Research Report of the Research Institute
of Industrial Safety, RIIS-RR-87, 1987.
UDC 519.21 : 62-192 : 605.52.007

潜在危険制御システムの構成原理と概念設計法

佐藤吉信*

The Architectionic Principles and Designing of Hazard Control Systems

by Yoshinobu SATO*

Abstract ; The technical terminology "Fail-safe" is now used as different concepts in various engineering fields. The discrepancy sometimes brings about confusion to the discussions on safety among the different engineering systems. It is important for carrying execution into safety plans for mechatronics, especially robotics which consists of overall engineering systems, that a generalized methodology to conceptualize saftety measures be established.

In this paper, first, hazard restraint measures are generalized as the following four principles, based on the "Action-change and Action-chain" hazard production theory :

(1) Careful selection of system elements,
(2) Prevention of undesirable changes in each system element,
(3) Inhibition which prevents the system from transferring to a system phase in which a damage can be brought about, and
(4) Control which prevents the system from causing a damage after the system has transferred to the system phase.

Second, hazard control, which materializes the Hazard Restraint Principles (3) or (4), is generalized in terms of a "Dissociation of Action-linkages." Dissociations of action links are categorized by the following dissociation principles :

P_1 ; Control of an action-source,
P_2 ; Control of an action-path,
P_3 ; Control of an action-source and path, and
P_4 ; Control by substitution for a failed function.

Third, the relationships between the dissociation principles and the action link dissociations, are given [Theorem 1]. Here, the dissociation actions, which act an element and are necessary conditions for dissociation of an action link from the element, are categorized as follows :

(a′) ; Energy-transmission type,
(b′) ; Information-propagation type,
(c′) ; Agent-transfer type,
(d′) ; Supply-obstruction type,
(e′) ; Existence-form type,
(f′) ; Function-cessation type, and
(g′&g″) ; Function-substitution type.

Next, the fundamental relationships between the dissociation principles and the dissociation

* 機械研究部 Mechanical Safety Research Division

actions are given [Theorem 2], and the schematic representation of the dissociations is shown in Fig. 2. Control chains, which link a dissociation element and are necessary conditions for generation of a dissociation action from the dissociation element, are introduced. Control chains consist of control action links. Control actions are categorized into types "a″", "b″", "c″", "d″", "e″", and "f″" like dissociation actions.

Then, reversal action, which, are produced by a element's failure to generate a control action or a dissociation action, are categorized into types "$\bar{a}$", "$\bar{b}$", "$\bar{c}$", "$\bar{d}$", "$\bar{e}$", and "$\bar{f}$",. The fundamental properties of control or dissociation action reversals are developed [Theorem 3]. For a reversal chain resulting from a reversal of a control action link, the fundamental properties are given [Theorem 4, 5, and 6].

Finally, quantitative characteristics of the control actions and dissociation actions are examined. A single-direction fluctuating action link, where the strength or property of the action is controlled in a single direction, and a dual-direction fluctuating action link controlled in dual or more directions, are introduced from the quantitative aspects of action control. Relationships between dual-direction fluctuating action links in a hazard control system are given [Corollary 15]. Relationships between control (or dissociation) action types and single-direction (or dual-direction) fluctuating actions are given [Theorem 7].

Last, architecture of hazard control systems is demonstrated by examples involving robot failures etc., (Fig. 2～5).

Last of all, some discussions are made for carrying execution into effective safety plans.

Keyword ; Hazard Control System, Conceptual Design, Fail Safe, Fault Tolerance, Redundant System, Safety, Reliability, Robot, Buzz Saw, Sensor.

1　はじめに

マイクロコンピュータの発展は，単に工場における生産システムの変革のみならず，自動車などの交通手段や家庭用コンシューマ機器にいたるまで，種々の機械システムのいわゆるメカトロニクス化の進展を促している。

こうしたメカトロニクスでは，システムの安全性向上のために，多様な安全技術が求められている。例えば，非常に厳格な安全性を要求されると言われる，鉄道の電子連動装置における安全技術の適用状況をみても，いわゆる狭義のフェイルセイフ技術(11%)，多重化などのいわゆる高信頼性技術（34%)，故障診断・回復（36%)，フールプルーフ（４%)，危険側故障の低減（９%)，その他の技術（６%）など非常に多彩な技術により安全化がはかられていることがわかる[1]。

メカトロニクスの中でも特にロボットは，構造系，駆動系，制御系，センサ系などのハード体系および人工知能を実現するためのソフト体系など工学全般にわたる体系から構成されるため，その安全性向上には総合的な事前安全計画の実施が不可欠である。

事前安全計画は次の過程に大別されよう：

(1)　潜在危険の同定
(2)　潜在危険抑制措置の検討
(3)　定性的安全性評価
(4)　定量的安全性評価

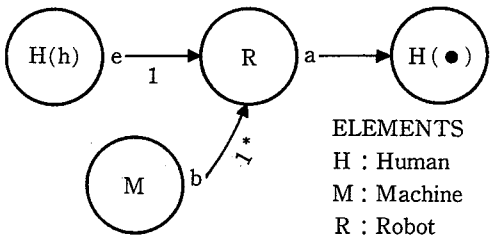
ロボットの事前安全計画過定(1), (3), (4)については，文献(2), (3), (4), (5), (6), (7)などにより，その一般的方法論や解析・評価モデルが提示されている。ところで，従来の安全性解析手法である FMEA, ETA, FTA, HAZOP などの系統的手法は，いずれも事前安全計画過程(1), (3), (4)を対象としたものである。(2)を対象とした系統的方法論が開発されてこなかったのは，従来の事前安全計画が，例えば原子力プラント，化学装置，宇宙・航空産業あるいは鉄道など単一の目的・機能として運用される系に限定されてきたことが原因としてあげられる。これまで，この過程の検討は，個々の工学体系のエキスパートにまかされてきた[8]。その結果，異なる工学体系でも共通して理解可能な，包括的な潜在危険生成理論に立脚した潜在危険抑制措置のシステム安全工学上の体系化がなされておらず，その概念設計法も確立していないのが実状である。

たとえば，潜在危険抑制手段のひとつとして“フェイルセイフ”の概念があげられる。この概念は，元来鉄道信号の分野で用いられ，信号系統に発生した障害が列車を停止させる方向に収束するというものであった。最近では，“フェイルセイフ”は原子力プラント，航空機の設計などの広範な分野で用いられ，例えば航空機ではある種の冗長系を構成することを“フェイルセイフ”と呼んでいるようにその意味するところが各分野で異なっている[9]。このような基本的術語をめぐる概念の不整合は，特に複合システムの安全論議に混乱をもたらしている。

ロボットなどの多目的・多様な環境で使用される柔軟なシステムでは，事前安全計画(2)の段階も系統的に行われることが必要である。そこで本報では，「作用—変化」と「作用—連鎖モデル[10]」(以下 A-C モデル) に基づき，次章で潜在危険抑制手段を体系化し，3章では潜在危険制御系の構成原理を「作用鎖の解離理論」として一般化して，異なる工学体系間に共通した系統的な潜在危険制御系の概念設計法を確立するとともに，4章ではいくつかの実システムにおける潜在危険制御系の構成事例を示す。

2 潜在危険の抑制原理

Fig. 1 は産業用ロボット R の作業者 H に対する潜在危険を A-C モデルにより同定したものである。すなわち作業者がロボットに近づいたとき $\{H(h)e_{1}\rightarrow R\}$，他の装置 M からロボットへ動作信号が伝達され $\{Mb_{1}^{*}\rightarrow R\}$，ロボットが動作することによって運動エネルギ伝播形の直接原因作用 $(a_{0}\rightarrow)$ が作業者に伝播される可能性 $\{Ra\rightarrow H(\cdot)\}$ を示している。ここで，(h) は「作業者がロボットに近づく」という作業者の心理的および空間的変化，(・) は作業者に生ずる傷害を表わしている。



Actions
a : Energy-Transmission-type action
b : Information-Propagation-type action
e : Existence-form-type action
Changes
(h) : Human's approach to robot
(●) : Damage in human

Fig. 1 Hazard identification of a robot by A-C Models
A-C モデルによるロボットの潜在危険の同定

潜在危険抑制の観点からみると，このシステムでは，もしも R または H が存在しなければ，作用連鎖 $\{Mb_{1}^{*}\rightarrow Ra_{0}\rightarrow H(\cdot)\}$ は生じないことがわかる。R および H が存在しても，変化 (h) が抑制されれば作用連鎖 $\{H(h)e_{1}\rightarrow Ra_{0}\rightarrow H(\cdot)\}$ の発現も抑制される。変化 (h) が生じても，これに対するインターロックにより，ロボットを動かないようにしておけば直接原因作用鎖 $\{Ra_{0}\rightarrow H(\cdot)\}$ の発現は抑止される。また，ロボットが動作中でも，ロボットの動作に非常停止をかけることによって，かろうじて $\{Ra_{0}\rightarrow H(\cdot)\}$ の発現を阻止することができよう。

以上の考察から容易に理解されるように，潜在危険の抑制過程は，次の抑制原理に分類される[11]：

(1) 作用源の排除
(2) 変化の抑制
(3) 作用連鎖生成相遷移の禁止
(4) 発現しつつある連鎖の解離

抑制原理(1)は，人間または機器に望ましくない作用を行う要素を系から排除，またはそのエネルギー状態や化学的性質などを作用源とならない状態に限定して使用することを意味する。これは，排除する要素に代替する要素の存在，リスク，代替あるいは限定使用によるコスト増，社会的要請との関係など系の基本的設計条件により実現が決定される。また(2)は，要素が機能を維持し，危険側への逸脱した挙動を行わないようにすることである。余裕をもった条件による系の設計・運用，高信頼性要素の採用，保全による信頼性の維持，フールプルーフなどによる危険側への変化の防止などによって達成される。次に(3)において作用連鎖生成相とは，要素の特性を表わすモードによって規定される系の相を意味する[12]。例えば，ロボットの運動特性を停止モードと作動モードに区分すると，系を停止モード相と作動モード相とに分割することができる。今，系が停止モード相にあるとき，ロボットの制動系が正常でない，またはそのまま作動モード相へ遷移すると故障が生ずることが診断または予測できれば，系の停止

モード相から作動モード相への遷移を禁止することができる。これは，異常診断，異常予測などによって達成される。続いて(4)は，系がすでに遷移した相において，ある条件下で発現しつつある作用連鎖をその途中で解離，すなわち切断することによって，人間または重要な機器に生ずるき損を抑制するものである。

抑制過程(3)，(4)は系にいわゆる潜在危険制御系を構成することによって実現される。

3　潜在危険制御系の構成原理

3.1　作用鎖の解離

A-Cモデルを以下のように拡張することにより，潜在危険制御系の構成のための基本的法則を明らかにする。

[定義1] 系の要素は，分割された系の部分である。

[定義2] 要素の変化は，電圧，温度などの物理量や，形状，情報量の変化も含む。

{系1} 要素のき損は他の要素の作用によって生ずる。

{系2} き損の発現過程は，要素間での1)作用の授受，2) 要素の変化で把握される。

[定義3] 作用を行う要素を作用要素，作用を被る要素を被作用要素と言う。

[定義4] 作用の形を次のように定義する：

(a) エネルギ伝播形作用：運動エネルギや熱エネルギなど，エネルギとしての意味をもつ要素間での働きかけとする。エネルギが伝播された要素には，エネルギ変換による変化が伴い得る。

(b) 情報伝達形作用：表示や信号など，情報としての意味をもつ働きかけとする。

(c) 作因物転移形作用：化学物質や病原体のようにエネルギや情報以外の物質として認識できる作因物が要素から要素へと転移することによる働きかけとする。

(d) 供給阻害作用：ある要素に，エネルギ，情報または作因物などの必需があって，それに対する供給を妨害することによる働きかけとする。

(e) 存在形態形作用：エネルギ，情報および作因物の移動を伴わない，要素間でのある要素の形状，重量，状態，条件などによる働きかけとする。

(f) 機能不履行形作用：ある要素が他の要素に対して，果たすべき機能を行わないことによる働きかけとする。

{系3} 作用は，a,b,c,d,e,fの各形に分類される。

{系4} 要素は，さらに下位要素に細分割される場合がある。

{系5} 作用は，要素間，および下位要素と上位要素間でも行われる。

[定義5] 要素がa,b,c,d,e形の作用を行うとき，その作用に関して能動的状能にあり，f形の作用を行うとき，その作用に関して非能動的状態にある。

[定義6] 能動的状態にある要素を，その作用に関して作用源と言う。

[定義7] 作用が行われる要素間の空間を，作用経路と言う。

[定義8] 作用を発現させる特定の変化が生じている条件下で，作用連鎖[13]のなかのある作用の発現を抑止することを，その作用鎖の解離（切断）と言う。

{系6} 誘因作用鎖[14]が解離されると，次の作用の発生確率が減少し，直接原因作用鎖[15]が解離されると，き損の発生が抑止される。

[定義9] 解離作用は，ある要素に作用して，その要素からの作用鎖を解離するための必要条件となる作用である。

[定義10] 解離作用を生成する要素を，解離要素と言う。

[定義11] 作用源の制御による作用鎖の解離を，作用源の制御と言う。

[定義12] 作用経路の制御による作用鎖の解離を，作用経路の制御と言う。

[定義13] 作用源と作用経路の制御によるものを，作用源と作用経路の制御と言う。

[定義14] 不履行機能の代替による作用鎖の解離を，不履行機能の代替制御と言う。

{系7} 作用鎖の解離は，次の解離原理に分類される：P_1（作用源の制御），P_2（作用経路の制御），P_3（作用源と作用経路の制御），P_4（不履行機能の代替制御）。

解離原理と作用鎖の解離との関係が，次の定理として得られる：

[定理1] a,b,c,d,e形の作用鎖は，解離原理P_1,P_2,P_3のいずれかにより，f形の作用鎖は解離原理P_4によってのみ解離される。

[定義15] 解離作用の形を次のように定義する：

(a′) エネルギ伝播形：解離要素と作用要素間でエネルギの授受が行われることにより生ずる解離作用。

(b′) 情報伝達形：表示や信号など，存在形態やエネルギ量としてよりは情報量として意味をもつ働きがおこなわれることにより生ずる解離作用。

(c′) 作因物転移形：化学物質，重量物質として認識可能な作因物の授受により生ずる解離作用。

(d′)　供給阻止形：要素が作用を行うために，エネルギ，情報，作因物などの供給を必要とするとき，その供給を阻止することにより生ずる解離作用。

(e′)　存在形態形：エネルギ，情報，作因物の移動を伴わず，それらの供給を妨害するものではない，形状重量，状態，条件または性質などにより生ずるf′およびg′&g″以外の解離作用。

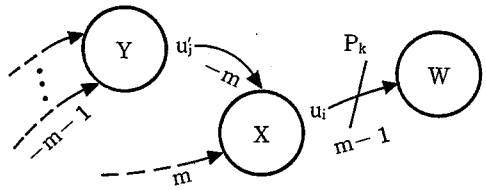
(f′)　機能停止形：解離要素が能動的な状態にあることによって解離要素と作用要素間で生じていた作用または複合された作用，すなわち機能が停止されることによって生ずる解離作用。

(g′&g″)　機能代替形：f形の作用を行うとしている要素に代わって，解離要素がその機能を代替することにより生ずる解離作用。

{系8}　解離作用は，a′,b′,c′,d′,e′,f′,g′&g″形に分類される。

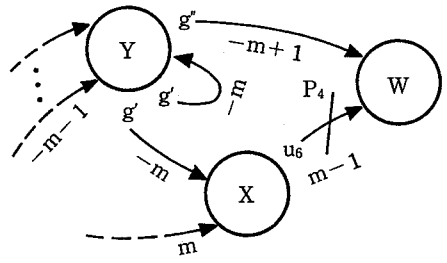
解離原理と解離作用の基本的関係が，次の定理として得られる：

[DISSOCIATION TYPE 1]



i=1,2,. . ,5　j=1,2,. . ,6　k=1,2,3
m=1,2,3,. . . (Action Order)
u_i : Action(u_1=a,u_2=b,u_3=c,u_4=d,u_5=e)
u_j' : Dissociation Action (u_1'=a′,u_2'=b′,u_3'=c′, u_4'=d′,u_5'=e′,u_6'=f′)

[DISSOCIATION TYPE 2]



u_6 : Action(u_6=f)
g′ & g″ : Dissociation Action
X : Generator Element, Y : Dissociation Element
W : Receiving Element, P_k : Dissociation Principle

Fig. 2　Dissociation principles and dissociation action links
解離原理と解離作用鎖

[定理2]　解理原理P_1,P_2,P_3は，a′,b′,c′,d′,e′(および／または)f′の解離作用により実現され，P_4は，g′&g″形の解離作用によってのみ実現される。

Fig. 2は，単一の解離作用による解離の図式表現である。解離形1は解離原理P_1,P_2,P_3を，解離形2は，P_4を表している(u_1'=a′,u_2'=b′,u_3'=c′,u_4'=d′,u_5'=e′,u_6'=f′,u_1=a,u_2=b,u_3=c,u_4=d,u_5=e,u_6=f；矢印と作用記号で作用鎖を表す)。矢印の下の“−m”及び“−m+1”(m=1,2,3,…)は直接原因作用鎖(m=0)からの連鎖順位に“−1”を乗じた値を示す。解離とその原理が作用鎖上にスラッシュ(／)と記号“Pi”(i=1,2,3,or4)を付記することにより示される。

3.2　制御連鎖と抑制作用

解離作用を発生させるためには，一般に，解離要素に結合する，ある種の作用連鎖が生成されることが必要である。

[定義16]　解離要素に結合し，解離作用の発生の必要条件となる作用連鎖を抑制連鎖，抑制連鎖の生成の必要条件となる作用を抑制作用，そして抑制作用を発生する要素を抑制要素という。

[定義17]　解離作用鎖と，その抑制連鎖からなる単連鎖[14]を，制御連鎖と言う。

{系9}　制御連鎖は，一方の端から解離作用鎖まで次々と連鎖する抑制作用鎖と，その解離作用鎖からなる単連鎖であり，各々の抑制作用鎖は，その次の抑制または解離作用鎖の発現の必要条件となっている。

{系10}　解離作用の発生には，必要とされる全ての制御連鎖，従って全ての抑制連鎖が生成されなければならない。

[定義18]　ある解離に必要な制御連鎖の集合を，その解離に関する潜在危険制御系と言う。

[定義19]　抑制作用を次のように定義する：

(a″)　エネルギ伝播形：エネルギの授受が行われることにより生ずる抑制作用。

(b″)　情報伝達形：情報量として意味をもつ働きが行われることにより生ずる抑制作用。

(c″)　作因物転移形：物質として認識可能な作因物の授受による生ずる抑制作用。

(d″)　供給阻止形：必要とされる供給を阻止することにより生ずる抑制作用。

(e″)　存在形態形：エネルギの伝播，情報の伝達，作因物の転移を伴わず，それらの供給を阻止するものでもないf″形以外の抑制作用。

(f″)　機能停止形：抑制要素が能動的な状態にあることにより行われる機能を停止することにより生ずる抑制作用。

{系11} 抑制作用は a″,b″,c″,d″,e″,f″ 形に分類される。

3.3 制御連鎖の反転と反転連鎖の解離

{系12} 要素から抑制または解離作用が生成されないことにより，ある種の作用が生ずる。

[定義20] 抑制または解離作用が生成されないことにより生ずる作用を，反転作用と言い，またそのとき，抑制または解離作用鎖が反転したと言う。

[定義21] 反転作用の形を，次のように定義する：

(ā)　エネルギ伝播形：エネルギの授受が行われることにより生ずる反転作用。

(b̄)　情報伝達形：情報量として意味をもつ働きが行われることにより生ずる反転作用。

(c̄)　作因物転移形：物質として認識可能な作因物の授受が行われることにより生ずる反転作用。

(d̄)供給阻害形：必要とする供給を阻害することにより生ずる反転作用。

(ē)　存在形態形：エネルギの伝播，情報の伝達，作因物の転移を伴わず，それらの供給を阻害するものでもない $\bar{f}$ 形以外の反転作用。

(f̄)　機能不履行形：はたすべき機能を行わないことによる反転作用。

{系13} 反転作用は ā,b̄,c̄,d̄,ē,$\bar{f}$ 形に分類される。

抑制および解離作用の解離に関する基本的性質が，次の定理として得られる：

[定理 3] a′,b′,c′,d′,e′,g′&g″ 形の解離作用，または a″,b″,c″,d″,e″ 形の抑制作用が反転すると，$\bar{f}$ 形の反転作用が生じ，f′ 形または f″ 形の解離または抑制作用が反転すると，ā,b̄,c̄,d̄,ē 形の反転作用のうち少なくともひとつが生ずる。

{系14} ある要素からの抑制または解離作用鎖は，1) その要素へ結合する抑制作用鎖が反転する，また 2) その要素に抑制または解離作用を反転させる変化が生ずることによって反転する。

[定義22] ある要素に生ずる変化のうち，1) その要素へ反転作用鎖が結合していない条件下で，その要素からの抑制または解離作用鎖を反転させるもの，または 2) その要素へ解離作用が結合していない条件下で，その要素から反転作用を，元の抑制または解離作用鎖へ再反転させるものを，引金変化という。

抑制作用鎖の反転により生ずる反転連鎖の基本的性質が，次の定理として得られる：

[定理 4] 抑制連鎖を構成する任意の要素に引金変化が発生すると，その要素からの抑制作用が反転することにより，そこから反転連鎖が生成され，解離は実現されなくなる。

反転作用の性質は，作用連鎖を構成する作用の性質と同じで，次の定理を得る：

[定理 5] ā,b̄,c̄,d̄,ē 形の反転作用鎖は，解離原理 P_1，P_2 または P_3 によって，$\bar{f}$ 形の反転作用鎖は，P_4 によってのみ解離される。

反転作用鎖の解離と，制御連鎖の復活との基本的関係が，次の定理として得られる：

[定理 6] 定理 4 において生じた反転連鎖の，ある反転作用鎖が解離されると，他に引金変化および反転連鎖が生じなていない条件下で，そこから部分的に抑制連鎖が復活し，作用連鎖の解離が再び可能となる。

3.4 抑制および解離作用の定量的性質

潜在危険制御系の設計では，抑制および解離作用の定量的な性質がしばしば重要な意味を持つ。例えば，抑制作用鎖 $\{Yb''\underset{-n}{\rightarrow}\}$ においては，情報 b″ が複方向(例えば信号が 0 と 1 の両方向) に変動することにより抑制作用が実現されるものと，(信号が 0 または 1 のみの) 単方向にのみ制御されるものとでは重要な相違が生ずる。これに関して，まず次の定義を行う。

[定義23] 作用の性質や強度が単一の方向に変動することにより実現される抑制または解離作用を，単方向制御作用，複方向に変動制御させることにより実現されるものを，複方向制御作用と言う。

[定義24] 潜在危険制御系に，複数の複方向制御作用鎖があり，一方の作用の制御の変動方向が，他方の変動方向に依存するとき，前者を外依複方向作用鎖と言う。

{系15} 潜在危険制御系に外依複方向作用鎖が存在するとき，それとそれが依存する複方向制御作用鎖を結ぶ，複方向制御作用鎖からなる抑制連鎖が存在しなければならない。

解離要素または抑制要素が複方向制御作用を発生するためには，それらの要素がその作用に関して能動的状態になければならない。他方，単方向制御作用は，能動的状態または非能動的状態のいずれの要素からも生成され得る。従って，次の重要な基本的定理を得る：

[定理 7] 単方向制御作用鎖は，任意の形の解離または

抑制作用鎖によって構成され得るが，複方向制御作用鎖は，f′ または f″ 形の解離または抑制作用鎖では構成できない。

4. 潜在危険制御系の概念設計

4.1 ロボットにおける潜在危険制御系の構成事例

プロトタイプロボットには，多様な潜在危険が同定されている[15]。ここでは，軌道走行ロボットと，救助ロボットに焦点をあてて，潜在危険制御系の構成事例を示す。ここで用いる記号は以下の通りである。R：ロボットおよびその {S：センサ，F：センサの Fail Safe 機能，S′：センサのフォールト・トレランス系，C：処理部，B：制動部，T：移動機能系，D：移動機能系の駆動系下位要素，A：移動機能系の構造系下位要素，I：空気供給系}，N：環境，H：人間。

4.1.1 軌道走行ロボット

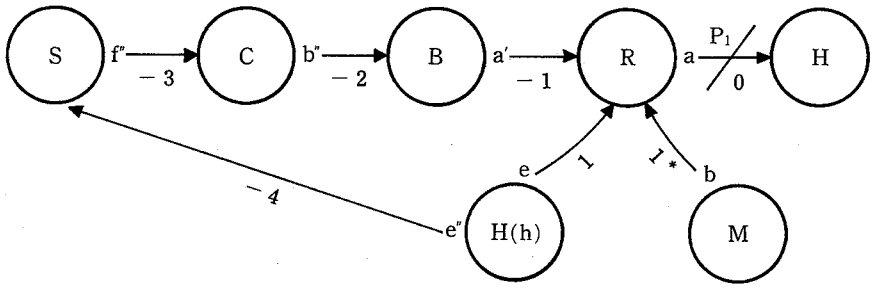
障害物を検出しながら，定められた経路を自律的に走行するロボットを想定する。「ロボット-環境」系に生ずる潜在危険として{$He \underset{1}{\rightarrow} Ra \underset{0}{\rightarrow} H(\cdot)$}，すなわち走行中のロボットが，障害物（人間など）と衝突する場合を特定する。

この潜在危険は，ロボットが経路上の障害物を検出して停止することにより抑制される。直接原因作用鎖 $\{Ra \underset{0}{\rightarrow}\}$ は，定理［1］より，抑制原理(4)における解離原理 P_1 で解離可能である。解離を実現するためには，次のような制御連鎖などからなる潜在危険制御系を構成することが必要である。

$$Hu_i'' \underset{-4}{\rightarrow} Su_j'' \underset{-3}{\rightarrow} Cu_k'' \underset{-2}{\rightarrow} Bu_l' \underset{-1}{\rightarrow} Ra \overset{P_1}{\underset{0}{\not\rightarrow}} H \qquad (1)$$

すなわち，センサ S は障害物の存在 $\{Hu_i'' \underset{-4}{\rightarrow}\}$ を検出して処理部へ $\{u_j'' \underset{-3}{\rightarrow}\}$ の作用を伝播する。C はこれを受けて制動部 B へ作用 $\{u_k'' \underset{-2}{\rightarrow}\}$ を伝播し，B が作動 $\{u_l' \underset{-1}{\rightarrow}\}$ してロボット R を停止させる。ここで，u_l' は「ロボットの運動エネルギ」を「他のエネルギ」に変換する働きをするため，「エネルギ伝播型解離作用 a′」としなければならない。ロボットが停止することによる潜在危険を無視するならば，この解離作用鎖 $\{a' \underset{0}{\rightarrow}\}$ は，ロボットの停止側のみの単方向制御作用鎖とすることができる。u_i'', u_j'' および u_k'' も同様に単方向制御作用鎖とすることができる。従って，定理［7］より，原則的に $u_i''=e''$ (or b″), $u_j''=f''$ (or a″or b″), $u_k''=f''$ (or a″or b″) とすることができる。

u_i'' と u_k' を f″ とすると，センサと処理部は，いわゆる安全検出型（すなわち系が安全なときに出力を発生



H,M,R,(h),(●),a,b,e : are same as in Fig. 1
B : Braking component of robot
C : Processor component of robot control system
S : Sensor of robot control system
a′ : Energy-transmission-type dissociation action
b″ : Information-propagation-type control action
e″ : Existence-form-type control action
f″ : Function-cessation-type control action
P_1: Action-source-control dissociation principle

Fig. 3 Conceptualization of a hazard control system for mobile robot
移動ロボットにおける潜在危険制御系の概念設計

し，危険となると出力を停止する）の構成と呼ばれ，f″としないときは，危険検出型（危険を検出して出力する）の構成とされる[16]。センサに安全検出型$\{Sf''\underset{-3}{\rightarrow}\}$，処理部に危険検出型$\{Cb''\underset{-2}{\rightarrow}\}$を採用すると，潜在危険制御系の概念設計がFig. 3として表わされる。

センサに断線故障が生ずると，系は停止側へ移行する。センサに短絡故障（s）が生ずると，$\{Sf''\underset{-3}{\rightarrow}\}$が$\{S_{(s)}\bar{b}\underset{3}{\rightarrow}\}$となり，定理[4]より反転連鎖が生成され，$\{a\underset{0}{\rightarrow}\}$の解離が不能となる。一方，反転作用鎖$\{a\underset{0}{\rightarrow}\}$は，定理[5]より原理$P_1$で解離可能である。これを実現するために，系にセンサの短絡故障に対するフエイルセイフ機能をもたせると，$\{a\underset{0}{\rightarrow}\}$が，Fig. 4のように解離される。

この潜在危険制御系では，原則的にセンサおよび処理部をf″形の抑制作用を行う安全検出形の系の要素として構成できるが，他の部分，すなわち$\{He''\underset{-4}{\rightarrow}\}$および$\{Ba'\underset{-1}{\rightarrow}\}$はf″形の抑制作用鎖またはf′形の解離作用鎖としては構成できない。

4.1.2　救助ロボット

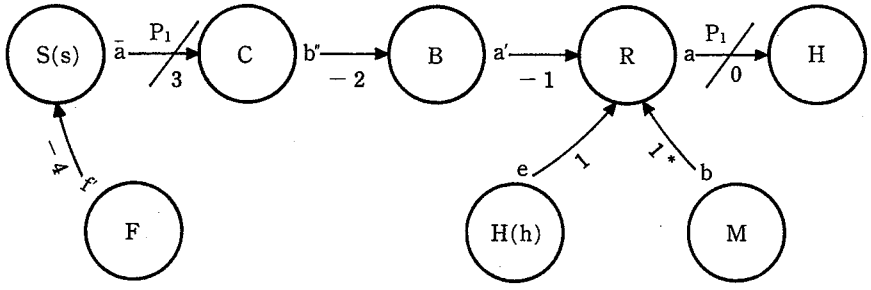
酸欠環境下に閉塞させられた被災者を救助するロボットを想定する。ロボットの使命は，(1)被災者を発見する，(2)被災者に人工呼吸を施す，ことである。ここでは潜在危険$\{He\underset{1}{\rightarrow}Nf\underset{0}{\rightarrow}H(\cdot)\}$，すなわち環境Nの酸素供給不履行による，窒息災害の危険性が特定される。

$\{Nf\underset{0}{\rightarrow}\}$は，定理[1]より，抑制原理(4)における解離原理P_4により解離される。これは，ロボットRがg′&g″型の解離作用を行うことによって実現される[定理2]。従って，潜在危険制御系は，次の制御連鎖などから構成されなければならない。

$$Hu_i''\underset{-6}{\rightarrow}Su_j''\underset{-5}{\rightarrow}Cu_k''\underset{-4}{\rightarrow}Du_l''\underset{-3}{\rightarrow}Tu_m''\underset{-2}{\rightarrow}\{(Rg'\underset{-1}{\rightarrow}Nf\overset{P_4}{\underset{0}{\rightarrow}}H)\&(Rg'\underset{-1}{\rightarrow}Rg''\underset{-0}{\rightarrow}H)\} \quad (2)$$

ここで$\{Tu_m''\underset{-2}{\rightarrow}\}$は，被災者からの距離情報，すなわち，近づいたか離れたかの複方向制作用鎖$\{Hu_i''\underset{-6}{\rightarrow}$すなわち$Hb''\underset{-6}{\rightarrow}\}$に従って，ロボットRを，前進・後退・旋回などの複方向に制御する外依複方向制御作用鎖$\{Ta''\underset{-2}{\rightarrow}\}$としなければならない。すると，{系15}より，制御連鎖(2)以外に，$\{Hb''\underset{-6}{\rightarrow}\}$と$\{Ta''\underset{-2}{\rightarrow}\}$を結ぶ抑制連鎖が存在しない条件下で，$u_j''$, u_k'', u_l''を全て複方向制御作用としなければならない。故に定理[7]から，u_j''およびu_k''を前節で述べた「安全検出型の抑制作用f″」として構成することは原理的に不可能となる。

ここで，センサSに異常（s）が生じると，$\{Sb''\underset{-5}{\rightarrow}\}$が$\{S_{(s)}\bar{f}\underset{5}{\rightarrow}\}$と反転し，$\{Nf\underset{0}{\rightarrow}\}$の解離が不能となる。一方，$\{S_{(s)}\bar{f}\underset{5}{\rightarrow}\}$は，解離原理$P_4$によって解離される。これは制御系に，センサのフォールト・トレランス系[17]を構成することにより，Fig. 5のように実現され，信頼性依存形の潜在危険制御系となる。



Symbols are as in Fig. 3 except the followings :
F ; Fail-safe function of sensor
f′ ; Function-cessation-type dissociation action
ā ; Energy-transmission-type reversal action
(s) ; Short-circuit failure of sensor.

Fig. 4　Conceptualization of a hazard control system with two a-type hazards
センサの短絡故障を考慮した潜在危険制御系の構成

4.2 木工丸のこ盤作業における潜在危険制御系

木工丸のこ盤による災害の70（%）以上は，作動中の刃物に作業者が接触することにより生じている[18]。すなわち主な潜在危険として{H(h)$e\underset{1}{\rightarrow}Wa\underset{0}{\rightarrow}$H(·)}が同定される。ここでHは作業者，Wは丸のこ刃，(h)は作業者（主として手指）が空間的に丸のこ刃に接近する変化，(·)は作業者に生ずる傷害をそれぞれ表している。

4.2.1 潜在危険抑制原理(3)の適用

この系では，系の相を：(イ)作業者の手指等が動作中ののこ刃付近に存在しない。(ロ)存在する；の2モードに分割することができる。接触予防装置Gや治具は，作用源Hの位置を制御し(P_1)，系の相が(イ)から(ロ)へ遷移させないようにすることによって直接原因作用鎖{Wa$\underset{0}{\rightarrow}$H(·)}の発現を抑止するものである。A-Cモデルでは次のように表わされる。

$$Ge'\underset{-2}{\rightarrow}H(h)\,e\overset{P_1}{\underset{1}{\not\rightarrow}}W \qquad (3)$$

4.2.2 潜在危険抑制原理(4)の適用

丸のこ盤作業では，小物加工，中抜き加工など接触予防装置を使用しにくい作業がある[19]。このとき，系は，(a)のこ刃が作動し，(b)手指がのこ刃に接触し得る状態にある，相に遷移するので，ここでは潜在危険抑制原理(4)を適用する必要がある。一例として次の制御連鎖などからかる潜在危険制御系が考えられる：

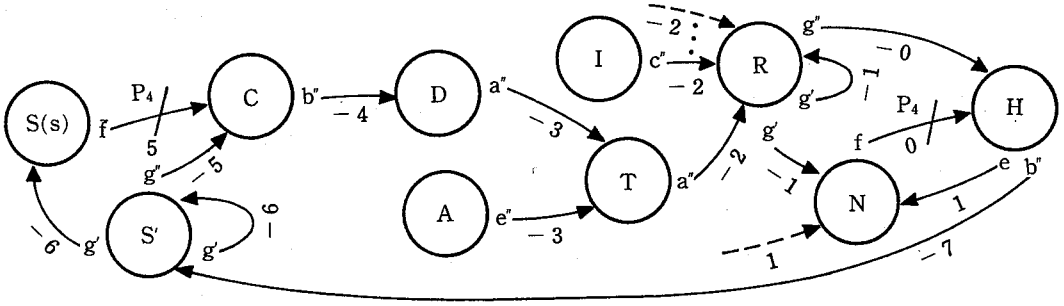
$$H(h)\,u_i''\underset{-4}{\rightarrow}Su_j''\underset{-3}{\rightarrow}Cu_k''\underset{-2}{\rightarrow}Bu_l'\underset{-1}{\rightarrow}Wa\overset{P_1}{\underset{0}{\not\rightarrow}}H \qquad (4)$$

すなわち，非常停止装置のセンサSは手指の接近H(h)を検出し，処理部Cへ抑制作用u_j''を行うことにより，処理部からのこ刃のブレーキ装置Bへ抑制作用u_k''が働き，解離作用u_l'が発現して制動がかかり，のこ刃は緊急停止される。

ここでは，解離作用鎖$\{u_l'\underset{-1}{\rightarrow}\}$は，のこ刃の停止方向のみの単方向制御作用鎖とすることができる。ブレーキ装置Bは，部分的にf''を行う要素とa'(運動エネルギ他のエネルギに変換する）を行う要素とに分割できるが，最終的にはa'を行わなければならないので，$u_l'=a'$とおく。u_i'', u_j'', u_k''も全て単方向制御作用鎖とすることができるので，センサおよび処理部は原則的に安全検出型の抑制作用鎖$\{f''\underset{-i}{\rightarrow}\}$とすることができる。丸のこ盤の潜在危険制御系はFig. 6のように表される。

4.3 考　察

Fig. 4とFig. 5を比較してわかるように，解離形1(P_1,P_2,P_3)の適用は，解離形2(P_4)に比し，構造が単純で，冗長系あるいは多重系の同時故障を考慮する必要がないなど，すぐれた利点をもつ。しかし，どち



Symbols are as in Fig. 4 except the followings :
N ; Environment, I ; Air-supply system of robot, T ; Transfer system of robot,
A ; Structure sub-system of transfer system, D ; Driving sub-system of transfer system,
S' ; Fault-tolerance function of sensor,
g'&g'' ; Function-substitution-type dissociation action,
a'' ; Energy -transmission -type control action, c'' ;Agency-transfer-type control action,
$\bar{f}$; Function-failure-type reversal action, (s) ; Sensor failure,
P_4 ; Function-substitution-control dissociation principle.

Fig. 5 Conceptualization of a hazard control system with rescue robot
救助ロボットによる潜在危険制御系の概念設計

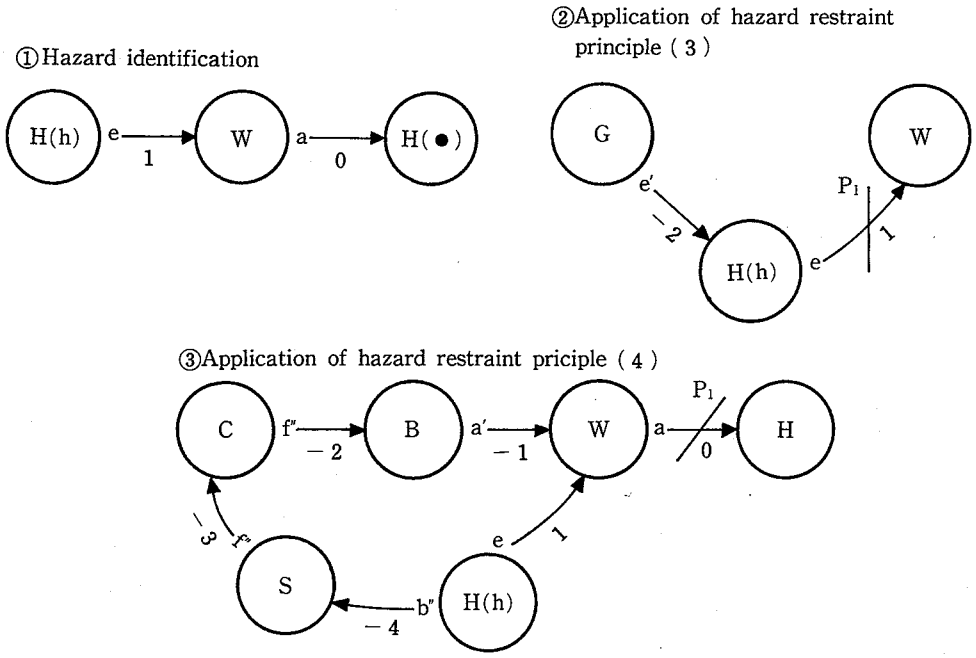


Fig. 6　Conceptualization of hazard control system for buzz saw machine
丸のこ盤における潜在危険制御系の概念設計

らの解離形が採用できるかは，解離しようとする作用鎖，または反転作用鎖と，系の構造に依存することになる。

本報では，センサシステムの故障のみを取り上げて，その制御系を例示した。他にも多様な故障モードが存在するので，それらを全て検討する必要がある。本報での構成事例からもわかるように，現実の系では，全ての異常モードに対して，解離形1の制御系で対処する，すなわち「絶対安全な系」とすることは，原理的に不可能である。従って，実際上の系では，潜在危険抑制原理(3)，(4)以外の安全措置も，総合的かつ効果的に検討していくことが肝要である。この際，フェイルセイフといえども確率事象であり[20]，抑制手段の優先順位の決定などのために，残存リスクの確率論的評価，すなわち安全計画過程(3)，(4)の実施が重要となる[21]。

潜在危険制御系に関する議論は，①潜在危険，②解離される作用鎖，③解離すに関する細目（解離原理，解離作用，その定量的制御方式など），④制御連鎖に関する細目（生じ得る変化，反転作用の解離など）を特定して行われることが肝要であり，そのためには安全計画の第1段階の潜在危険の同定が系統的に行われていなければならない。その理由として，

(1)　高度なロボットにより構成される複雑な系では，未知の現象も含めて，一般に生じ得るすべての変化および潜在危険を事前に容易には特定できない。

(2)　一つの系内に複数の潜在危険が生じ，それらおのおのの潜在危険制御系間において，解離または抑制作用鎖の制御の方向が逆になることがある。

5. 結　論

フェイルセイフなどの概念は，各産業分野でそれぞれ異なったものとして用いられている。これは，それらの概念が，機械，電子，情報，化学などの異なる工学体系間に共通して適用可能な潜在危険生成理論に立脚して構築されていないためである。

本報では，一般潜在危険生成理論でもある作用一変化と作用連鎖モデルにもとずき，まず潜在危険抑制過程を潜在危険抑制原理として体系化した。次に，潜在危険抑制過程の最後の防衛線である，発現しつつある潜在危険を最終的なき損の発生以前に解消する制御系，すなわち潜在危険制御系の構成原理を制御連鎖による作用鎖の解離理論として一般化した。さらに，いくつかの実システムに対して，潜在危険制御系の概念設計を示した。

(昭和63年3月29日受理)

参考文献

1）榎本，佐々木，電気鉄道におけるフォールトトレランス技術，電学誌，Vol.107，No.4，(昭62)，282

2）佐藤，井上，人間—ロボット系の安全性評価（第1報），機械学会論文集，51-468C（昭60），2188

3）佐藤，井上，熊本，人間—ロボット系の安全性評価(第2報)，機械学会論文集，52-474C，(昭61)，823

4）佐藤，井上，熊本，人間—ロボット系の安全性評価(第3報)，機械学会論文集，52-475C，(昭61)，1110

5）Sato，Y.，Kumamoto，H.，and Inoue，K.，On hazard identification and analysis of human-robot system, Proc. Japan-USA Sympsium on Flexible Automation, Osaka Japan (1986)，679.

6）Sato，Y.，Iuoue.，K.，and Kumamoto，H.，The Safety Assessment of Human-robot Systems (4th Report, Evaluation of Hazard Control Measures for an Industrial Robot Handling Work Pieces, JSME International Journal, Vol. 30, No.260, (1987), 350.

7）佐藤，新技術を用いたシステムに生ずる潜在危険の評価，RIIS-SRR-86，No.1，(1986)，103.

8）E. J. Henley, H. Kumamoto, Designing for Reliability and Safety Control, Prentice-Hall Inc, Engle-wood Cliffs, N. J., 1985

9）奥村，コンピュータを用いたフェイル・セイフなシステム，情報処理，22-9，(1981)，P.863

10）文献2）の2189ページ.

11）佐藤，井上，人間—ロボット系の安全性評価（第5報)，機械学会関西支部総会論文講演抜刷，No.911A，3/18（昭63)，神戸.

12）文献3）の829ページ

13）文献2）の2189ページ.

14）文献7）の107ページ.

15）文献2）の2192ページ.

16）佐藤，井上，ロボットの安全性について，機学誌，Vol.90，NO.827，(昭62)，1351.

17）当麻，南谷，フォールト・トレランス・システム，電子情報通信学会誌，63-10，(1980)，P.1031.

18）佐藤，深谷，江川，木工機械作業における安全対策のMORTによるシステム的検討，RIIS-SRR-82，No.1，(1982)，24.

19）文献18）の32および33ページ.

20）佐々木，鉄道における安全技術，電子情報通信学会技術研究報告，S87-13，12/22，(1987)，P.30.

21）文献16）の1355ページ.