人間 - ロボット系の安全性評価*

(第5報, 潜在危険制御系の構成原理)

佐藤吉信^{*1}, 井上 紘一^{*2}The Safety Assessment of Human-Robot Systems
(5th Report, The Constitution Principles of Hazard-Control Systems)

Yoshinobu SATO and Koichi INOUE

Robots, which are constructed from many elements that are related to various engineering systems including mechanical systems, electronic systems, artificial intelligence and so on, are going to be utilized in various fields. It is necessary to examine overall safety techniques for the establishment of robot safety. First, hazard control principles are systematized based on the accident-causation theory "Action-change & Action-chain Models". Secondly, the constitution principles of hazard control systems that are the final line of defense against hazards are generalized and systematized using the theory of hazard control chains, in order that the principles can be applied to the overall fields of engineering. Finally, illustrative examples constituting hazard control systems are demonstrated for some robots, such as a transfer robot, a rescue robot etc., based on the principles.

Key Words: System Safety Engineering, Robot, Safety, Fail Safe System, Fault Tolerant System, Man Machine System, Action Change and Action Chain Model, Hazard Control System, Hazard Control Chain Theory

1. 緒 言

本研究は, 現在実用化されているものも含めて, 将来出現の予想されるロボットの安全性向上に貢献することを目的としている⁽¹⁾⁻⁽⁴⁾.

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などを実現するためのソフト体系などから構成されているため, その安全性向上には総合的な安全計画の実施が必要である. その重要な過程として, 潜在危険抑制措置の検討があげられている⁽⁵⁾. 個々のロボットに対する潜在危険抑制措置の検討を効果的に行うためには, 潜在危険抑制原理が一般化・体系化されている必要がある⁽⁶⁾. しかしながら現状は必ずしもその必要性が満足されていない. 例えば, 潜在危険抑制措置の概念としてフェイルセーフ系 (Fail-safe System) がある. この術語はもともと鉄道信号の分野で用いられ始めたものであるが, 現在では原子炉, 航空機, プラント, 道路交通管制システム, 医用電子機器など非常に多様な分野で使用され, その概念もそれぞれ異なったものとなっている⁽⁷⁾. こ

のような基本的手法の概念上の食違いは, 異なる工学体系間での議論に混乱を生じさせることがある. このようなことが生じている原因は, それらの概念が異なる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一般化されていないためと考えられる.

本報では, 一般潜在危険生成理論でもある作用連鎖モデルにもとづき, 潜在危険抑制過程を体系化するとともに, 潜在危険の制御連鎖理論を導入して潜在危険制御系の構成原理を一般化する. また, 具体的な人間-ロボット系への構成原理の適用事例を示す.

2. 潜在危険の抑制過程

潜在危険抑制原理を一般化・体系化するためには, その前段階として災害発生理論, または潜在危険生成理論が異なる工学体系間でも整合できるよう一般化される必要がある. 従来, 災害発生過程を論じた一般理論として「災害発生過程の5要因モデル」などがあげられる⁽⁸⁾. しかしながら, それらの一般理論は, 概念的で具体性あるいは包括性に欠けるなどの問題点があった. 本研究では, 文献(1)において, 災害発生過程を潜在危険の生成とその発現過程として把握し, 作用-変化と作用連鎖モデルによって論じている. これにより, 潜在危険の生成と発現過程が具体的かつ包括的に把握

* 昭和63年3月18日 関西支部第63期定時総会講演会において講演, 原稿受付 昭和62年6月3日.

^{*1} 正員, 労働省産業安全研究所 (〒108 東京都港区芝5-35-1).

^{*2} 正員, 京都大学工学部 (〒606 京都市左京区吉田本町).

されるようになった。

このモデルによると、災害発生の防止は、潜在危険すなわち作用連鎖の生成と発現の抑制にほかならない。したがって、潜在危険の抑制過程は次のような抑制原理に体系化される。

- (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

潜在危険抑制過程(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。

(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。

(3)において作用連鎖生成相とは、要素の特性を表すモードによって規定される系の相を意味する⁽⁹⁾。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。

(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止するものである。これは、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。

以下には、潜在危険抑制過程の最後の防衛線である潜在危険制御系の構成原理を論ずる。

3. 潜在危険制御系の構成原理

3.1 解離と解離原理および解離作用 作用-変化と作用連鎖モデルの基本的概念は文献(1)に述べられている。その拡張概念を次のように定義することにより、作用鎖の解離、解離原理および解離作用に関する基本的性質を明らかにする。

〔定義1〕系の要素とは、人間、装置、材料、構造物、環境条件あるいは達成目標などの心理的要因も含んだ系を構成している分割可能な系の部分とする。

〔系1〕要素はさらに下位要素に分割できる場合がある。例えば、上位要素ロボットは、下位要素、構造系、駆動系、制御系、検出系要素などに分割できる。

〔系2〕作用の伝ばは、要素間および下位要素と上位要素間で行われ得る。

〔系3〕ある要素が a, b, c, d または e 形の作用を行い得るとき、要素はそれらの作用に関して能動的な状態にあり、 f 形の作用を行い得るとき、要素はその作用を行い得る非能動的状態へ遷移している。

〔定義2〕ある作用を行う要素をその作用に関して作用要素、作用が行われる要素をその作用に関して被作用要素という。

〔定義3〕作用鎖の解離とは、ある特定された変化と作用の生起の条件下で、発現しようとするある作用鎖を切断する(すなわち作用の授受が現実化することを抑止する)ことと定義する。

〔系4〕ある作用鎖の解離により、これが誘因作用鎖(誘因作用による作用鎖)となって生ずる次の作用鎖の発現確率が減少し、これが直接原因作用鎖(直接原因作用による作用鎖)の場合ではそれによるき損の発生が抑止される。

〔定義4〕解離作用とは、作用要素に作用して、その作用要素からのある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5〕解離作用を行う要素を、その解離作用に関して解離要素という。

〔定義6〕作用源の制御とは、作用要素が能動的な状態にあることにより生ずる作用鎖を、その作用要素の作用源となるエネルギー状態、化学的性質などを制御することにより解離することと定義する。

〔定義7〕作用経路の制御とは、作用要素が能動的な状態にあることにより生ずる作用鎖を、その作用要素と被作用要素との間の作用経路を制御して解離することと定義する。

〔定義8〕作用源と作用経路の制御とは、作用要素が能動的な状態にあることにより生ずる作用鎖を、その作用源および作用経路を制御して解離することである。

〔定義9〕不履行機能の代替制御とは、作用要素が非能動状態へ遷移することにより生ずる作用鎖を、能動的な要素がその機能を代替することにより解離することと定義する。

〔系5〕作用鎖の解離は、次の原理に一般化される。

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

作用鎖の解離と解離原理に関する基本的な関係が、定義〔6, 7, 8, 9〕, 系〔3, 5〕などから定理1として得られる。

〔定理1〕 a, b, c, d, e 形の作用鎖は、原理的にすなわち技術的に可能であれば、解離原理 P_1, P_2, P_3 のいずれかによってのみ解離され、 f 形の作用鎖は原理的に解離原理 P_4 によってのみ解離される。

〔定義10〕 解離作用の形を次のように定義する。

(a') エネルギー伝ば形: 解離要素と作用要素間でエネルギー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ー量としてよりは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解離作用。

(c') 作因物転移形: 化学物質、重量物など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、エネルギー、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: エネルギー、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もない、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6〕 解離作用は、 a', b', c', d', e', f' および $g' \& g''$ 形に分類される。

解離原理と解離作用の基本的関係が、定義〔6, 7, 8, 9, 10〕 および系〔6〕などから定理〔2〕として得られる。

〔定理2〕 解離原理 P_1, P_2, P_3 は原理的に a', b', c', d', e' または/および f' 形の解離作用によってのみ実現され、解離原理 P_4 は原理的に $g' \& g''$ 形の解離作用によってのみ実現される。

以上の検討の結果得られた解離原理と解離作用および解離され得る作用鎖の関係を表1として示す。

3.2 解離の図式表現 作用鎖を解離するためには、その必要条件となる解離作用鎖がすべて発現しなければならない。図1は、1組の解離作用鎖が解離を実現する場合の図式表現である。図1中、解離形式1は、解離原理 P_1, P_2, P_3 による解離を、解離形式2は解離原理 P_4 による解離を表している。

表1 解離原理とそれを実現する解離作用および解離可能な作用鎖との関係

PRINCIPLES OF DISSOCIATION OF ACTION-LINKS	POSSIBLE DISSOCIATION-ACTION TYPES TO REALIZE PRINCIPLE	ACTION TYPES WHICH PRINCIPLE CAN DISSOCIATE THEORETICALLY
CONTROL OF ACTION-SOURCE	a', b', c', d', e', f'	a, b, c, d, e
CONTROL OF ACTION-PATH	a', b', c', d', e', f'	a, b, c, d, e
CONTROL OF ACTION-SOURCE & PATH	a', b', c', d', e', f'	a, b, c, d, e
CONTROL BY SUBSTITUTION FOR FAILED FUNCTION	$g' \& g''$	f

〔DISSOCIATION TYPE 1〕

$$i=1, 2, \dots, 5 \quad j=1, 2, \dots, 6 \quad k=1, 2, 3$$

$$u_1=a, u_2=b, u_3=c, u_4=d, u_5=e \quad u'_1=a', u'_2=b', u'_3=c', u'_4=d', u'_5=e', u'_6=f'$$

〔DISSOCIATION TYPE 2〕

図1 解離原理と解離作用鎖

作用連鎖の記法は文献(1)で述べられている。ここで解離形式1では、解離要素 Y から要素 X へのアークとアルファベット a', b', c', d', e', f' で、解離形式2ではアークとアルファベット $g' \& g''$ でそれぞれ解離作用鎖とその形を示している。アークの下に数字 $-m$ および $-m+1 (m=1, 2, 3, \dots)$ は、直接原因作用鎖 ($m=0$) からの連鎖順位に -1 をかけたものである。

解離形式1では、発現しようとしている作用鎖 $u_i \rightarrow_{-1} (i=1, 2, \dots, 5)$ が解離作用鎖 $u'_j \rightarrow_{-m} (j=1, 2, \dots, 6)$ によって解離原理 $P_k (k=1, 2, 3)$ で解離されている。解離形式2では、作用鎖 $f \rightarrow_{-m-1}$ が解離作用鎖 $g' \rightarrow_{-m}$ および $g'' \rightarrow_{-m+1}$ によって解離原理 P_i で図1のように解離されている。解離される作用鎖に斜線および解離記号 $P_i (i=1, 2, 3, 4)$ を付記することによって、その解離とそれを実現する解離原理を表す。

3.3 制御連鎖と抑制作用 一般的に、解離作用鎖を発現させるためには、解離要素へ結びつくある種の作用連鎖が生成される必要がある。これに関して、以下の定義を行う。

〔定義11〕解離要素へ結びつく単連鎖で、その生成がある解離作用鎖を発現させるための必要条件となる作用連鎖を抑制連鎖、その発現が抑制連鎖生成の必要条件となる作用鎖を抑制作用鎖、抑制連鎖の構成に必要な要素を抑制要素という。

〔定義12〕ある解離作用鎖およびこれを実現するある抑制連鎖からなる単連鎖を制御連鎖という。

〔系7〕制御連鎖は、最終的にある作用要素に結びつく抑制要素および解離要素間での方向性のある抑制作用鎖および解離作用鎖の連鎖として表現でき、ある抑制要素または解離要素へ結合される抑制作用鎖の発現は、その抑制要素から次の抑制作用、または解離要素からの解離作用が発現するための必要条件となっている。

〔系8〕一般に、ある解離作用鎖が発現するためには、いくつかの制御連鎖、すなわちいくつかの抑制連鎖が生成されることが必要である。

〔定義13〕ある解離を実現するため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いう。

〔定義14〕抑制作用の形を次のように定義する。

(a'') エネルギー伝ば形：エネルギー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り生ずる抑制作用。

(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：エネルギーの伝ば、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9〕抑制作用は、 a'', b'', c'', d'', e'' および f'' 形に分類・一般化される。

3.4 制御連鎖の反転と反転作用鎖の解離

〔系10〕何らかの原因により、抑制作用鎖または解離作用鎖の発現に失敗すると、その抑制作用または解離作用が生じないことによるある種の作用が生ずる。

この作用によって形成される作用鎖に関して次のように定義する。

〔定義15〕抑制作用鎖または解離作用鎖の発現に失敗することを抑制作用鎖または解離作用鎖が反転するといい、反転により生ずる作用鎖を反転作用鎖という。

〔定義16〕反転作用の形を次のように定義する。

(a) エネルギー伝ば形：エネルギーの授受が行われることにより生ずる反転作用。

(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反転作用。

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

(d) 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。

(e) 存在形態形：エネルギーの伝ば、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 f 形以外の反転作用。

(f) 機能不履行形：抑制要素または解離要素が能動的な状態にあることによって生ずる a'', b'', c'', d'', e'' 形の抑制作用、または $a', b', c', d', e', g' \& g''$ 形の解離作用が履行されないことにより生ずる反転作用。

〔系11〕反転作用は、 $\bar{a}, \bar{b}, \bar{c}, \bar{d}, \bar{e}$ および $\bar{f}$ 形に分類・一般化される。

解離作用または抑制作用の反転に関する基本的法則が、定義〔4, 10, 11, 14, 15, 16〕, 系〔6, 9, 11〕などより定理〔3〕として得られる。

〔定理3〕解離作用 $u'_i (u'_i = a', u'_2 = b', u'_3 = c', u'_4 = d', u'_5 = e'), g' \& g''$, または抑制作用 $u'_j (u'_1 = a'', u'_2 = b'', u'_3 = c'', u'_4 = d'', u'_5 = e'')$ によって構成される作用鎖

が反転すると、反転作用 $\bar{f}$ が生じ、 f' または f'' による作用鎖が反転すると一つまたは複数の反転作用 $\bar{u}_k$ ($\bar{u}_1 = \bar{a}$, $\bar{u}_2 = \bar{b}$, $\bar{u}_3 = \bar{c}$, $\bar{u}_4 = \bar{d}$, $\bar{u}_5 = \bar{e}$) が生ずる。すなわち次の反転公式が成立する。

$$[u_i \rightarrow] \xrightarrow{-m \text{ reverse}} [\bar{f} \rightarrow] \dots\dots\dots (1)$$

$$(i=1, 2, \dots, 5 \quad m=1, 2, 3, \dots)$$

$$[f' \rightarrow] \xrightarrow{-m \text{ reverse}} [\bar{f} \rightarrow] \dots\dots\dots (2)$$

$$(m=1, 2, 3, \dots \quad j=1, 2, \dots, (\text{and/or}) 5)$$

$$[(g' \rightarrow) \& (g'' \rightarrow)] \xrightarrow{-m+1 \text{ reverse}} [(\bar{f} \rightarrow) \& (\bar{f} \rightarrow)] \dots\dots\dots (3)$$

$$(m=1, 2, 3, \dots)$$

$$[u_k'' \rightarrow] \xrightarrow{-n \text{ reverse}} [\bar{f} \rightarrow] \dots\dots\dots (4)$$

$$(k=1, 2, \dots, 5 \quad n=2, 3, 4, \dots)$$

$$[f'' \rightarrow] \xrightarrow{-n \text{ reverse}} [\bar{u}_l \rightarrow] \dots\dots\dots (5)$$

$$(n=2, 3, 4, \dots \quad l=1, 2, \dots, (\text{and/or}) 5)$$

抑制作用鎖の反転により生ずる反転連鎖に関して、系〔7〕などから次の基本的性質が得られる。

〔定理4〕ある作用鎖 $Xu_r \rightarrow$ ($r=1, 2, \dots, 6 \quad m=1, 2, 3, \dots$) の解離作用鎖を実現するための抑制連鎖 $\{Y_n u_i'' \rightarrow Y_{n-1} u_j'' \rightarrow \dots Y_1 u_k'' \rightarrow Y\}$ ($i=1, 2, \dots, 6$ $j=1, 2, \dots, 6$ $k=1, 2, \dots, 6$ $n=1, 2, 3, 4, \dots$) において、変化 y_p が Y_p ($1 \leq p \leq n$) に生起することにより抑制作用鎖 $Y_p u_l'' \rightarrow$ ($l=1, 2, \dots, 6$) が反転して反転作用鎖 $Y_p(y_p) \bar{u}_h \rightarrow$ ($h=1, 2, \dots, 6$) となると、 y_p の変化が他の要素の変化に独立、および y_p 以外に反転を生じさせる変化が生起していない条件下で、反転連鎖 $\{Y_p(y_p) \bar{u}_h \rightarrow Y_{p-1} \bar{u}_s \rightarrow \dots Y_1 \bar{u}_q \rightarrow Y\}$ ($s=1, 2, \dots, 6$ $q=1, 2, \dots, 6$) が生成される。これにより解離作用鎖が反転するため解離が実現しない。

反転作用は作用と同じ性質をもつので、反転作用鎖の解離には作用の解離と同じ原理が適用される。

〔定理5〕 $\bar{a}$, $\bar{b}$, $\bar{c}$, $\bar{d}$, $\bar{e}$ 形の反転作用鎖は原理的に解離原理 P_1 , P_2 , P_3 のみによって、また $\bar{f}$ 形の反転作用鎖は原理的に P_4 のみによって解離される。

作用を解離する解離作用鎖の発現にその抑制連鎖が生成されることが必要であると同様に、一般的に反転作用鎖を解離する解離作用鎖の発現にも抑制連鎖の生成が必要である。定理〔4〕で生成された反転連鎖の任意の反転作用鎖を解離すると、他に変化が生じていない条件下で、次々と抑制作用鎖が発現される必要条件が満足され、制御連鎖が部分的に復活する。この性質に関して定理〔6〕が得られる。

〔定理6〕定理〔4〕で生成された反転連鎖

$\{Y_p(y_p) \bar{u}_h \rightarrow Y_{p-1} \bar{u}_s \rightarrow \dots Y_1 \bar{u}_q \rightarrow Y\}$ における任意の反転作用鎖 $Y_w \bar{u}_t \rightarrow$ ($t=1, 2, \dots, 6 \quad 1 \leq w \leq p$) を解離することにより、 y_p のほかに反転を生起させる変化が生じていない条件下で、その解離作用鎖、その解離を実現させるための抑制連鎖、および解離により復活した部分抑制連鎖 $\{Y_{w-1} u_v'' \rightarrow Y_{w-2} u_z'' \rightarrow \dots Y_1 u_k'' \rightarrow Y\}$ が生成されることにより、再び作用鎖 $Xu_r \rightarrow$ の解離が可能となる ($v, z=1, 2, \dots, 6$)。

3.5 作用の定量的制御方式 作用の制御では、制御の定量的側面も非常に重要である。例えば、抑制作用鎖 $Y_p a_{q-r}''$ において、作用すなわち授受されるエネルギーの強度を増大または減少のいずれかの単一方向へ固定することにより制御を行う方式と、増大と減少の複方向へ変化させることによる制御を行う方式における違いが非常に重要な意味をもつ場合がある。これに関して、まず次の定義を行う。

〔定義17〕単方向制御作用鎖：作用の強度や性質が単一方向に制御されることにより生ずる解離（抑制）作用鎖。

複方向制御作用鎖：作用の強度や性質が複数の方向に制御されることにより生ずる解離（抑制）作用鎖。

作用の強度や性質を複方向に変化させるには、作用要素がその作用に関して能動的な状態になければならない。これに対して、能動的または非能動的のいずれかの方向のみに固定された作用は、要素が能動的状態にあることにより生ずる作用、または要素が非能動的状態に遷移することにより生ずる作用のいずれかによって実現される。これより定理〔7〕を得る。

〔定理7〕単方向制御作用鎖は、原理的に解離（抑制）作用 $a', b', c', d', e', f', g' \& g''(a'', b'', c'', d'', e'', f'')$ によって構成されるが、複方向制御作用鎖は、原理的に解離（抑制）作用 $a', b', c', d', e', g' \& g''(a'', b'', c'', d'', e'')$ のみによって構成される。

4. 潜在危険制御系の構成事例

センサにより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、酸欠環境下に閉そくさせられた被災者を救助するロボット、患部に発生した悪性しゅようを外科的に除却するロボットを想定する。この種のロボットにはいくつかの潜在危険が同定されている⁽¹⁰⁾。ここでは、それぞれ以下に示すような潜在危険を特定して、その潜在危険制御系の構成事例を示す。

4.1 軌道走行形ロボット 系の基本的要素を、

$H(h)$ (人間, そのロボットへの干渉), R (ロボット), $B(R)$ の制動系要素), $A(B)$ の構造系下位要素), $E(B)$ のエネルギー変換系下位要素), $C(R)$ の制御系要素), $S(R)$ のセンサ)として, 走行中のロボットと人間との衝突による直接潜在危険 $He \rightarrow Ra \rightarrow H$ を特定する.

ロボットが停止することにより衝突が回避される. すなわち直接原因作用鎖 $Ra \rightarrow H$ は, 定理 [1] より解離原理 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.

$$H(h)e \xrightarrow{-5} Sb \xrightarrow{-4} Cb \xrightarrow{-3} Ea \xrightarrow{-2} Ba \xrightarrow{-1} R \quad \cdots (6)$$

$$Ae \xrightarrow{-2} Ba \xrightarrow{-1} R \quad \cdots (7)$$

ロボットが停止することにより生ずる潜在危険は無視できるものとする, 解離作用鎖 $Ba \xrightarrow{-1} R$ は, 定理 [7] よりロボットの停止側への単方向制御作用鎖とすることができる. したがって, 制御作用鎖 $Ea \xrightarrow{-2}$ (運動エネルギーを熱または電気的エネルギーに変換する), $Cb \xrightarrow{-3}$ (停止信号を与える), $Sb \xrightarrow{-4}$ (障害物検出信号を与える), $H(h)e \xrightarrow{-5}$ (人間の存在から生ずる), $Ae \xrightarrow{-2}$ (構造体としての力学的存在形態作用) はいずれも原理的にロボットの停止側への単方向制御作用鎖とすることができる.

ここで, S および C は, 障害物を検出したときに出力を発生するいわゆる危険検出形の回路構成が仮定されている. 障害物を検出しないときのみ出力を発生するいわゆる安全検出形の回路構成を仮定することでも

きる. この場合, 次のような制御連鎖などからなる制御系が構成される.

$$H(h)e \xrightarrow{-6} Sf \xrightarrow{-5} Cf \xrightarrow{-4} Ef \xrightarrow{-3} Ea \xrightarrow{-2} Ba \xrightarrow{-1} R \quad \cdots (8)$$

$$A'f \xrightarrow{-3} A'e \xrightarrow{-2} Ba \xrightarrow{-1} R \quad \cdots (9)$$

ここでは E を f 形の抑制作用を行う要素として構成可能な部分 E'' と不可能な部分 E' とに分割している. A も同様に A'' と A' に分割している.

次に, S に断線 (s) または短絡 (s') 故障が発生すると, $Sb \xrightarrow{-4}$, $Sf \xrightarrow{-5}$ がそれぞれ $S(s)\bar{f} \xrightarrow{-4}$, $S(s')\bar{b} \xrightarrow{-5}$ と反転するための, 定理 [4] より, 制御連鎖 (6), (8) が反転して解離が実現されない.

図2は, 危険検出形センサの場合の反転作用鎖の解離を表したものである. ①では, 系に S' (センサのフォルトトレランス系要素)⁽¹¹⁾⁽¹²⁾を解離要素として構成して, 定理 [5] より, 解離原理 P_4 で $S(s)\bar{f} \xrightarrow{-4}$ を解離している. ②では, 解離要素として V (センサ断線検出系要素)を構成して, $C\bar{f} \xrightarrow{-3}$ を P_4 で解離している. こうして, それぞれ再び $Ra \rightarrow H$ の解離が実現される.

図3では, 系に解離要素 F (センサの短絡故障に対するフェイルセーフ機能要素)⁽¹³⁾を構成することにより, $S(s')\bar{b} \xrightarrow{-5}$ を P_1 で解離している.

4.2 救助ロボット 系の基本的要素を, H (被災者), N (環境), R (ロボット), $I(R)$ の人工呼吸機能系要素), $T(R)$ の被災者探索移動系要素), $A(T)$ の構造系下位要素), $D(T)$ の駆動系下位要素) $C(R)$ の制御系要素

H: Human R: Robot B: Braking and Steering System of R A: Structure Sub-system of R
E: Energy-transduction Sub-system of B C: Control System of R S: Sensor of R
S': Fault-tolerance System for S V: Sensor-disconnection Detection System of R

図2 軌道走行形ロボットの潜在危険制御系の構成事例 (危険検出形センサ)

素), $S(R$ のセンサ)として, 環境 N の酸素供給不履行による直接潜在危険 $Nf \rightarrow H$ およびセンサ故障によるロボットの救助失敗の間接潜在危険を特定する。

$Nf \rightarrow$ を P_4 で解離するためには, 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必要がある。

$$Hb'' \rightarrow_{-6} Sb'' \rightarrow_{-5} Cb'' \rightarrow_{-4} Da'' \rightarrow_{-3} Ta'' \rightarrow_{-2} \{(Rg' \rightarrow_{-1} N) \& (Rg' \rightarrow_{-1} Rg'' \rightarrow_{-0} H)\} \dots\dots\dots (10)$$

$$Ae'' \rightarrow_{-3} Ta'' \rightarrow_{-2} \{(Rg' \rightarrow_{-1} N) \& (Rg' \rightarrow_{-1} Rg'' \rightarrow_{-0} H)\} \dots\dots\dots (11)$$

$$Ic'' \rightarrow_{-2} \{(Rg' \rightarrow_{-1} N) \& (Rg' \rightarrow_{-1} Rg'' \rightarrow_{-0} H)\} \dots\dots\dots (12)$$

ここでは, $Rg' \rightarrow_{-1} Rg'' \rightarrow_{-0}$ は呼吸量の増加と減少の複方向制御とし, $Ta'' \rightarrow_{-2}$ も速度の増加と減少の複方向制御とすると, $Da'' \rightarrow_{-3}$, $Cb'' \rightarrow_{-4}$, $Sb'' \rightarrow_{-5}$ などを複方向制御作用鎖としなければならないので定理[7]より, 4.1 節のような安全検出形センサを用いることはできない。したがって, センサの故障 (変化 s) による $S(s) \bar{f} \rightarrow_{-5}$ は, 定理 [5] より, 解離要素 S' (センサのフォルトトレランス系要素) によって図 4 のように解離される。

4.3 外科ロボット 系の基本的要素を, H (患者), R (ロボット), $A(R$ の構造系要素), $O(R$ の作動系要素), $C(R$ の制御系要素), $S(R$ のセンサ)として, 悪

性しゅようの転移による直接潜在危険 $Hc \rightarrow_0 H$ とセンサの異常によるしゅよう除去の失敗による間接潜在危険を特定する。

$Hc \rightarrow_0$ を P_1 で解離するためには, 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必要がある。

$$Hb'' \rightarrow_{-5} Sb'' \rightarrow_{-4} Cb'' \rightarrow_{-3} Oa'' \rightarrow_{-2} Ra'' \rightarrow_{-1} H \dots\dots\dots (13)$$

$$Ae'' \rightarrow_{-2} Ra'' \rightarrow_{-1} H \dots\dots\dots (14)$$

ここで $Ra'' \rightarrow_{-1}$ は, 患部の状況に従って作用強度の増大と減少の微妙な制御を繰返す複方向制御作用鎖となり, その制御を表現するために $Oa'' \rightarrow_{-2}$, $Cb'' \rightarrow_{-3}$, $Sb'' \rightarrow_{-4}$ なども複方向制御作用鎖となる。したがって, センサの異常 (変化 s) により生ずる反転作用鎖の解離は, 系に解離要素 S' (センサのフォルトトレランス系要素) を構成することにより図 5 のようにして行われる。

4.4 考察 図 3 のような狭義のフェイルセーフ系⁽¹⁴⁾の信号系への適用は, 図 2 のような多重系による潜在危険制御系に比し, 構造が単純で冗長系の同時故障を考慮する必要がないなどのすぐれた利点をもつ。しかし, 制動時にロボットの転倒回避も制御するような高級な制動系をもつ歩行形ロボット, あるいは事例のような救助ロボット, 外科ロボットでは, 一般的に信号系からの抑制作用鎖が複方向制御となり, 信号系

H, R, C, B, S: are same as in Fig.2. A'', A': Structure Sub-system of B E'', E': Energy-transduction Sub-system of B F: Fail-safe Function for Short-circuit of S

図 3 軌道走行形ロボットの潜在危険制御系の構成事例 (安全検出形センサ)

H, R, C, S, S': are as in Fig.2. N: Environment I: Air-supply System of R T: Transfer System of R A: Structure Sub-system of T D: Driving and Steering Sub-system of T

図 4 救助ロボットによる潜在危険制御系の構成事例

図5 外科ロボットによる潜在危険制御系の構成事例

を狭義のフェイルセーフ系とすることはできない。

信号系で用いられる狭義のフェイルセーフは、抑制(解離)作用鎖を単方向制御作用鎖として構成できる特殊な場合に実現できるが、複方向制御の信号系では、フォルトトレランス機構により反転作用鎖(出力エラ)が解離(フォルトマスク)される。

軌道走行形ロボットの事例では、障害物検出センサの断線および短絡による変化に対して潜在危険制御系の構成事例が示された。これ以外に、例えば、センサの見落としなどの故障以外の性能にかかわる異常、ロボットの制御能力以上の急速な人間の干渉、制動機構の破壊などによる異常や故障、冗長要素の同時故障などを考慮しなければならない。一般に、すべての潜在危険に有効な制御系を構成することは、系が複雑になればなるほど困難となる。制動機構の破壊に対しては、材料の信頼性向上や予防保全による変化の抑制(潜在危険抑制原理2)、人間がある範囲内に存在したら系のロボット作動モード相への遷移を禁止する(潜在危険抑制原理3)など総合的な安全計画の実施が必要である。変化が時間、空間、質量、エネルギー密度などの物理量をパラメータとして確率論的に発生するので、潜在危険制御系構築の優先順位の決定や、残存リスクの評価などに対して、潜在危険の確率論的评价が重要となる。

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、それらのおおのこ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

フェイルセーフなどの概念は、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-変化と作用連鎖モデルにもとづき、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、軌道走行形ロボット、救助ロボット、外科ロボットなどに生ずるいくつかの潜在危険に対して潜在危険制御系の構成事例を示した。

文 献

- (1) 佐藤・井上, 人間-ロボット系の安全性評価 (第1報), 機論, 51-468, C (昭60), 2188.
- (2) 佐藤・井上・熊本, 人間-ロボット系の安全性評価 (第2報), 機論, 52-474, C (昭61), 823.
- (3) 佐藤・井上・熊本, 人間-ロボット系の安全性評価 (第3報), 機論, 52-475, C (昭61), 1110.
- (4) 佐藤・井上・熊本, 人間-ロボット系の安全性評価 (第4報), 機論, 52-482, C (昭61), 2754.
- (5) 文献(1)の2188ページ.
- (6) Sato, Y., ほか2名, On Hazard Identification and Analysis of Human-robot Systems, Proc. Jap. USA Symp. Flexible Autom., (1986), 679.
- (7) 奥村, コンピュータを用いたフェイルセーフなシステム, 情報処理, 22-9 (昭56), 863.
- (8) Heinrich, H. W., Industrial Accident Prevention, (1959), 14, McGRAW-HILL, New York.
- (9) 文献(2)の829ページ.
- (10) 文献(1)の2192ページ.
- (11) McCluskey, E. J., 上原, フォルトトレラントシステム, 情報処理, 23-4 (昭57), 378.
- (12) 当麻・南谷, フォルトトレラントシステム, 電子通信学会誌, 63-10 (昭55), 1031.
- (13) 文献(7)の865ページ.
- (14) 文献(7)の866ページ.

討 論

〔質問〕 幸 田 武 久

〔工業技術院機械技術研究所〕

(1) 貴論文は、第1報の作用連鎖と6種類作用のモデルに基づき、潜在危険制御系の基本的性質を考察し興味深い。具体的事例で構成された制御系の性質は理解しやすいが、構成原理が制御系の構成にどのように活用されたかご説明願いたい。

(2) 定義や系での使用語句が多く理解を妨げるようだが、(i)作用を大きく能動形と不履行形に分類し議論すると理解しやすいのではないか、(ii)作用鎖、作用経路と作用連鎖の違い、作用源と要素の関係や違いをご説明願いたい。(iii)式(1)~(5)などの作用の添字は $i \in \{1, 2, \dots, 5\}$ のほうが適切ではないか。

(3) 制御の定量的側面として単方向と複方向を取扱われているが、作用連鎖モデル上の区別は困難ではないか。また、救助ロボットに安全検出形センサ不採用の理由を詳しくご説明願いたい。

(4) 緒言や結論でフェイルセーフの概念は多様な分野で異なるとあるが、概念は同じで安全な状態の定義が分野ごとに異なるのではないのか。

〔回答〕 (1) 救助ロボットを例としてご説明する。まず(i)潜在危険 $\{Nf \xrightarrow{0} H\}$ が同定され、(ii)こ

れは定理[1]より P_4 で解離される。(iii)定理[2]より P_4 は $g' \& g''$ で実現される。(iv)制御に関する知識から制御連鎖 $[Hu_1'' \xrightarrow{-6} Su_2'' \xrightarrow{-5} Cu_3'' \xrightarrow{-4} Du_4'' \xrightarrow{-3} Tu_5'' \xrightarrow{-2} \{(Rg' \xrightarrow{-1} N) \& (Rg' \xrightarrow{-1} Rg'' \xrightarrow{-0} H)\}]$ が仮

定される。(v)ロボットは前進・旋回などを繰返えして被災者を探索し、接近しなければならない。 $u_5'' (= a'')$ は被災者からの情報 $u_1'' (= b'')$ に従う外依複方向制御作用となる。(vi)制御を実現するためには、外依複方向制御作用 (ここでは u_5'') と、それが依存する複方向制御作用 (u_1'') を結ぶ複方向制御作用からなる抑制連鎖が少なくとも1本存在する必要がある。そこで、上記制御連鎖以外にそのような抑制連鎖が存在しないとき、 u_2'', u_3'', u_4'' はすべて複方向制御作用となる。すると(vii)定理[7]より、 u_2'', u_3'', u_4'' は f'' 形をとれないため安全検出形のセンサ ($u_2'' = f''$) を構成できない。したがって、センサの故障には P_4 で対処しなければならない〔定理3, 4, 5, 6〕。

(2) (i) ご指摘のとおりである。ただし、系統的な潜在危険の同定とその制御系の概念設計という観

点からは、作用に関して具体性が必要であり、作用を2種類のみに抽象化することは本方法論本来の意味を失わせる恐れがある。(ii)作用鎖とは、作用が行われることを示すモデル上でのシンボルである。作用連鎖は、因果関係にある作用鎖がいくつか結合したものである。作用経路は、ある作用が伝ばする空間である。要素とは系の分割可能な部分である。能動形の作用を行う要素は、その作用に関して作用源である。(iii)式(1)の添字 i は1から5までの値の一つをとり、式(2)の j は1から5までの値の少なくとも一つをとることを意味している。すべての添字を $i \in \{1, 2, \dots, 5\}$ とおくと、上記 i と j の差異が不明となる。

(3) 複方向制御作用鎖はアークを二重線で描くなどの工夫をしたい。その他、回答(1)を参照されたい。

(4) 工学的制御の対象は潜在危険である。未知の要因によっても危険が生じ得るので、「安全な状態」とは制御の結果生ずる仮想的・相対的な状態にすぎない。各分野での定義自体があいまいであるが、概見例えば、鉄道では P_1 、航空機では P_4 による解離をフェイルセーフと呼称しており、しかも鉄道では P_4 をフェイルセーフとは言わず、両者間で異なった概念となっている。

〔質問〕 大 田 芳 晴 (川崎重工業(株))

ロボットの安全管理など、将来に互って極めて重要な研究であり、一連の研究成果、効果を期待する。

研究過程にあるのにある程度先を予測しろというのは失礼な言い方だが、研究を通じての経験、事例からのご意見をお伺いしたく思う。

作用鎖の解離、フェイルセーフなどの概念を体系化され、潜在危険制御系の構築をどのようにすればよい、かを示されているが、安全という観点からはやはり、情報伝達系の解離問題よりは、エネルギー伝ば形の解離問題に気が引かれる。すなわち、作用鎖を解離するため本来ロボットが所有する機能を損うことなく、順応形の人間に対応させるための具体的解離手段にはどのようなものがあるか (または、技術的問題点)、人間が介在するシステムにおいて、人間とロボットがうまくつき合う方法およびその安全対策はどのように考えていくべきかなど、技術動向を含めて、将来展望などをお伺いしたい。

〔回答〕 潜在危険 $\{Ra \rightarrow W\}$ に対しては、(1)ロボットの軽量、柔構造、軟材質、低出力化、あるいはノイズ発生源の排除、(2)ロボットと環境の保全、(3)

動作中のロボットと対象物 W との接触を減らす、(4)ロボットの非常停止機構の確立、などが考えられる。潜在危険 $\{Rf \rightarrow W\}$ に対しては、ロボットの高信頼化、システムの冗長化などが考えられる。ロボットが置かれる環境によっては、高信頼化と軽量化あるいは低出力化とは必ずしも一致しないことに注意すべきである。ロボット自体の対策はもとより、ロボット-環境系としての視点で捉えることが肝要である。

信号は情報とエネルギーの両側面をもつ。例えば、

ノイズ問題に対して(1)信号の高出力化(エネルギー面)、(2)スペクトラム拡散による暗号化(情報量的側面)などが考えられる。しかし、それらの適用性は、ロボット-環境系の構造と、潜在危険のタイプに依存するので、潜在危険制御系をその構成原理に基づいて概念設計する必要がある。また、複数の方式が構成可能な場合は、システム評価を行い、最も望ましいものを適用していくべきであると考えられる。