

4. 新技術を用いたシステムに生ずる潜在危険の評価

佐藤吉信*

On Hazard Assessment of Innovative Systems

by Yoshinobu SATO*

In this paper the problem of how to assess hazards posed in innovative man-machine systems is discussed. First, the procedure of hazard assessment for innovative systems with fewer operation data is discussed. Secondly, action-change and action-chain models for identification of hazards are presented, and useful identification results of hazards that could be posed in present or future human-robot systems are shown. Thirdly, the second step of hazard assessment that is minute qualitative analysis of accident-causing-mechanisms is discussed, and requisites to safety interlock systems or safety monitoring systems are mentioned quoting fault trees extracted as subsets of comprehensive logic models which analyze general accident-causing-mechanisms. Lastly, methodology of quantitative evaluations is described especially emphasizing sequential nature of basic events for quantification of cut sets.

Keywords : Safety Engineering, Safety Assessment, Robot, Human-Robot Systems, Hazard Assessment, Hazard Analysis, Logic Models, Innovative Systems, System Safety, Fail Safe Mechanism

* 機械研究部 Mechanical Safety Research Division

4.1 緒言

人間—機械に限らず一般的に、系の安全化を意図するときは、まずどこに危険性が潜在しているかを見出し、適切な対策を検討し実施することとなる。そして、対策の適切さは、それによりどの程度リスクが抑制されるかという問題を中心として評価される。

この一連の災害防止活動において、潜在的な危険性の認識から対策の適切さの判定に至るまでのプロセスが広義の安全性または潜在危険評価過程である。

本論文では、潜在危険評価の中でも予測型評価に必要とされるシステムの潜在危険評価について論じる。

4.2 システム的潜在危険評価とその必要性

潜在危険評価の実施対象としての系において両極端の場合が考えられる。そのひとつは、対象とする系がすでに長期にわたる運用経験を有し、しかも類似の系が多数存在する場合である。一方は、対象とする系の運用経験が乏しいか無い場合、あるいは運用経験はあるものの類似の系が少なく災害経験の少ない場合である。

前者の場合では十分な災害データがすでに得られており、系の潜在的な危険性の認識はそれらデータを解析することによって可能となることが多い。

後者の場合では、新技術を用いた系や、比較的災害件数（度数率）は少ないが、一旦事故が生ずると損害が大きくなる大規模プラントなどが該当する。ここでは実データが十分には得られていないので、評価が演繹的あるいは予測的に行われなければならない。予測的な評価はシステムの（系統的）に行われる必要がある。さもないと、藁束の中に落ちたとされる針を捜す場合に簡単に見い出せないからといってその存在を全く否定できないのと同様に、評価は有効な結論を導き出すことが期待できないものとなる¹⁾。

システムな安全性評価は、

- (イ) 評価が合理的な手順で行われる、
- (ロ) 評価の各過程で、システム的手法やモデルが用いられる、

ことが必要であり、逆にこのような条件を具備した評価はシステム的であるといつてよい²⁾。

4.3 評価手順と各過程での実施要領

システム的な安全性評価の手順は次の3段階に大別される^{3,4,5)}。

- (1) 系に生ずる潜在危険*の認識
 - (2) 潜在危険による生ずる災害発生機構の定性的解析及び潜在危険抑制措置の検討と定性的評価
 - (3) 残存リスク（潜在危険抑制措置）の定量的評価
- 一般に安全性評価は所与の具体的な系に対して実施される。一方、任意に行われた評価に見落としなどないかチェックする機能が非常に重要である。このような機能は、対象とする個々の系を含んだできるだけ包括的な系を想定し、その包括的な系に対するいわば評価モデルを作成しておくことにより達成される。また、個々の具体的な系に対する評価は、評価モデルを所与の具体的細目及び条件に従って特殊化することによっても得られる。

システム的安全性評価の各段階において、包括的な系および個々の系で実施すべき要項はそれぞれの Table 4-1 のように示される。

4.4 系に生ずる潜在危険の同定

システム的な安全性評価の第1段階は、系に生ずる潜在危険の認識である。これは、安全性評価の中で最も重要な過程のひとつである。ここでの不都合は、後続の全ての段階に影響を及ぼす。

ところで認識という精神活動は、認識者の五感が対象物あるいは情報と接触し、これにより生ずる刺激が意識へ伝達され、ここにかねてより蓄積された知識（記憶）の体系上へ投射され分類・定形化すなわち同定されることにほかならない。

潜在的に存在する危険性すなわち潜在危険の同定は安全性評価にとって非常に重要なものであるが、潜在危険の概念はさほど明確ではなく、その同定手法も特に人間—機械系に関しては殆んど開発されていない。例えば、システム的安全性評価で一般的によく使用される手法として、Failure mode and effect analysis (FMEA)⁶⁾、Hazard and operability study (HAZOP)^{7,8)}、Fault-tree analysis (FTA)⁶⁾などがあげられる。

* 「潜在危険」の定義については、後述 4.4.3 節参照。

Table 4-1 Tasks on each step of hazard assessment
安全性評価の各段階で実施すべき事項

Procedure of hazard assessment	Tasks on each step	
	Comprehensive systems	Particular systems
Recognition of hazards	Hazard identification	Hazard enumeration based on identification
Qualitative analysis of accident-causation mechanisms	Preparation of comprehensive logic models for analysis	Preparation of fault-trees obtained by customizing comprehensive logic models, and examination of hazard controls
Quantitative evaluations	Examinations of algorithms	Calculation of expected numbers of occurrences of top events

FMEA は、装置の安全上重要な箇所など特定の部分に対して、部品やサブシステムの故障頻度やその影響を評価するための手法である。しかし、装置のハード面の故障を主な検討対象としているため、ヒューマン・エラーなどによる操作の失敗などは考慮されない。また、一連の故障伝播の最初のひき金となる異常または故障にどのようなものかを考えるべきか、また故障の影響の伝播としてどのようなものかを考えるべきかについて体系的な方法論を与えていない。

HAZOP は、主として化学プラントを対象として、プラントの各プロセス及び各要素において、その正常な稼動状況からの考え得る可能な逸脱状態を表に示すことを行い、それらの逸脱がどのようにして生ずるのかを検討し、それらの逸脱状態がプラントにどのような影響を与えるかを予測するための手法である。そしてこれに基づき、それらの逸脱状態を検出し、処理するための手段が意味される。HAZOP は、潜在危険の同定のための手法とも言えるが、逸脱状態の発掘のためのガイド・ワードが流量、圧力、温度、水位などプラントに密接した物理量に限定的な“None”, “More of”, “Less of”, “Part of”, “More than”, “Other” などであるため人間-機械系への適用は困難である。

FTA は、同定された潜在危険による生ずる事故や災害など、望ましくない事象を頂上事象として、それがなぜ生起するのかを演繹的に解析していくための手法である。FTA は、異常事象生起の原因を効果的に幅広く解析するための非常に有効な手法であるが、潜在危険の同定のための手法ではない。

このように従来、人間-機械系における潜在危険の同定手法については、有効な手法が開発されていないというのが実情であった。これは、従来のシステム安全が、航空宇宙産業、原子力や化学プラントを主な対

象としており、それらの系では非常に突出した高エネルギー状態により生ずる潜在危険が顕著であり、例えば作業員が通路でつまづく部類の潜在危険は相対的に無視される程度のものであったことにも原因がある。ところが、今後の技術的発展によって非常に多方面での使用が期待されるロボットを取りあげると、それ単体では巨大なプラントのもつエネルギーに比較して桁外れに小さなエネルギーしかもたないが、プラント類が単一の用途にしか使用されないのに対して、高度なロボットであればある程、非常に多様な使われ方をする可能性がある。従って、そこに生じ得る潜在危険も多様なものとなり、その同定には木目の細かい検討が必要となってくる。そこで本章では、そのような人間-機械系における潜在危険の同定のための方法論を展開する。

さて潜在危険 (Hazard) の概念について、システム安全工学の観点からさほど確立した定義は与えられていない。一般には、例えば「ある状況において、エラー、見落とし、変化そしてストレスの連鎖が物または人身の損害を伴うエネルギーの望ましくない移行 (Transfer) に結びつく潜在力⁹⁾」という定義と類似した概念で用いられることが多い。文献 10) もこの観点から潜在危険を論じている。システム安全工学の立場からの潜在危険についての共通した認識は、ある事物それ自体が独立して潜在危険を有するのではなく、必ず他の事物との関係において潜在危険が生ずるということである。これは、例えば、爆発物がある特定の環境に置かれたときのみ、人や物を破壊する危険性が生ずるのであって、無人の太平洋のまん中に置かれているときは、少なくとも人や物がそこに近づかない限り人や物に対する危険性は生じないということを意味している。しかしながら、それらの事物すなわちある系の要素間の潜

在危険生成過程における関係を体系的に取扱った研究は見当らない。また、何らかのエネルギーの移行の結果災害が発生するという災害発生論の観点のみから潜在危険を取扱うと、情報、病原体、有害物質あるいは心理的影響によっても生ずる災害を全て網羅するのに不自然さが残る。

そこでそれらの問題点を解決するための潜在危険同定モデルが以下のようにして与えられる¹¹⁾。

4.4.1 系の要素間における作用—変化モデル

一般に、系が人間、構造物、機械装置、物質、環境条件、遂行目標などの要素から構成されているとき、ある要素に毀損が生ずる過程に他の要素の介在が含まれる場合と含まれない場合とがある。毀損を生ずる要素が人間であるなら、介在が含まれない場合は災害とは言えない*。従って、ここでは他の要素との関係によって毀損が生ずる場合のみを考えるものとする。ここで、系に複数個の同類要素、例えば複数の人間あるいは複数の同類の装置があるとき、それらの各要素は、人間 A, B, C, ……装置 a, b, c, ……のように全て個別的な要素として扱われるものとする。

さて、系のある要素の毀損発生過程における要素間の関係は、要素から要素へのある種の作用の授受とそれによって生ずる要素の状態や動作における変化（エラーも含む）の過程として把握することができる。作用の連鎖がいくつかの要素間で成立することにより、ある要素の毀損発生の必要条件となる作用が生起する。Fig. 4-1 は、このような作用連鎖のある要素AとBの部分を示したもので、要素AからBへの作用が矢印で、さらにこれが引き金となって要素Bに生ずる変化が $\alpha \rightarrow \beta \dots$ と表わされている。

要素間での作用を調べると、次の a) から f) までの 6 種類のタイプにモデル化することができ、各タイプの作用を定義することにより作用の全体概念が明確化される。

a) エネルギー伝播型作用：運動エネルギー、熱エネルギー、あるいは電気エネルギーなど、エネルギーとしての意味をもつ要素間での働きかけである。エネルギーが伝播された要素には、エネルギー変換による変化が生じ得る。

b) 情報伝達型作用：表示や信号など、エネルギーとしてよりは情報としての意味をもつ働きかけである。情報が伝達された要素には、その制御系などの状態に

* 例えば老すい死など

変化が生じ得る。

c) 作因物転移型作用：化学物質、病源体あるいは重量物など、エネルギーや情報以外の物質として認識可能な作因物を要素AがBに転移させることによるものである。作因物が転移された要素には、化学変化、ポテンシャルエネルギーや濃度の増大などの変化が生じ得る。

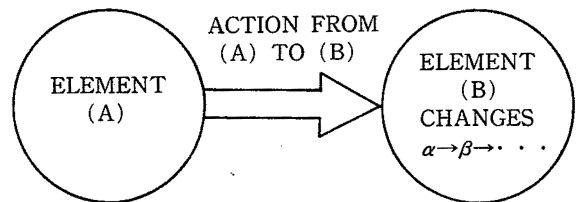
d) 供給阻害型作用：ある要素に、エネルギー、情報及び作因物の必需があつて、それに対する供給を妨害することによる働きかけである。供給阻害作用を受けた要素には、例えば人間ならば窒息、装置ならば運転停止などの変化が生じ得る。

e) 存在形態型作用：エネルギー、情報及び作因物の移動を伴わず、またそれらの供給を妨害するものでもない、要素間でのある要素の形状、重量、状態、条件または性質などによる、a), b), c), d), f) 以外の働きかけである。

f) 機能不履行型作用：ある要素が他の要素に対して、エネルギー伝播、情報伝達、作因物転移、供給阻害または存在形態によるはたすべき機能を行わないことによる働きかけである。

4.4.2 作用連鎖モデル

ここで、ある要素AからBへの作用は他の要素の媒介がなく行われるものとする。仮に要素Cの媒介があれば、要素AからCへの作用と要素CからBへの作用



- KIND OF ACTIONS
- a. ENERGY-TRANSMISSION TYPE
 - b. INFORMATIONAL PROPAGATION TYPE
 - c. AGENT-TRANSFER TYPE
 - d. SUPPLY-OBSTRUCTION TYPE
 - e. EXISTENCE-FORM TYPE
 - f. FUNCTION-FAILURE TYPE

Fig. 4-1 Action-Change Model
作用—変化モデル

が行われたものとする。作用には、例えばある種の運動エネルギーのように、2要素の接触によって伝播が行われるものと、音のエネルギーが空気によって伝播されるように2要素の媒体による場合、または光や電磁波

のエネルギーのように放射によって伝播されるものがある。接触による場合には他の要素の媒介がないことは明らかであるが、他の場合においても、作用を伝える媒体が、その作用の性質や強度を望ましくない方向に変化させることがない限り、その媒体を作用連鎖中の要素とはしないこととし、従って、その場合には2要素間の作用として考えるものとする。

ここで、系のある要素に作用して、その要素にある毀損を生じさせる必要条件となる作用を、その要素のその毀損発生に関する直接原因作用ということとし、ある要素AからBへの作用が、要素Bからのある作用の発生確率を増大させるとき、この要素AからBへの作用を、その要素Bからの作用の誘因作用ということとする。すると、ある要素にある毀損が生ずるための必要条件となる直接原因作用生起の過程は、系の要素間で、いくつかの誘因作用が次々と連鎖してその直接原因作用に結びつく方向性のある作用連鎖として把握される。系のある要素AからBへの連鎖には、経路が2通り以上存在する複連鎖と経路が一連のみの単連鎖が考えられる。このうち単連鎖は、要素A、B及び他の要素との関係において以下のようないくつかのタイプにモデル化される。

作用連鎖1型：要素AからBへ直接原因作用が行われる単連鎖。

作用連鎖2型：要素AからBへ直接原因作用は行われないが、要素Bへ要素Aからの誘因作用が行われる単連鎖。

作用連鎖3型：要素AからBへ直接原因作用や誘因作用は行われないが、要素Bへ直接原因作用を行う要素Cに対して、要素Aからの誘因作用が行われる単連鎖。

作用連鎖4型：1~3型以外の単連鎖とする。

単連鎖は、各型において多様なものが考えられるが、そのうち代表的な連鎖例をFig. 4-2に示す。

Fig. 4-2では、要素間の作用の授受がアークで表わされている。また各アークの下の数字は、そのアークの直接原因作用からの位置を示し、0のときはその作用が直接原因作用であり、 $i(i \neq 0)$ のときはその作用が $i-1$ の作用の誘因作用であることを表わしている。

任意の作用連鎖は、各型におけるいくつかの作用連鎖を複合することによって得られる。例えば、Fig. 4-2の複連鎖は、連鎖順序が $3 \rightarrow 2 \rightarrow 1 \rightarrow 0$ の2型の単連鎖と $2^* \rightarrow 1^* \rightarrow 0$ の3型の単連鎖が複合されたものとなっている。

なお、特別な場合として、毀損発生の必要条件に関する知見が不明であることなどによる直接原因作用のない作用連鎖2型と4型が、例えばFig. 2の2型と4型の連鎖例において、それぞれ要素BとC、要素BとEを同一要素とすることにより得られる。

4.4.3 潜在危険のシステム安全工学上の定義

作用一変化と作用連鎖モデルに基づいて潜在危険を次のように定義する。

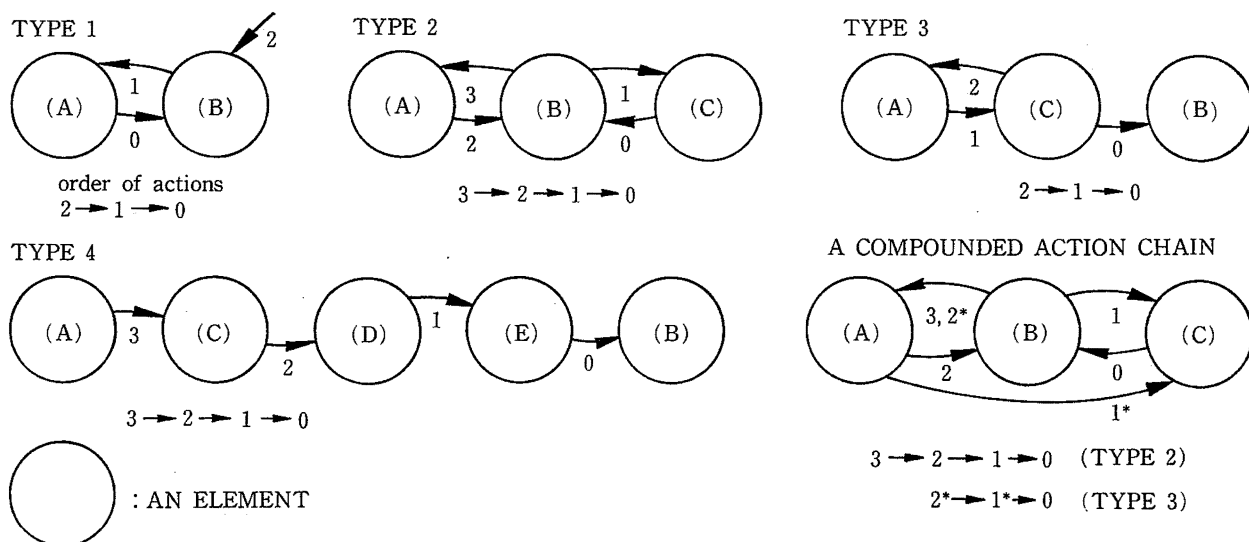


Fig. 4-2 Action-Chain Models and examples for each Action-Chain type
作用連鎖モデルとおのおののタイプにおける連鎖例

直接潜在危険：系のある要素Aがある要素Bに、ある毀損発生への直接原因作用を行い得る潜在力を、その系における、その毀損発生に関する要素AのBに対する直接潜在危険とする。

間接潜在危険：要素AがBのある毀損発生の直接原因作用は行わないものの、その作用連鎖中の誘因作用を行う潜在力を、その系における、その毀損発生に関する要素AのBに対する間接潜在危険とする。

更に、要素AのBに対する直接潜在危険と間接潜在危険の全集合を、その系における要素AのBに対する潜在危険の全集合とする。従って、要素AのBに対する潜在危険の同定とは、その系で生じ得る各要素の作用と変化、それによって生じる要素AからBへの作用連鎖、そして要素Bに生ずる毀損の性質を可能な限り同定することであるといえる。

4.4.4 潜在危険とリスクとの関係

ある直接原因作用の潜在力の数量的尺度として次のような発現確率を用いることができるならば、潜在力とリスクとの関係は式(1)として表わされる¹²⁾。

$$R_{ijk}(x) = \int_0^{\infty} \frac{\partial F_{ijk}(u, x)}{\partial u} \cdot u du \quad \dots\dots(1)$$

ただし記号を以下のように定義する：

- $R_{ijk}(x)$; ある系の状態 x 下において、要素 i への直接原因作用 j による要素 i に生ずる毀損 k のリスク [Loss/Time]
- $F_{ijk}(u, x)$; 状態 x 下において、要素 i への強度 u 以下の毀損 k を生じさせる直接原因作用 j の単位時間あたりの発現回数の期待値 [Events/Time]
- u ; 毀損の強度 [Loss/Event]
- x ; 系の状態ベクトル

ここで式(1)を労働災害のみに限定すれば、 u は災害1件あたりの損失日数に、 $F_{ijk}(u, x)$ は状態 x で労働者 i が直接原因作用 j による日数 u 以下の災害 k を被る期待累積度数率に、そして、 $R_{ijk}(x)$ は状態 x において労働者 i が直接原因作用 j により生ずる災害 k によって被る期待損失日数にそれぞれ相当している。

4.5 作用—変化と作用連鎖モデルによるロボットの潜在危険の同定

メカトロ化による自動化の進展の中で、急速に設置

台数を増大させている産業用ロボットが危険・有害作業を作業者に代替して行う反面、災害発生の潜在危険を有することについては、災害事例からも明らかである。本節では、現在使用されているものも含めて、将来実用化が予想されるロボットシステムの潜在危険評価の第1段階として、系に生じ得る潜在危険を作用—変化と作用連鎖モデルにより同定する。

ここでは、ロボットを系の要素として、その本体、支援システムおよびロボットが所持している工具、加工物、材料などの扱い物も含めたものとして定義する。

4.5.1 要素への作用と変化

4.5.1.1 ロボットへの作用と変化

ロボットへの作用とそれによる変化は以下のように同定される。

a) **エネルギー伝播型作用：**接触により伝播して得るものとして、運動エネルギー、熱エネルギーそして電氣的エネルギーが、媒体により伝播し得るものには爆風などの運動エネルギー、音響的振動エネルギー、熱流などによる熱エネルギー、体中を伝播する電気エネルギーが、そして放射によるものとして、可視光線、赤外線、紫外線、レーザー光、アーク、電子ビーム、X線、電磁波そして放射線などを考えなければならない。

これらの作用により、ロボットの運動量の変化、転倒、機械的破損、部材の劣化、制御系の故障、制御系への異常信号の発生、制御の不能、誤動作などの変化が生じ得る。

b) **情報伝達型作用：**他要素との整合性を保持しなければならないロボットでは、信号などによる情報伝達作用が行われることを考えなければならない。

これにより、その運動状態および運動量などに変化が生じ得る。

c) **作因物転移型作用：**腐食性物質や放射性物質などの作用により、電子回路の短絡、機械的破損や劣化、制御系への異常信号の発生、制御の失敗、誤作動などが生じ得る。

d) **供給阻害型作用：**ロボットに必需されるものとして、動力源の供給、情報などがあるとき、これらの供給が阻害されると、制御の不能や誤作動が生じ得る。

e) **存在形態型作用：**重量物による重力の作用、ロボットの移動経路の状態などの環境条件による作用を考えなければならない。

これにより、ロボットの運量の変化、制御変数の変

化や逸脱が生じ得る。

f) **機能不履行型作用**：ロボットへの情報やエネルギー供給機能が働かないと、ロボットに制御不能や誤作動などの変化が生じ得る。

4.5.1.2 ロボットからの作用

ロボットにより生じ得る作用は以下のように同定される。

a) **エネルギー伝播型作用**：ロボットは、その本体や所持物の自律的運動を行うほか、重力の作用や衝突あるいは把持物の放出などによる制御を逸した他律的運動、さらに静止しているロボットに人間が打ち当たることによる反作用も含めて、運動エネルギーによる作用を行い得る。

ロボット本体に高温部の存在するもの、高温物質、低温物質、溶接ツールなどを扱うものでは熱的エネルギー作用を行い得る。

本体や工具などの動力源として電力源を有する場合は電気的エネルギー作用を行い得る。

本体や工具などから振動や騒音が発生せられる場合には、いわゆる振動・音響エネルギーによる作用が行われ得る。

工具やセンサが電磁波やレーザー光など、いわゆる放射エネルギーを発生する場合には、これによる作用が生じ得る。

b) **情報伝達型作用**：他要素との整合を保持するために、電気的あるいは放射的エネルギーを用いた信号などを発生する場合には、これによる作用を行い得る。

c) **作因物転移型作用**：腐食性物質、放射性物質、中毒性物質などを扱うロボットでは、これを他の要素に転移することによる作用を行い得る。

d) **供給阻害型作用**：移動を自由に行うなどの高度なロボットほど他の要素への干渉の機会が増大すると考えられ、他の要素へのエネルギーの供給や情報の供給を阻害する作用を行い得る。

e) **存在形態型作用**：人間に対しては、保全作業、設置作業そして教示作業の難易度による作用を、また人間も含んだ一般的な要素に対しては、形状、構造、位置的關係による作用を行い得る。

f) **機能不履行型作用**：ロボットが果たすべき機能には、エネルギー供給機能、情報伝達機能、作因物供給機能、供給阻止機能そして存在形機能が考えられ、これらの機能が達成されないことによる作用が考えられる。

4.5.1.3 人間への作用と変化及び毀損

人間への作用とそれによる変化及び毀損は、以下のように同定される。

a) **エネルギー伝播型作用**：これが直接原因作用として人体に働くと、運動エネルギーでは、打たれ、挟まれ、切られ、押し潰おされることによる骨折、内臓損傷、創傷、打撲傷、そして破砕傷などが生じ得る。熱エネルギーとして作用すると、各部の火傷や凍傷、熱射病などが生じ得る。電気的エネルギーとして作用すると、感電による火傷やショックによる心臓停止などが生じ得る。音響や振動エネルギーとして作用すると聴力障害や振動障害が、いわゆる放射エネルギーの作用により視力障害、火傷、X線や放射線障害などが生じ得る。

誘因作用として働いた場合は、生理的反応または心理的動揺を生じせしめ、各種の誤動作やヒューマン・エラーを誘発させる。

b) **情報伝達型作用**：主として誘因作用として働き、判断に影響を与えることにより各種のヒューマン・エラーを誘発させ得る。

特別な場合として、直接原因作用として働き、心因性障害(ex.ショック死)などを生じさせる。

c) **作因物転移型作用**：作因物としては、一酸化炭素などの中毒性物質、高・低温物質、酸・アルカリ性の腐食物質、有機溶剤、放射性物質などの化学物質、細菌やウイルスなどの病原体そして重量物などが考えられる。

これらが直接原因作用として働くと、中毒、火傷、凍傷、表皮損傷、粘膜または内臓損傷、視力障害、呼吸困難による窒息、細菌やウイルスによる疾病、押し潰おされることによる損傷が生じ得る。

誘因作用として働くと各種のヒューマン・エラーが誘発される。

d) **供給阻害型作用**：人間に必需される供給には、呼吸気としての空気(酸素)、ある状況においては情報、飲食物そして体温保持のためのエネルギーなどが考えられる。

これらの供給を阻害する作用が直接原因作用として働くと、窒息、失調症などが生じ得る。

誘因作用として働くと熱射病や凍傷そして各種のヒューマン・エラーが誘発される。

e) **存在形態型作用**：人間に作用する存在形態としては、人間に対するその要素の位置関係、形状、重量、作業の難易性、職務の要求度そして各種の環境条件な

どが考えられる。

これらの作用は、主として誘因作用として働き、ヒューマン・エラーの誘発や災害の型 (ex. 墜落災害) を規定する。

職務上の過度や要求度が精神または神経障害の直接原因作用として働くこともあり得る。

f) **機能不履行型作用**：人間に対して行われる機能には、呼吸気(酸素)や情報などの供給機能、支持機構のように人間の物理的存在状態を規定する補助機能、保護具や安全装置などの防護機能などが考えられる。

これらの機能の不履行が、例えば人工呼吸器の故障による酸素供給機能の喪失などのように直接原因作用として働くと窒息が生ずる。

誘因作用として働くと、例えば安全帯の切断による墜落災害のように、補助機能・防護機能が達成されないことによる各種の災害およびヒューマンエラーが誘因され得る。

4.5.1.4 その他の要素への作用と変化

人間—ロボット系におけるその他の要素としては、周辺の機械、装置、設備、器具などが考えられる。これらに生じ得る変化は次のように同定される。

a) **エネルギー伝播型作用**：これがその他の要素への直接原因作用として働くと、運動エネルギーでは破壊、変形、倒壊などが、熱的エネルギーでは爆発、暴走反応、熱的破壊、燃焼などが、電気的エネルギーでは回路上の損傷などが、放射的エネルギーでは劣化などが発生することによる毀損が生じ得る。また、それらの毀損(変化)によりさらに次の作用が生ずることも考えなければならない。この場合、その他の要素への作用は、直接原因作用であるとともに誘因作用としての働きをもつこととなる。

エネルギー伝播型作用が誘因作用としてのみ働くと、運動エネルギーではその他の要素の運動量の変化などが、熱的エネルギーでは昇温、降温、反応の促進または抑制などの変化が、電気的エネルギーでは電気的ノイズによる誤信号の発生から暴走などが生じ得る。

b) **情報伝達型作用**：これが直接原因作用として働くと、例えば誤信号によるユーティリティの放出による毀損が生じ得る。

誘因作用として働くと、誤作動などが生じ得る。

c) **作因物転移型作用**：これが直接原因作用として働くと、腐食性物質の転移による腐食や破壊、触媒作用による反応の促進そして暴走反応、導電物質の転移

による絶縁性の喪失そして破損、重量物の転移による崩壊や転倒が生じ得る。

誘因作用として働くと、機器の誤動作や構造物の破壊・崩壊などの変化から生ずる作用をひき起こすことを考えなければならない。

d) **供給阻害型作用**：これが直接原因作用として働くと、例えば冷却媒体の供給阻害による昇温と破壊や爆発などが生ずる。

誘因作用として働くと、エネルギー・情報・燃料などの作因物の供給阻害による機器の運転不調や不能から例えば墜落、機能異常や停止、誤作動などの変化を生じ得る。

e) **存在形態型作用**：主として誘因作用として働き、質量として作用することによる運動量や重力の変化、位置エネルギーの増大、経路の変化などの変化が生じ得る。

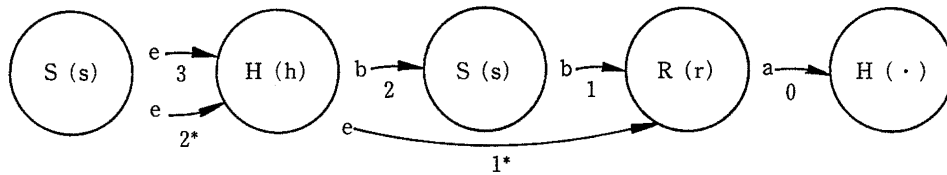
f) **機能不履行型作用**：エネルギー伝播、情報伝達、作因物転移の各機能の不履行により供給阻害型作用の場合と同様に、直接原因作用として働くと、例えば化学物質の暴走反応などをひき起こす。誘因作用として働くと、機器や装置の誤作動などの変化が生ずる。存在形態型機能のうち、例えば支持機能の不履行により倒壊な墜落、防護機能の不履行により破壊などが生ずる。

4.5.2 人間—ロボット系における作用連鎖とその生起のシナリオ

実際に発生した産業用ロボットによる災害に次のようなものがある。

災害事例：作業者が、シェービングマシンとそれへワークを供給し取り出すための産業用ロボットからなるワークステーションで、シェービングマシンの調整作業を行っていた。作業終了後、マシンの起動ボタンを押したところ、マシンからロボットへ作動命令が伝達されたためオペレータが作業者の背後から伸展した。作業者は逃げる間もなく、オペレータとマシンとの間に身体をはさまり死亡した。

この災害を作用連鎖モデルで記述すると Fig. 4-3 となる。すなわち、シェービングマシン $S_{(s)}$ の作業者に対する運転遂行職務(存在形態型作用 e_3)が作業者 $H_{(h)}$ のシェービングマシンの起動操作(情報伝達型作用 b_2)を誘発させ、更にこれがシェービングマシン $S_{(s)}$ からロボット ($R_{(r)}$) への作動命令(情報伝達型作用 b_1)を生じさせた。また、シェービングマシン $S_{(s)}$ が存在してい



H (h) : Human & Changes R (r) : Robot & Changes
 S (s) : Shaving Machine & Changes
 H (·) : Human & Injuries

Fig. 4-3 A representation of an accident by A-C models
 実災害の A-C モデル記述

たため(存在形態型作用 e_2^*),これによって作業者(H(h))が逃げられずマニプレータの作動点に存在することになってしまった(同様に e_1^*)。

以上のことから明らかのように、この災害は、

[単連鎖 1] $S_{(s)}e_3 \rightarrow H_{(h)}b_2 \rightarrow S_{(s)}b_1 \rightarrow R_{(r)}a_0 \rightarrow H(\cdot)$

[単連鎖 2] $S_{(s)}e_2^* \rightarrow H_{(h)}e_1^* \rightarrow R_{(r)}a_0 \rightarrow H(\cdot)$

の少なくとも 2 通りの単連鎖により構成されている。

このように現実の災害は何らかの複合連鎖の生起によって発生する場合が多い。しかし、前述の事例では、

2つの単連鎖を共に予見しなくとも、例えば単連鎖 1 のみが予見できればその潜在危険性を認識できる。従って、複合連鎖によって生ずる災害の発生も、その発生の主要な必要条件である単連鎖がひとつ特定されることによって予見可能となる。

更に厳密な災害発生論理の展開は、安全性評価の第 2 段階である災害発生機構の解析によって得られる。

Table 4-2 には、ロボットから人間への典型的な作用連鎖(単連鎖)が同定されている。

Table 4-2 Typical action-chains from robot to human
 ロボットから人間への典型的な作用連鎖

Kinds of robot's actions	Typical action-chains among elements	Kinds of robot's actions	Typical action-chains among elements	
a) Energy-transmission type Kinetic Thermal Electrical Acoustical Radiative	Type 1 : $R(a)a \rightarrow H(\cdot)$ $H(h)a \rightarrow R(r)a \rightarrow H(\cdot)$ $H(h)e \rightarrow R(r)a \rightarrow H(\cdot)$ $R(r)e \rightarrow H(h)a \rightarrow R(r)a \rightarrow H(\cdot)$ $H(h)b \rightarrow R(r)a \rightarrow H(\cdot)$	Disease-causing agents etc.	2 : $R(r)c \rightarrow H(h)a \rightarrow P(p)a \rightarrow H(\cdot)$ 3 : $R(r)c \rightarrow P(p)a \rightarrow H(\cdot)$ $R(r)c \rightarrow P(p)c \rightarrow H(\cdot)$ $R(r)c \rightarrow P(p)d \rightarrow H(\cdot)$ $R(r)c \rightarrow P(p)f \rightarrow H(\cdot)$	
	2 : $R(r)a \rightarrow H(h)a \rightarrow P(p)a \rightarrow H(\cdot)$ $R(r)a \rightarrow H(h)b \rightarrow P(p)a \rightarrow H(\cdot)$ $R(r)a \rightarrow H(h)b \rightarrow P(p)c \rightarrow H(\cdot)$ $R(r)a \rightarrow H(h)b \rightarrow P(p)d \rightarrow H(\cdot)$ $R(r)a \rightarrow H(h)e \rightarrow P(p)a \rightarrow H(\cdot)$ $R(r)a \rightarrow H(h)e \rightarrow P(p)c \rightarrow H(\cdot)$ $R(r)a \rightarrow H(h)e \rightarrow P(p)d \rightarrow H(\cdot)$		d) Supply-obstruction type	3 : $R(r)d \rightarrow P(p)a \rightarrow H(\cdot)$ $R(r)d \rightarrow P(p)c \rightarrow H(\cdot)$ $R(r)d \rightarrow P(p)f \rightarrow H(\cdot)$ 4 : $R(r)d \rightarrow P(p)f \rightarrow Q(q)a \rightarrow H(\cdot)$
	3 : $R(r)a \rightarrow P(p)a \rightarrow H(\cdot)$ $R(r)a \rightarrow P(p)e \rightarrow H(\cdot)$ $R(r)a \rightarrow P(p)d \rightarrow H(\cdot)$ $R(r)a \rightarrow P(p)f \rightarrow H(\cdot)$		e) Existence-form type	1 : $R(r)e \rightarrow H(h)$ 2 : $R(r)e \rightarrow H(h)a \rightarrow P(p)a \rightarrow H(\cdot)$ $R(r)e \rightarrow H(h)b \rightarrow P(p)c \rightarrow H(\cdot)$
	b) Information-propa. type	2 : $H(r)b \rightarrow H(h)e \rightarrow P(p)a \rightarrow H(\cdot)$ 3 : $R(r)b \rightarrow P(p)a \rightarrow H(\cdot)$	f) Function-failure type	1 : $R(r)f \rightarrow H(\cdot)$ 2 : $R(r)f \rightarrow H(h)a \rightarrow P(p)a \rightarrow H(\cdot)$ $R(r)f \rightarrow H(h)e \rightarrow P(p)c \rightarrow H(\cdot)$ 3 : $R(r)f \rightarrow P(p)a \rightarrow H(\cdot)$ $R(r)f \rightarrow P(p)c \rightarrow H(\cdot)$ $R(r)f \rightarrow P(p)f \rightarrow H(\cdot)$
		c) Agent-transfer type Chemical agents		1 : $R(h)c \rightarrow H(\cdot)$ $H(h)a \rightarrow R(r)c \rightarrow H(\cdot)$ $H(h)b \rightarrow R(r)c \rightarrow H(\cdot)$ $H(h)e \rightarrow R(r)c \rightarrow H(\cdot)$

$R(r)$: A robot & changes. $H(h)$: A human & changes.
 $P(p)$: A peripheral element & the changes.
 $H(\cdot)$: The human & injuries.

Table 4-3 Typically assumed scenarios of action-chain occurrences
作用連鎖生起に想定される典型的シナリオ

Typical action chains among elements	Typically assumed scenarios of action-chain occurrences
R(r)a→H(·)	Signal to start has been propagated to robot accidentally, which suddenly moves and strikes human.
H(h)a→R(r)e→H(·)	Electromagnetic waves has been radiated to robot, which fails to control its power and crushes human.
H(h)e→R(r)a→H(·)	Human strikes against robot.
H(h)b→R(p)a→H(·)	Human has approached robot, which suddenly begins to move and strikes him.
H(h)b→R(p)a→H(·)	Human has pushed start button of robot accidentally, which strikes him.
R(r)a→H(h)a→P(p)e→H(·)	Human has received electric shocks from robot and touched sensors of peripheral equipment accidentally, which suddenly starts and pours down acid upon him.
R(r)a→H(h)b→P(p)c→H(·)	Robot has pushed human, who reels and strikes against peripheral facilities.
R(r)a→H(h)e→P(p)d→H(·)	Human has received electric shocks from robot and touched sensors of peripheral equipment accidentally, which suddenly starts and pours down acid upon him.
R(r)a→P(p)a→H(·)	Robot has struck human, who falls into water and drowns.
R(r)a→P(p)c→H(·)	Robot has radiated electromagnetic waves to peripheral machinery, which falls into reckless driving and crushes human.
R(r)a→P(p)f→H(·)	Robot has shattered tank of chemical agent, which pours down on human.
R(r)b→H(h)e→P(p)a→H(·)	Robot has destroyed heart-lung machine, which stifles human.
R(r)b→P(p)a→H(·)	Robot has given wrong information to human, who enters dangerous zone and get caught in equipment.
R(r)c→H(·)	Robot has touched sensors of peripheral machinery, which suddenly begin to move and crushes human.
H(h)a→R(r)c→H(·)	Signal to release has been propagated to robot accidentally, which suddenly pours chemical agent on human.
R(r)c→H(h)a→P(p)e→H(·)	Human has struck against robot, which pours acid on him.
R(r)c→P(p)a→H(·)	Robot has transferred heavy material to human, who reels and strikes against peripheral facilities.
R(r)d→P(p)f→H(·)	Robot has poured conductive liquid on machinery, which falls into disorder and strikes human.
R(r)e→H(·)	Robot has cut supply of information to heart-lung machine, which stifles human.
R(r)e→H(h)a→P(p)e→H(·)	Association with robot has been so hard that human becomes a stomach ulcer.
R(r)f→H(·)	Robot has approached human, who tries to avoid it and strikes against peripheral facilities.
R(r)f→H(h)a→P(p)e→H(·)	Robot has failed to supply air for breath, and human suffocates.
R(r)f→H(h)a→P(p)e→H(·)	Robot has failed to support human, who begins to fall and strikes against the ground.

Typical action chains among elements	Typically assumed scenarios of action-chain occurrences
$R(r)f \rightarrow H(h)e \rightarrow P(p)c \rightarrow H(\cdot)$	Robot has failed to support human, who falls into acid tank.
$R(r)f \rightarrow P(p)a \rightarrow H(\cdot)$	Robot has failed to operate machinery, which is reversed and crushes human.
$R(r)f \rightarrow P(p)c \rightarrow H(\cdot)$	Robot has failed to operate equipment, which pours radioactive substance on human.

各作用連鎖に対して、多様な具体的なシナリオが考えられる。そのうちの代表的なものについて、Table 4-3 に示す。

4.6 災害発生機構の定性的解析

潜在危険評価の次の段階は、それら潜在危険によって生ずる災害の発生機構の解析である。

通常この種の解析は具体的な系に対して行われる。しかし、例えばロボット系では、今後出現の予想される高度なロボットが非常に広い汎用性を持つようになると考えられ、そのロボットを用いた多くの具体的な系を想定しなければならなくなり、解析が繁雑となる。そこで、個々の考え得る系を包括するような系を想定し、そこでの災害発生機構を包括的論理モデルとして与えることにより、任意の具体的な系に対して実施された解析をチェックすることができる。また、包括的論理モデルを、具体的な系の諸条件に従って特殊化、個別化することにより、個々の系の災害発生論理を得ることができる。

この観点から、人間がロボットの腕または本体に打たれる災害発生機構について、その包括的論理モデルが FT の記号を用いて作成されている^{13,14)}。

さて論理モデルの FT を構成している基本事象 i はつぎのように定義される。

$$x_i = \begin{cases} 1 & \text{基本事象 } i \text{ が生起している} \\ 0 & \text{基本事象 } i \text{ が生起していない} \end{cases} \quad \dots\dots(2)$$

同様に、頂上事象の状態が

$$\phi = \begin{cases} 1 & \text{頂上事象が生起している} \\ 0 & \text{頂上事象が生起していない} \end{cases} \quad \dots\dots(3)$$

として表わされる 2 値変数 ϕ で表現される。

頂上事象の状態 ϕ は基本事象の状態 $x_i (i=1, \dots, n)$ によって決定されるので、 ϕ は $\mathbf{x} = (x_1, x_2, \dots, x_n)$ の関数として

$$\phi = \phi(\mathbf{x}) \quad \dots\dots(4)$$

と表わせる¹⁵⁾。

論理モデルが k 個の最小カットセット^{*16)} $\kappa_j (j=1, \dots, k)$ をもつとすれば、各最小カットセット κ_j は最小カット AND 構造

$$\kappa_j(\mathbf{x}) = \prod_{i \in \kappa_j} x_i \quad \dots\dots(5)$$

として得られる。

構造関数 $\phi(\mathbf{x})$ は

$$\phi(\mathbf{x}) = \prod_{j=1}^k \kappa_j(\mathbf{x}) = \prod_{j=1}^k \prod_{i \in \kappa_j} x_i \quad \dots\dots(6)**$$

と書くことができる。

文献 13) 及び 14) では、論理モデルを構成している系を 42 個からなる相に分割し、そのいくつかの主要な相における主要な最小カット集合 κ_j を求めている。

式(6)からわかるように、頂上事象の生起すなわち災害の発生を抑制することは各最小カット集合の生起を抑制することと同義である。また、各最小カット集合の生起の抑制は、それを構成している基本事象の生起を抑制することによって達成される (ϕ がコヒーレント関数のとき)。

例えば、文献 14) では、ロボットの自動運転、意図された命令による自律的運動、人が必要上接近して存在の各モードからなる系の相における主要な最小カット集合として、16 個の最小カット集合が抽出されている。それらの各々には、人が侵入してきたときロボットを停止させる「インターロックの失敗」(E_{d10}) 事象が含まれている。従って、この事象が生起しないようにすることは、少なくともこの相における安全対策上非常に有効であることがわかる。

ところで「インターロックの失敗」 E_{d10} 事象は、包括的論理モデル¹⁶⁾からさらに Fig. 4-4 に示すように、「検出の失敗」(E_{e18})、「作動の失敗」(E_{e19})、「人が無

* 最小カット集合とは、頂上事象(災害)を発生させる必要最小限の基本(原因)事象の集合である。

** ただし記号 \prod は

$$\prod_{i=1}^n x_i \triangleq 1 - \prod_{i=1}^n (1 - x_i)$$

ここで \triangleq は定義式を意味する。

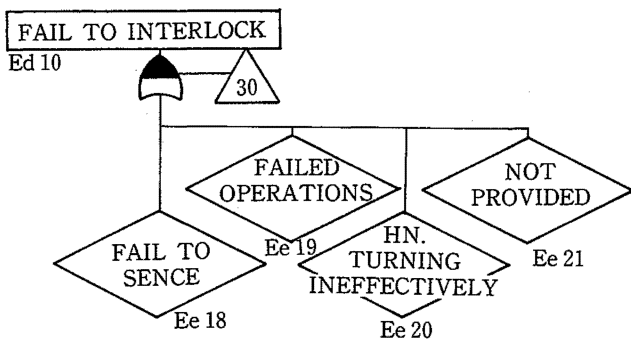


Fig. 4-4 Partial FT extracted from Comprehensive Logic Models (Part-1)
包括的論理モデルの部分ツリー (その1)

効にする」(E_{e20})、そして「装置がとりつけられていない」(E_{e21})の各事象に展開される。ここで、センサーなど電子部品やインターロック装置などハード面については、Fail Safe 化など適切な回路構成などをとることによって満足すべき信頼性を得ることができるであろう。すなわち、事象 E_{e18}, E_{e19} については比較的容易に発生確率を減らすことが可能である。しかしながら、センサーなどについては、通常2種類の故障モードが存在する¹⁸⁾。一方は、危険側の故障モードすなわち欠報であり、他は、侵入できないときに侵入信号を出してしまう安全側の故障モードすなわち誤報である。例えば、現行の火災報知器においては、誤報がかなり多

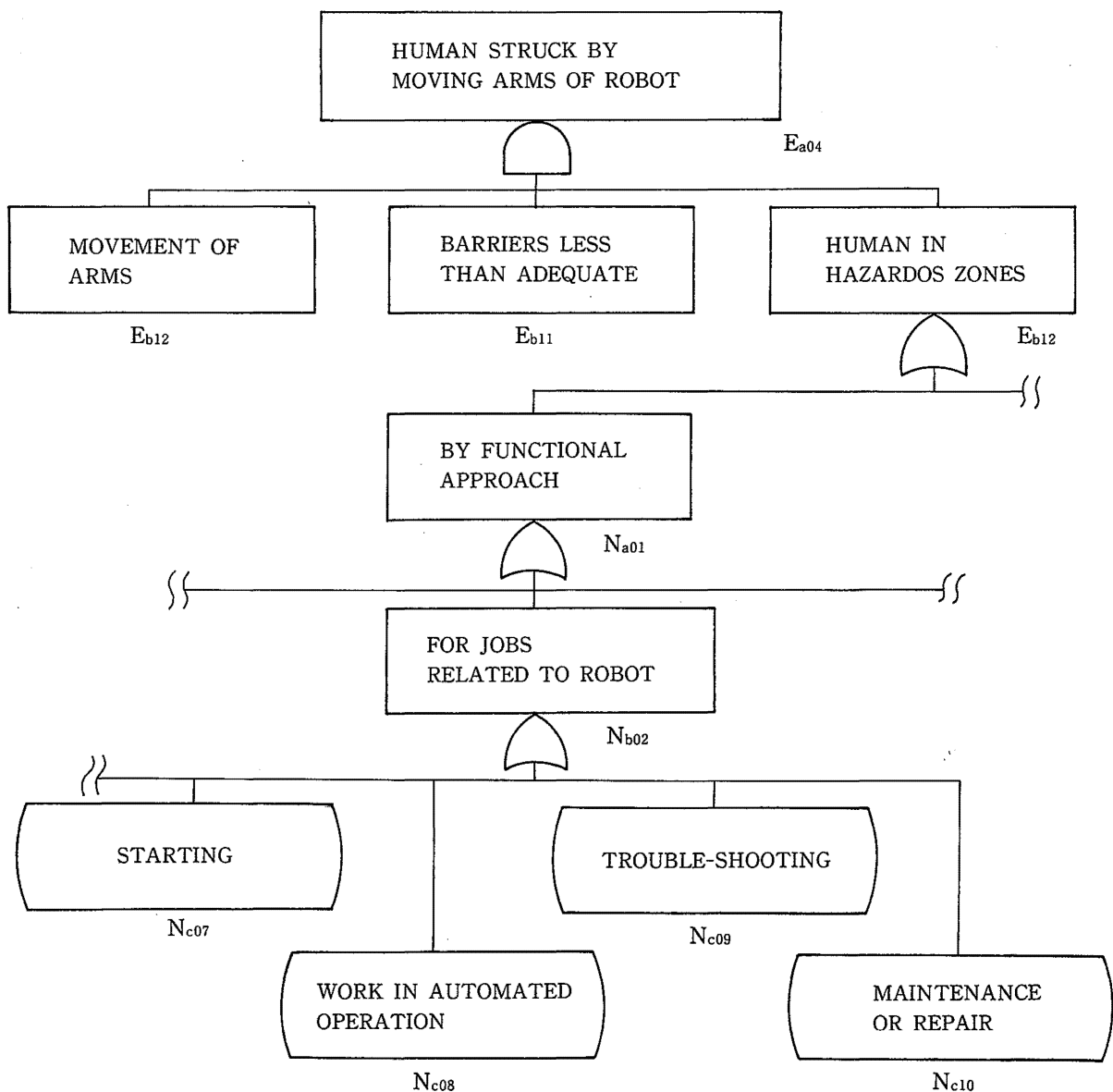


Fig. 4-5 Partial FT extracted from Comprehensive Logic Models (Part-2)
包括的論理モデルの部分ツリー (その2)

く、このためしばしば人がセンサーシステムを無効にしてしまうことがある。従って、火災時に報知器が作動しない結果となる。

また、誤報の発生すなわちインターロック機構の故障により、Fig. 4-5 に示されるように、人が「異常処理」(N_{c09})や「保全・修理」(N_{c10})のために危険域に入らなければならない事象(Eb₁₂)の生起確率が增大する。

以上のことから、欠報側と誤報側の2種類の故障モードがあるセンサーなどについては、そのどちらの側の信頼性も同時に向上させることが望ましいことがわかる。すなわち、もしも欠報側の故障発生確率の減少が誤報側の故障発生確率の増大を招く場合では、これにより「人がインターロックを無効にする」(E_{c20})、「異常処理」(N_{c09})あるいは「保全・修理」(N_{c10})の各事象の生起確率を増大させるために、全体として災害発生確率を増大させる場合があり、一概には頂上事象の生起の抑制が単純に欠報側の故障発生確率の抑制のみに依存しなくなることに注意すべきである。

4.7 定量的評価

潜在危険評価の第3段階は定量的評価である。通常、定量的尺度としてはリスクを用いるのが最も一般的である。リスクは、4.4節の式(1)で定義されるように、毀損の強度とそれの単位時間あたりの発現回数の期待値を乗じたものとなるので、単位時間あたりの期待損失値とも言うことができる。

ところで、状態 \mathbf{x} 下において、要素 i へ強度 u 以下の毀損 k を生じさせる直接原因作用 j の単位時間あたりの発現回数の期待値 $F_{ijk}(u, \mathbf{x})$ を求めることは極めて複雑である。従って、一般には、

$$\frac{\partial F_{ijk}(u, \mathbf{x})}{\partial u} \doteq \phi_{ijk_u}(\mathbf{x}) \quad \dots\dots(7)$$

としてしまう場合が多い。

すると式(1)は

$$R_{ijk}(\mathbf{x}) \doteq \phi_{ijk_{u_1}}(\mathbf{x}) u_1 + \phi_{ijk_{u_2}}(\mathbf{x}) u_2 + \dots\dots + \phi_{ijk_{u_n}}(\mathbf{x}) u_n \quad \dots\dots(8)$$

と書き換えられる(ただし、 n はたかだか有限な値である)。

ここで簡単のために

$$Pr\{\phi(\mathbf{x})=1\} = \phi_{ijk_u}(\mathbf{x}) \quad \dots\dots(9)$$

とおくと、これは、式(4)に期待値操作を施したもののほかならない。いい換えれば、我々の論理モデルの頂上

事象は、ある要素 i に対して、直接原因作用 j がある要素から行なわれることにより毀損 x が生ずる事象を示しており、更なる論理モデルを構成している各事象が状態 \mathbf{x} であり、その論理構造が構造関数 ϕ を形作っていることにほかならない。

式(9)は、式(6)より

$$Pr\{\phi(\mathbf{x})=1\} = Pr\left\{\left(\prod_{j=1}^k x_j(\mathbf{x})\right)=1\right\} \quad \dots\dots(10)$$

となるので頂上事象の定量化のためには、カットセットの定量化が基本的問題となる。

現在カットセットの定量化に関する最も基本的アルゴリズムは、Kinetic Tree Theory (KITT)¹⁹⁾ であろう。KITT においては、以下のような条件下でカット集合の出力事象の生起確率及び発生頻度の期待値を与える。

- (イ) カットへの入力事象は統計的に独立とする。
- (ロ) 入力事象は、発生と消滅に関して指数分布の統計量を有する。
- (ハ) 入力事象は時刻 $t=0$ で非生起である。
- (ニ) 出力事象は全ての入力事象が生起しているときにのみ生起する。
- (ホ) このときに入力事象の発生順序は出力事象の生起に無関係である。

しかしながら、特に人間—機械系では、入力事象の発生順序が出力事象の生起に本質的な意味をもつ場合が多い^{20,21)}。

このような場合、従来は Markov モデルの適用が原理的に考えられていた²²⁾。しかし、Markov モデルでは入力事象の数に制約を受け、解析解は得られておらず、安全性評価上より重要な意味をもつ出力事象の発生頻度の期待値の計算がめんどろである。発生順序依存形のカット集合の定量化に関するアルゴリズムが(ホ)の制約を外したより一般的な条件下で文献^{20,21)}において与えられている。

4.8 まとめ

本論文では、まず新技術を用いた系など運用経験の乏しい系に対するシステムの潜在危険評価とその実施の必要性を論じ、評価手順と各過程での実施上の要件とを述べた。

次に、潜在危険評価の第1段階である潜在危険の同定について論じ、従来のシステム安全では、人間—機

械系における潜在危険の同定を行うための方法論が欠如していることを指摘すると共に、これを行うための新しい手法である作用—変化と作用連鎖モデル (A-Cモデル) を提案した。これにより潜在危険の概念が明確になると共に、潜在危険とリスクとの関係が定式化されている。

また、A-Cモデルを用いて、現在及び将来出現が予想される人間—ロボット系において生じ得る潜在危険の同定例が示されている。

次に、潜在危険評価の第2段階である定性的解析について論じ、ロボットなど多方面において多様な使われ方をするシステムについては、その災害発生機構の解析のための包括的論理モデルの展開が必要なることを述べた。特に、異常時にシステムを停止させるインターロック機構を取り上げ、インターロック機構を構成しているセンサーシステムの故障について論理モデルから考察している。すなわち、センサーシステムなど、危険側である欠報側故障と異常でないとき異常信号を出してしまう誤報側故障など、複数の故障モードを有する系については、安全性向上のためにはそのどちらの側の故障も抑制する必要がある。なぜならば、論理モデルより、もしも欠報側故障の抑制が誤報側故障を増大させる場合には、センサーシステムが人為的に無効にされたり、センサー故障による異常処理作業や修理作業の発生確率が増大されることが指摘されこれが災害にむすびつくことがあるからである。

最後に潜在危険評価の第3段階である定量的評価について論じ、潜在危険、論理モデルおよびリスク間の関係を定式化した。定量的評価ではカット集合の定量化が基本的であることを示し、特に人間—機械系では、事象の発生順序および時間依存性を考慮したアルゴリズムが必要なることを述べ、そのアルゴリズムを示している。

謝辞

本論文は、筆者が科学技庁国内留学制度により、文部省受託研究員として京大工学部システム制御研究室へ派遣され、井上紘一教授、熊本博光博士の御指導を仰いだところが多い。また、関連する各論文発表にあたっては、産業安全技術協会・川口邦供、近藤太二の各氏および中央大学理工学部・塩見弘教授、仮設工業会・森直制博士の諸氏から貴重なコメントをいただい

た。各位に対し、衷心より感謝する。

参考文献

- 1) 佐藤吉信・井上紘一, 潜在危険同定論, 第17回安全工学研究発表会予稿集, pp.71~74, 昭59
- 2) 佐藤吉信, 災害のシステムの解析手法, Quality, No.102, (1985-12), pp.14~14, 昭和シェル石油㈱
- 3) 佐藤・井上・熊本, ロボットの潜在危険評価手法について, 第16回日科技連信頼・安全性シンポジウム報文集, pp.339~344, 昭61
- 4) Ozog, H., "Hazard identification, analysis and control", *Hazard Prevention*, Mag/June, 1985, pp.11~18
- 5) Sate, Y., Inoue, K., and Kumamoto, H., "On hazard identification and analysis of human-robot systems", *Proc. Japan - U.S.A. Symposium on flexible automation*, 1986 pp.679~684
- 6) 塩見弘他, MAEA, FTAの活用, 日科技連
- 7) Lawley, H.G., "Operability studies and hazard analysis", in "Loss Prevention" series Vol.8. AICHE., 1974
- 8) 佐山隼敏, 化学プラントの危険度(1)——オペラビリティ・スタディ——, 安全工学, Vol.19 No.2, pp.93~98, 1980
- 9) Johnson, W.G., *MORT Safety Assurance Systems*, Marcel Dekken, INC., p.247, 1980
- 10) 佐藤吉信・杉本旭・前郁夫, マイクロエレクトロニクスを用いた自動生産システムの安全性評価(第1報; エネルギー転移連鎖と産業用ロボットの潜在危険), 産業安全研究所研究報告 RIIS RR-32-5, pp.1~10, 昭59
- 11) 佐藤・井上, 人間—ロボット系の安全性評価(第1報, 作用—変化と作用連鎖モデルによる潜在危険の同定), 日本機械学会論文集, Vol.51 No.468 pp.2188~2195, 昭60
- 12) 佐藤・井上, 潜在危険とその同定モデルについて, 第15回安全工学シンポジウム講座予稿集, p.55, 昭60
- 13) 佐藤・井上・熊本, 人間—ロボット系の安全性評価(第2報, 作災害発生機構の解析のための論理モデル—その1), 日本機械学会論文集, Vol.

- 52 No.474, pp.2188~2195, 昭61
- 14) 佐藤吉信, マイクロエレクトロニクスを用いた自動生産システムの安全性評価 (第2報, ロボットによる災害を析するための包括的論理モデル—その1), 産業研安研究報告 RIIS-RR-85, pp.21~31
 - 15) 井上監修, FTA 安全工学, 日刊工業, p.73, 昭54
 - 16) Barlow, R., and Proshan, F., *Statistical theory of reliability and life testing probability Models*, McArdle Press, Inc., p.9, 1981
 - 17) 文献14)の p.25, Fig.2
 - 18) 井上・幸田・熊本・高見, 安全監視システムの最適論理構成, 計測と制御, Vol.24 No.2, pp.142~154, 昭60
 - 19) Vesely, W.E., and Narum, R.E., PREP and Kitt; *Computer cords for automatic evaluation of fault trees*, IN-1349, (1970)
 - 20) 佐藤・井上・熊本, 人間—ロボット系の安全性評価 (第3報, 発生順序依存形故障論理の定量化について), 日本機械学会論文集, Vol.52, No.475, pp.1110~1117, 昭61
 - 21) 佐藤吉信, マイクロエレクトロニクスを用いた自動生産システムの安全性評価 (第3報, 修復系の入力事象からなる優先 AND 故障論理の定量化について), 産安研研究報告 RIIS-RR85-5, pp.45~55, 昭61
 - 22) Fussel, J.B., On the quantitative analysis of priority AND failure logic, *IEEE Trans. Reliab.*, R-25(5), pp.324~326 (1976)
-