ないという対策も必要となる。この例では，2 つの領域を恒久的に分けているため，分離も恒久的な手段で行うことができた。しかし，自動倉庫においては，人間と機械の共同作業は定常作業としてはなく，非定常

な作業であることから，恒常的な分離手段を設けることはできない。すなわち，柵のような人間の行動に対するインターロックを設けることはできないので，今回の研究においては，安全停止方式による危険領域の防護手段を開発した。

1つは，安全バンパ(走行用挟まれ防止装置：第4章4.3節参照，長ストロークバンパ：**Photo 2**) である。これはスタッカクレーン本体を危険領域とし，その前方に，小さな監視領域を設定し，この範囲内に人間が入ることで，スタッカクレーンを安全停止させるものである。この設定範囲内で停止できるために，走行用挟まれ防止装置の適用に際して走行速度が小さいことが条件であり，長ストロークバンパでは逆に通常の運転速度に対応できるように検出装置を離している。

もう1つは，位置設定式暴走検出装置 (**Photo 2** 参照) である。これは，倉庫の柱に沿って立ててある検出用センサを走行路に対して倒すことでスタッカクレーンの走行路内に人間の領域を設定するものである。この装置においては，スタッカクレーンが設定された危険領域から出ないように (a-1) の防護をしているが，人間が危険領域に入らないという (a-2) の防護はない。また，(a-1) についても人間がセンサを倒さなければ機能しない。この意味で，これは事故防止の切り札となるものではなく，安全支援装置である。

4. 考　察

4.1 進入防止方式と安全停止方式

進入防止方式は，**Table 2** に示すように確認先行方式によっているので，実際に安全状態が実現されてから人間の危険領域への進入が許可されるが，安全停止方式は予測方式に基礎を置きそれを現在の状態の外挿で予測することになる。この予測が正しいとをいうためには一定の条件が必要である。

すなわち，最悪の事態を考えれば，人間が危険領域に到着したときには機械は停止していなければならない。しかし，人間の進入を予測してブレーキをかけたときにはまだ運転状態なので，停止の予測を行っていることを意味するが，それぞれの予測において不確定性が紛れ込むおそれがある。

危険領域への人間の到達を事前に予測するには，危険領域の外側で人間との相対的接近速度に対応した距離以上離れたところで進入を監視する必要がある。人間との接近速度は，原則として最大値をとるべきである。例えば，長ストロークバンパーの場合には、スタッカクレーンの最大速度と人間の移動速度の和になり，走行用挟まれ防止装置の場合は，スタッカクレーンが低速であるので，ほぼ人間の移動速度である。機械側の速度は制御可能であるが，人間側の速度を制限するのは困難である。そうかといって，運動競技における最高速度を採ることは現実的ではない。この速度の設定によっては時間の逆転が生じるおそれがある。

また，停止時間の予測については，ブレーキが効かないと停止時間が延びるという問題がある。ブレーキの有効性は保守点検等の信頼性に依存することになり，これも不確定要素が入る一因となる。

さらに，危険領域の手前で予測を行ってはいるが，これに伴う誤差も考えられる。例えば，作業者が監視領域に入りかけて戻ることもあり得る。これについては，誤って進入を予測することは許されるが，誤って進入を予測しないことは許されない。この観点からは，作業者が監視領域に接近した場合はすべて危険領域に達するものと見なす必要がある。

このように，安全停止方式は予測に基づくため，若干の不確定性があり，これが無視できるものであるか否かを確認しておくことが必要である。

これに対し進入防止方式は，現在の状態の確認に基づくので，このような不確定性はない。従って，純粋に安全面から考えた場合には，進入防止方式を基本とすべきである。

4.2 防護の形態と高齢者の特性についての考察

機械の可動部周辺等の危険領域に対する防護の形態としては，人間の注意に依存して全く設備的防護のないものから，危険領域を完全にカバーで覆ってしまうというものまで，各種のものがある。これらの安全防護の形態と高齢者の行動様式との関連について考察する。

人間の注意に依存する形態は，人間が主体となったインターロックに相当し，**Table 1** に示すように人間が自分自身で危険回避を行うものと，機械を非常停止させる等の機械に対するものがある。いずれも，人間の知覚能力に依存するところが大であるが，高齢者では視覚・聴覚等の知覚能力の低下は免れず，注意力に依存する形態は高齢者に不利になる。また，注意の結果危険を感じても，高齢者には敏速な回避行動を期待することはできず，この面でも高齢者に不利になる。高齢者の職域拡大という観点からは，その責任感の強さや生産への意欲を活かすためにも，危険に対して注意させるのではなく，これらは設備対策に任せて，生産に対して注意させることが望ましい。

人間が接近した場合に，それを検知して機械を自動的に停止するという安全停止方式は，人間による停止操作

を含まないので，事故防止のための有効性は高い。しかしながら，安全停止方式では，監視を前提に人間の危険領域への自由な接近を許しており，開口部を設けることも少なくないが，開口部があると，機械側でのトラブル発生等の際には高齢者のように仕事に責任感が強い作業者の進入を誘うことになりがちである。

従来は危険領域の囲いが完全ではないことが多く，そのため監視対象である開口部以外の所から手を出すことが可能なこともその傾向を助長していたものと思われる。

それに対して進入防止方式では，本研究の自動倉庫での例のように，開口部を作らないことが必要であり，そのため，手が出しにくいという印象を作業者に与え，危険領域に入ろうという気持ちを持つ自体を防止できる。「何かあったときは停止してから入る。」と規則に決められていても，責任感から機械を止めることには心理的抵抗がある。機械を止めてよいということを高齢者に心理的に納得させるためにも，進入防止方式が必要であろう。

5. おわりに

機械に対する従来の日本の安全防護の対策は，労働者の質の高さに依存する部分が多く，カバーにしろ安全装置にしろ必ずしも十分ではなかった。例えば，危険領域に手が届くカバーや，作業者が容易に無効化ができる安全装置も少なくなかった。そのため，日本の高齢者のような責任感が強く生産意欲の高い労働者が，安全装置を回避して危険領域に進入することもあった。

このような現状から，機械の安全防護のありかたを見直すため，人間と機械が同一時刻同一場所に存在するとき発生する事故の論理的モデルをもとに，事故を防止するための条件を論理的に考察し，安全対策の論理的意味を明らかにした。すなわち，

(1) 空間を人間の存在領域と機械の動作領域に分けることの必要性（隔離の原則）
(2) 機械の動作領域に人間が進入する場合には機械を停止することの必要性（停止の原則）
(3) 人間のインターロックと機械のインターロックによる上記2つの原則の実現
(4) 領域の境界で制御を行う意味の明確化
(5) 運転の制御における時間遅れと予測の意味の明確化
(6) 「停止の原則」を実現するための2つの方式：安全停止方式と進入防止方式の明確化
(7) 危険領域を限定して安全対策を行う場合の対策

などを示し，この論理の枠組みの中で，安全対策は何を前提に意味を持つかということを明らかにした。

進入防止方式は，停止という確かな安全の状態を確認して初めて人間の接近を許可するものであり，システム全体のフェールセーフ化が可能であるが，安全停止方式は確かに止まるという停止性能への信頼の上に成り立つものであり，一般的にはこれはフェールセーフ化が困難である。この意味で，進入防止方式を基本とすべきであると考えられる。

進入防止方式は，中高年作業者が機械の停止を嫌うという心理特性からも必要となる。すなわち，安全停止方式では人間の接近を監視して機械を停止するが，中高年作業者は停止を嫌うために監視領域を迂回して危険領域に進入することがある。このような事態を防止するためには，柵・囲い等の徹底と，機械を停止しなければ接近できない進入防止方式の採用など，従来日本では軽視されてきた「人間に対するインターロック」の活用をはかることが必要であると結論される。

参考文献

1) 杉本旭・蓬原弘一・向殿政雄，安全作業システムの原理とその論理構造，電気学会論文誌，107-D-9, 1092～1098 (1987).
2) 杉本旭・粂川壮一・深谷潔・他，安全確認型安全の基本構造，日本機械学会論文誌 C, 54-505, 2284～2292 (1988).
3) 杉本旭・深谷潔，安全の基本原理と安全制御技術，産業安全研究所特別研究報告，RIIS-SRR-90,7 ～21 (1990).
4) JIS B 8433-1993 (ISO 10218:1992)，産業用マニピュレーティングロボット－安全性
5) 杉本旭・深谷潔，日本人の身体計測と安全ガードの標準化，産業安全研究所技術資料，RIIS-TN-84-4, (1984).
6) 杉本旭・深谷潔・蓬原弘一・向殿政雄，インターロックの論理構造，第20回安全工学研究発表会講演予稿集，39～42 (1987).
7) prEN1008 Safety of machinery-Interlocking devices with and without guard locking-General principles and provisions for design, (1993).
8) 深谷潔，人間と荷物の識別機構，第10回ロボット学会講演会予稿集，1113～1116 (1992).
9) 粂川壮一・杉本旭・深谷潔・清水尚憲，安全制御における計測技術，産業安全研究所特別研究報告，RIIS-SRR-86, No.1, 64～68 (1986).

(平成8年3月15日受理)