Research Report of the Research Institute of
Industrial Safety, RIIS-RR-86, 1986.
UDC 519.21 : 62-192 : 005 : 007.52

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4報）
—産業用ロボットの潜在危険抑制手段の抑制力評価—その1—

佐　藤　吉　信*

Safety Assessment of Automated Production Systems Using Microelectronics (4 th Report)
—Evaluation of Hazard Controllability of an Industrial Robot-Part 1—

by Yoshinobu SATO*

Abstract ; An actual unmanned manufacturing station consisting of an NC machine and an industrial robot is assumed (Fig.1). The main hazards of the robot to a human, which occur during troubleshooting in an automatic operation mode, are enumerated using "Action-Chain-models" (Fig.2). Fault Trees of accidents caused by the hazards are given as subsets of "Logic Models for the Analysis of Accident-causation-Mechanisms" (Fig.3), and minimal cut structures are represented by Priority-AND Gates to consider sequential properties of basic events (Fig.4). Furthermore, a manual safety mechanism, an automatic one, and a combination of the two, which cut off the power sources of the robot when a human enters a hazardous zone, are evaluated by comparing expected numbers of occurrences of the top events (Fig.5).

Keywords ; Safety Engineering, Reliability Engineering, Safety, Hazard Assessment, Robot, FTA, Kinetic Tree Theory, Fail Safe Mechanism, Sensor, Safety Equipment

1. 緒　言

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という産業安全上望ましい機能を有する反面，ロボットが災害原因となり得ることについては，いくつかのロボットによる災害事例からも明らかである[1]。また，将来，産業用のみならず日常生活にもロボットが普及されることが考えられる[2]。このような状況に至った場合，その安全性が社会的にも重要な関心事となるであろうことは想像に難くない。

特に産業用ロボットに関しては，その潜在危険に対処するために，労働安全衛生規則が一部改正されるとともに，その使用に関する技術指針なども公示されている。これらにより，現時点での産業用ロボットに対する安全上の方策が示されたこととなる。

しかし，一方では，現代的システム安全手法を用いた体系的な安全性評価が未実施であるという問題も残されている。

一般に，現実の人間—機械系では，見落とし，誤操作あるいは怠慢などによるいわゆるヒューマンエラー，および機器の故障，異常あるいは破壊など，系の個々の要素の異常発生を皆無にすることは実際上不可能である。また，人間に対する潜在危険が存在する系においては，それら個々の要素の異常が，競合することに

* 機械研究部　Mechanical Safety Research Division

よって生ずる災害の発生確率を，非常に小さくすることはできても零にすることはできない。

したがって，安全性向上の合理的に対処しようとする立場からは，系に生ずる潜在危険を同定，解析，そして評価し，そこで用いられる安全上の方策の潜在危険抑制力を把握する必要性か生ずる。そして系の残存リスクが許容できない場合は，さらに別の潜在危険抑制手段を講じなければならない。本研究は，そのようなロボットシステムの安全性評価に貢献することを目的としている。第1報[3]では，予測型安全性評価の第1段階として，潜在危険の同定手法を提案し，これを用いて，人間—ロボット系において生じ得る多様な潜在危険を同定した。第2報[4]では，それら潜在危険のうち，ロボットの運動エネルギー伝ぱ作用による人間への直接潜在危険によって生ずる「人間がロボットの本体または腕に打たれる災害」を取りあげ，その災害発生機構の解析のための包括的論理モデルを作成した。個々の系の潜在危険は，このような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し，頂上事象の生起確率を定量化するなどにより評価可能となる。さらに第3報[5]では，そのような特殊化において，頂上事象の生起に関して基本事象の発生順序が本質的な意味をもつ事例を示し，いわゆる順序依存形故障論理の定量化の必要性を指摘するとともに，そのアルゴリズムを提案した。

本報では，具体的な人間—ロボット系を想定し，これまでに論じた一般化されたモデルやアルゴリズムにもとづいて，そこで用いられる潜在危険抑制手段すなわち安全上の方策を評価する。

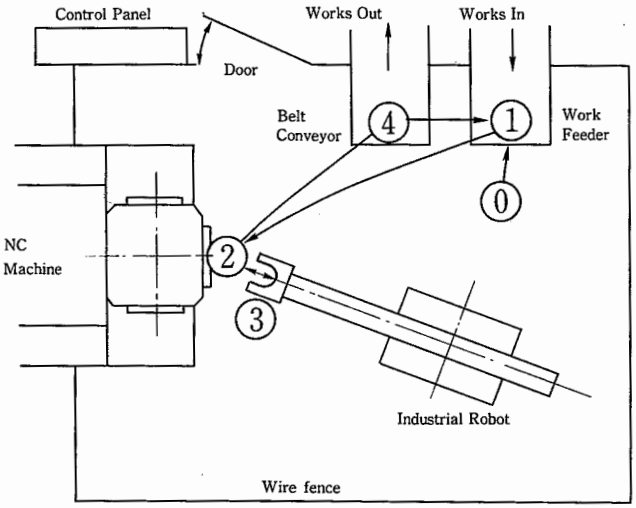


Fig.1　An unmanned-manufacturing work station.
無人ワークステーション

2.　産業用ロボットを用いた無人NCマシン加工ステーションの設定

本報では，産業用ロボットを用いた以下のようなNCマシン加工ステーションを設定する。ただし，ここでは，ロボットの運転状態特性が自動運転モード，作業者などの人間の危険域への存在特性が作業などのため必要上接近して存在するモードからなる系の相に限定して検討する[6]。

2.1　ロボットの自動運転モード

NCマシン，ロボット，ワークフィーダそしてワーク搬出コンベアなどがFig.1のように配置されている。

ロボットの自動運転による作業は，その開始合図とともに，Fig.1の位置⓪で待機していたマニプレータの把持部が作動し，ワークフィーダ上の位置①より室温の金属からなるワークをつかみあげ，マニプレータがこれを把持したまま，NCマシンへのセット位置②まで旋回して，ワークをセットすることにより開始される。

マニプレータは，ワークの加工中，セット位置②よりやや離れた位置③で把持部を待機させ，NCマシンより加工完了の信号を受けるとともに，再びセット位置②でワークを取り出す。さらに，これを把持したまま旋回して，ワーク搬出コンベヤ上の位置④まで搬送する。

作業が1ブロックシーケンスで行われる場合には，ロボットは，ここでマニプレータの把持部を元の位置⓪へ戻し再び作業開始操作が行われるまで，その動力源を切断した状態で停止する。

作業が連続自動運転で行われる場合には，ロボットは，さらに位置④より位置①まで把持部を移動させ，すでにワークフィーダによって供給されている次のワークをつかみあげ，セット位置②でNCマシンにセットし，以下，位置③で待機，位置②で取り出し，位置④まで搬送と同様の作業を作業終了の合図があるまで，くり返し行う。

この加工ステーションの周囲には，ここへの人間の侵入を阻止するとともに，ロボットがワークの把持に失敗することによるワークの外部への飛来を防止するために金網がめぐらされている。加工ステーションの中へは，Fig.1に示すような1箇所のみ存在する入口のドアを開けて入ることができるが，通常，これは施錠され，専任の作業者のみがその鍵を所持している。ま

た，ロボットの操作盤は，入口横の金網外側に設置されている。

2.2 作業者が危険域へ必要上接近して存在するモード

当該加工工程は，連続自動運転時において，通常無人で作業が行われる。しかし時として，ロボットの落としたワークの処理など異常処理作業を行うために，作業者がマニプレータの作動域である危険域内へ立ち入ることの必要が生ずる。ただし，ワークの落下などの異常が生じても，系の自動運転モードは自動的には解消されず，作業は続行される。

作業者が，金網内の危険域に入る場合には，入口横の操作盤で，ロボットの運転モードを連続自動運転から1ブロックシーケンスに切換える操作を行い，これによって，ロボットはNCマシンで加工完了となったワークを位置④まで搬送した後，把持部を位置⓪に戻し，動力源を切断した状態で完全に停止する。作業者は，ロボットの完全停止を確認して中に入らなければならない。

3. 潜在危険の特定

ロボットの人間に対する潜在危険には種々のものが同定されている[7]。Fig.1に示す系の設定条件より，主要な潜在危険として，ロボットのマニプレータおよびワークの運動エネルギーによる直接原因作用が特定される。この直接原因作用により，作業者がマニプレータによって打たれたり，マニプレータとコンベヤの間に挟まれるなどの災害が発生することが想定されるが，本報では，作業者がマニプレータにより打たれる場合を検討する。

3.1 手動停止機構を備えた系

前章で設定された系において，想定された災害をひき起こす作用連鎖が，次のように特定される。

Case 1：作業者が危険域に入る際に，Fig.1に示される入口横の操作盤でのロボット停止操作を怠り(f 1*；Fig.2の記号に対応し，アルファベットが作用の種類，数字が作用の順序を表す[8])，NCマシンからワーク加工完了記号（b 1）により，マニプレータが作動し，危険域に存在する作業者（e 1**）に対して直接原因作用が行われる（a 0)。

Case 2：作業者はロボット停止操作を行うが，完全停止の確認を怠り（f 2*)，完全停止以前に侵入する（e 1*)ため，NCマシンからロボットへのワーク加工完了信号により(b 1)，マニプレータが作動して作業者に対し直接原因作用が行われる（a 0)。

このほか，作業者はロボットの完全停止後に入るが，第三者がロボットの再起動操作を行ってしまう場合や機器の異常などによる場合も想定されるが，本報ではそれらは省略する。

3.2 自動停止機構を備えた系

前述の手動操作による停止機構のかわりに，いわゆる人間の危険域侵入の検出システムによる自動停止機構を備えた系も想定される。この場合には，次のCaseが特定される。

Case 3：作業者が危険域に侵入したとき(e 1**)，センサシステムが誤信号を発生し（b 1*)，NCマシンの加工の完了信号により(b 1)，マニプレータが作動するため作業者に対して直接原因作用が行われる（a 0)。

Case 4：作業者が危険域に侵入したとき(e 1**)，インターロックが駆動せず（a 1*)，NCマシンの加工完了信号により（b 1）マニプレータが作動し，作業者に対して直接原因作用（a 0）が行われる。

3.3 手動停止と自動停止の両機構を備えた系

前述の手動停止と自動停止の両機構を二重に備えた系では，次のCaseが同様に特定される。

Case 5：作業者が手動停止操作を怠り(f 1*)危険域に侵入する(e 1***)。このとき，センサシステムが誤信号を発生し(b 1**)，NCマシンからの加工の完了信号により(b 1)，マニプレータが作動するため作業者に対し直接原因作用が行われる（a 0)。

Case 6：作業者は手動停止操作を行うが，ロボットの完全停止の確認を怠り（f 2**）危険域に侵入する（e 1**)。このときセンサシステムが誤信号を発生し(b 1*)，NCマシンから，加工完了信号が送られ(b 1)，マニプレータが作動するため，作業者に対し直接原因作用が行われる（a 0)。

Case 7：作業者が手動停止操作を怠り(f 1***)危険域に侵入する(e 1**)。このときインターロックが駆動せず（a 1*)，NCマシンからの加工完了信号（b 1）によりマニプレータが作動し，作業者に対し直接原因作用（a 0）が行われる。

Case 8：作業者は手動停止操作を行うが，ロボットの完全停止の確認を怠り（f 2**）危険域に侵入する（e 1**)。このときインターロックが駆動せず(a 1*)，NCマシンからの加工完了信号（b 1）によりマニプレータ

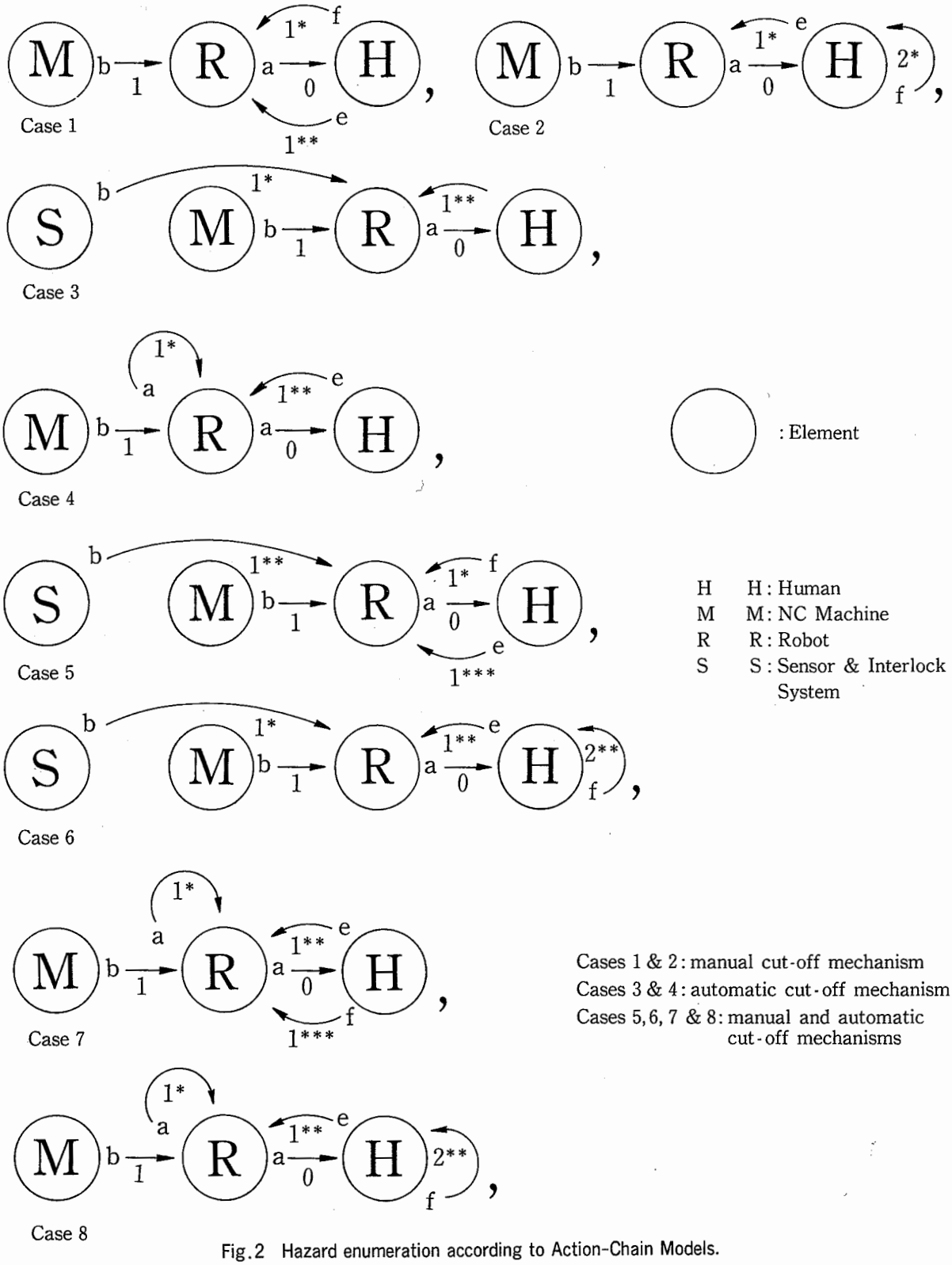


Fig. 2　Hazard enumeration according to Action-Chain Models.
作用一連鎖モデルによる潜在危険の特定

が作動し，作業者に対し直接原因作用（a 0）が行われる。

4. 災害発生機構の Fault Trees

3章で Fig.2 のように特定された作用連鎖による災害発生論理は，論理モデル[9]からそれぞれ Fig.3 の様に Fault Trees で表される。ただし，マニプレータの強度，出力，速度などは災害を生じさせるのに十分なほど大きいものとする。ここで，Fig.3 および本文における各事象記号は論理モデルの事象識別記号に，作用とその順序記号は Fig.2 にそれぞれ対応している。

すなわち，Case 1 では，「マニプレータの作動」(Eb_{10}) 事象は，ワーク加工完了の「停止条件の解消」(Ef_{24}) による動作記号(b 1)，インターロックによる自動停止機構の「不設置」(Ee_{21}) 常起事象，および「停止のための操作を怠る：f 1*」($Ed_{11,1}$) による「動力源の存在」(Ed_{11}) 事象がすべて生起することにより生ずる。そして，頂上事象「マニプレータによって打たれる：a 0」(Ea_{04}) は，「防護の不設置」(Oa_{02}) 常起事象，「異常処理作業」(Nc_{09}) のための「危険域に存在 e 1**」(Eb_{12}) 事象，および「マニプレータの作動」(Eb_{10}) 事象がすべて生起することにより生ずる。

Case 2 では，「1ブロックシーケンス運転の完了以前」($Ed_{11,2}$) のために「動力源が存在する」(Ed_{11}) 論理以外は Case 1 と等価な論理となる。

Case 3 では，作業者の侵入を誤信号（b 1*）により「検出しない」ことによるインターロック失敗論理，および手動停止機構の「不設置」($Ed_{11,3}$) により動力源が常に存在する論理以外は，Case 1 と等価は論理となる。

Case 4 では，「インターロックが駆動しない」(Ee_{19}) ことによるインターロック失敗論理以外は Case 3 と等価な論理となる。

Case 5 では，「停止のための操作を怠る：f 1*」($Ed_{11,1}'$) ことによる「動力源の存在」(Ed_{11}') 論理以外は，Case 3 と等価な論理となる。

Case 7 では，「停止のための操作を怠る：f 1*」($Ed_{11,1}'$) ことによる「動力源の存在」(Ed_{11}') 論理以外は，Case 4 と等価な論理となる。

Case 8 では，「1ブロックシーケンス運転完了以前」($Ed_{11,2}'$) のために「動力源が存在する」(Ed_{11}') 論理以外は，Case 4 と等価な論理となる。

Fig.3 より，各ケースにおける最小カット集合 $C(x)_i$ が次のように得られる。

$$\text{Case 1}: C(x)_1=\{Ef_{24}, Ed_{11,1}, Eb_{12}\} \quad \cdots\cdots(1)$$

$$\text{Case 2}: C(x)_2=\{Ef_{24}, Ed_{11,2}, Eb_{12}\} \quad \cdots\cdots(2)$$

$$\text{Case 3}: C(x)_3=\{Ef_{24}', Ee_{18}, Eb_{12}'\} \cdots\cdots(3)$$

$$\text{Case 4}: C(x)_4=\{Ef_{24}, Ee_{19}, Eb_{12}'\} \cdots\cdots(4)$$

$$\text{Case 5}: C(x)_5=\{Ef_{24}'', Ee_{18}', Ed_{11,1}', Ed_{12}''\} \cdots\cdots(5)$$

$$\text{Case 6}: C(x)_6=\{Ef_{24}'', Ee_{18}', Ed_{11,2}', Eb_{12}''\} \cdots\cdots(6)$$

$$\text{Case 7}: C(x)_7=\{Ef_{24}'', Ee_{19}', Ed_{11,1}', Eb_{12}''\} \cdots\cdots(7)$$

$$\text{Case 8}: C(x)_8=\{Ef_{24}'', Ee_{19}', Ed_{11,2}', Eb_{12}''\} \cdots\cdots(8)$$

5. 基本事象の生起条件

カット $C(x)_i$ を構成する基本事象に，次のような生起条件を設定しても不自然ではない。

条件（1） 連続運転モードでは，作業開始後十分時間の経過した定常状態で，単位時間当たり平均 a_1 個のワークが加工される。すなわちマニプレータは，Fig.1 に示された③→②→④→①→②→③の動作の平均 a_1 h^{-1} 行い，この動作持続時間は平均 b_1^{-1} h である。

条件（2） 作業者に危険域内での異常処理作業を行わせようとする事象の期待発生回数は，作業が開始されて十分時間の経過した定常状態で a_2 h^{-1}，また危険域内へとどまる時間の期待値は b_2^{-1} h である。

条件（3） 作業者が危険域に入ろうとする条件下で，停止操作を怠る確率は，q_1（一定）である。

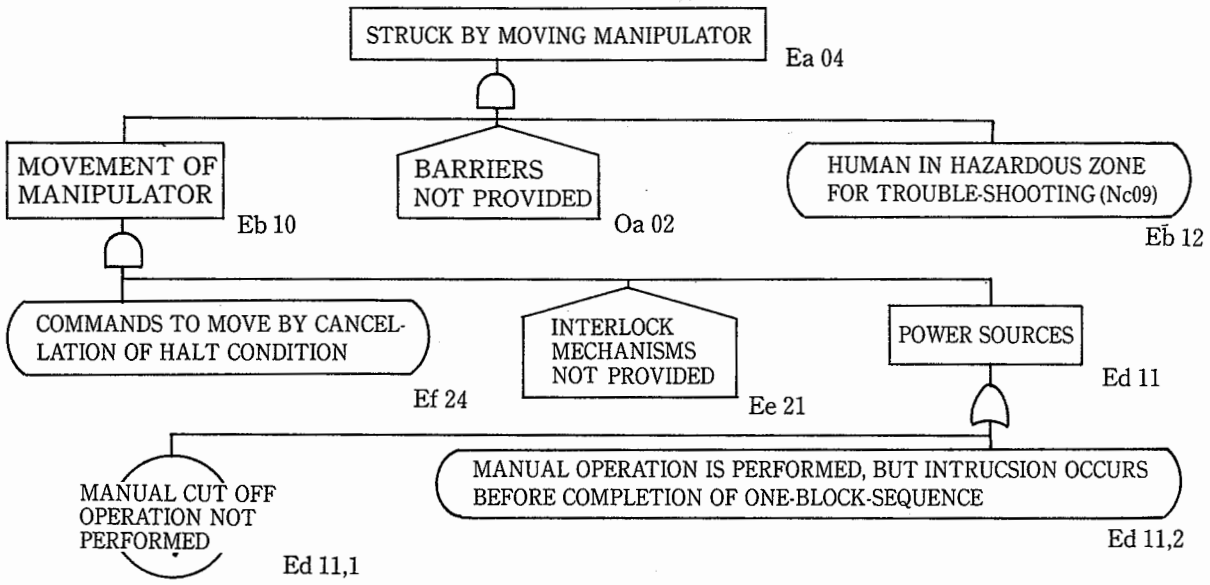
条件（4） 作業者の侵入検出失敗は，センサの故障により生じ，センサの MTTF は a_3^{-} h，MTTR は b_3^{-1} h である。

条件（5） インターロックの駆動失敗はリレーの open 側故障または機械的構造の破壊により生じ，その発生確率は1作動要求あたり p_1（一定）である。

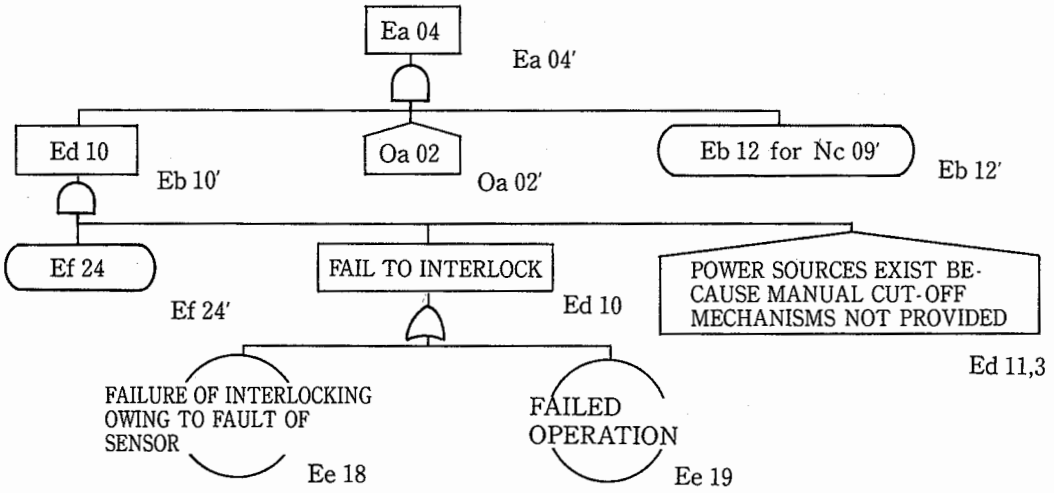
条件（6） インターロックによる停止は，検出と同時に行われ，いったん停止されると，作業者が金網外へ出て，再起動操作を行わないかぎり停止状態を保つ。また，センサは必ず作業者が危険域に入る前に検出するものとし，検出してから作業者が危険域に入るまでの時間は十分小さく無視できる。

条件（7） 作業者が手動停止操作を行った条件下で，マニプレータの完全停止の確認を怠り危険域に入ろうとする確率は q_2（一定）である。また，操作してから

a) Cases1 & 2 : Systems with Manual Cut-Off Mechanisms



b) Case 3 & 4 : Systems with Automatic Cut-Off Mechanisms



C) Cases 5, 6, 7 & 8 : Systems with Manual and Automatic Cut-Off Machanisms

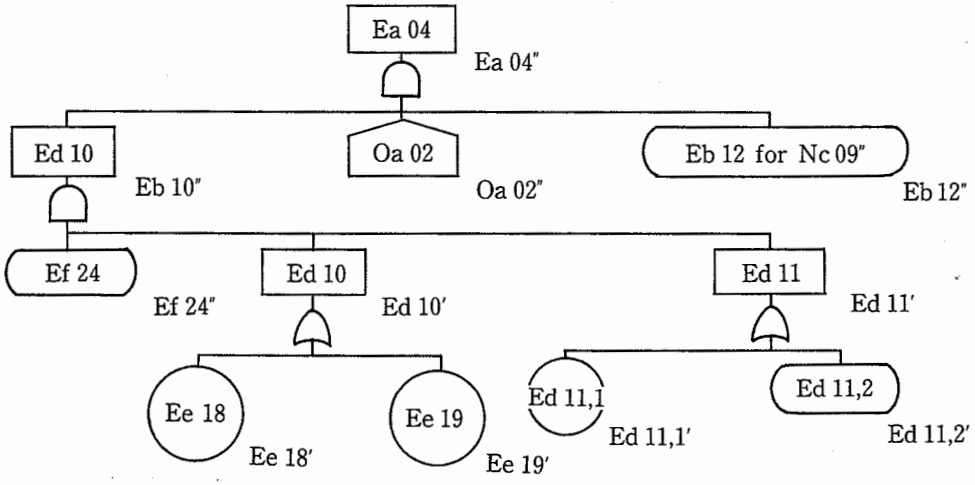


Fig. 3　Fault trees of accident-causation mechanisms.
災害発生機構のフォールト・ツリー

侵入しようとする時間は無視できる。

条件(8)　作業者が事象 $Ed_{11,1}$, $Ed_{11,2}$, Ee_{18}, $Ed_{11,1}'$ または $Ed_{11,2}'$ の条件下で，危険域に入ろうとしたとき，マニプレータが待機中では必ず侵入し，目前を動作している最中での侵入はまれであり無視できる。また，入ろうとしてから侵入完了までの時間は無視できる。

6. 発生順序を考慮した最小カット

4章で得られたカットは，事象 $U_1=\{$事象 $Ed_{11,1}$ の条件下での条件での事象 Nc_{09} の生起$\}$, $U_2=\{Ed_{11,2}$ の条件下での Nc_{09} の生起$\}$, $U_3=\{Ee_{19}$ の条件下での Nc_{09}' の生起$\}$, $U_4=\{Ed_{11,1}'$ の条件下での Nc_{09}'' の生起$\}$, $U_5=\{Ed_{11,2}'$ の条件下での Nc_{09}'' の生起$\}$, $U_6=\{Ed_{11,1}'$ および Ee_{19}' の条件下での Nc_{09}'' の生起$\}$ および $U_7=\{Ed_{11,2}'$ および Ee_{19}' の条件下での Nc_{09}'' の生起$\}$ とすると，次のように書きかえられる。

$$C(x)_1=\{Ef_{24}, U_1\} \quad \cdots\cdots(9)$$

$$C(x)_2=\{Ef_{24}, U_2\} \quad \cdots\cdots(10)$$

$$C(x)_3=\{Ef_{24}', Ee_{18}, Nc_{09}'\} \quad \cdots\cdots(11)$$

$$C(x)_4=\{U_3, Ef_{24}'\} \quad \cdots\cdots(12)$$

$$C(x)_5=\{Ef_{24}'', Ee_{18}', U_4\} \quad \cdots\cdots(13)$$

$$C(x)_6=\{Ef_{24}'', Ee_{18}', U_5\} \quad \cdots\cdots(14)$$

$$C(x)_7=\{U_6, Ef_{24}''\} \quad \cdots\cdots(15)$$

$$C(x)_8=\{U_7, Ef_{24}''\} \quad \cdots\cdots(16)$$

これらのカットの生起には，前章の条件(6)，(8)より

(i)　事象 Ee_{18}, Ee_{18}' がそれぞれ，事象 Nc_{09}', U_4, U_5 に先立って生起している。

(ii)　事象 $U_1, U_2, Nc_{09}', U_3, U_4, U_5, U_6, U_7$ が，それぞれ事象 $Ef_{24}, Ef_{24}', Ef_{24}''$ に先立って生起していることが必要である。

以上の条件を考慮したカットの生起の正確な論理は，優先 AND ゲートを用いて，Fig.4 のように表現される。

7. 基本事象の定量化とカットの発生回数評価アルゴリズム

7.1 基本事象の定量化

基本事象の定量化に際し，次の仮定を置く。

仮定(1)　条件(1)より，事象 Ef_{24}, Ef_{24}', Ef_{24}'' の生起は，定数発生率 $a_1b_1/(b_1-a_1)\,\mathrm{h}^{-1}$ と修復率 $b_1\,\mathrm{h}^{-1}$ の指数分布でモデル化される。

仮定(2)　条件(2)より，事象 Nc_{09}, Nc_{09}', Nc_{09}'' の生起は，定数発生率 $a_2b_2/(b_2-a_2)\,\mathrm{h}^{-1}$ と修復率 $b_2\,\mathrm{h}^{-1}$ の指数分布でモデル化される。

仮定(3)　条件(4)より，事象 Ee_{18}, Ee_{18}' の生起は，定数発生率 $a_3b_3/(b_3-a_3)\,\mathrm{h}^{-1}$ と修復率 $b_3\,\mathrm{h}^{-1}$ の指数分布でモデル化される。

仮定(4)　基本事象は，その生起に関して統計的に独立で，時刻零でそれぞれ非生起とする。

7.2 カット発生回数評価のアルゴリズム

Case 1：事象 U_1 の生起は，仮定(2)および条件(3)などより，定数発生率 $q_1a_2b_2/(b_2-q_1a_2)\,\mathrm{h}^{-1}$ と修復率 $b_2\,\mathrm{h}^{-1}$ の指数分布に従う。さらに仮定(1)より，時刻零ですべての入力事象が非生起の条件下で，時刻 t までのこのカットの発生回数の期待値 ${W_1}^*_{(0,t)}$ は，前報式(4)，(5)，(26)などから，2入力事象として得られる式(17)において，

$$\lambda_1=q_1a_2b_2/(b_2-q_1a_2),\quad \mu_1=b_2$$
$$\lambda_2=a_1b_1/(b_1-a_1),\quad \mu_2=b_1$$

として与えられる。

Case 2：事象 U_2 の生起は，仮定(2)および条件(6)などより，定数発生率 $(1-q_1)q_2a_2b_2/\{b_2-(1-q_1)q_2a_2\}\,\mathrm{h}^{-1}$ と修復率 $b_2\,\mathrm{h}^{-1}$ の指数分布に従う。したがって，Case 1 と同様に，このカットの ${W_2}^*_{(0,t)}$ は，式(17)において，

$$\lambda_1=(1-q_1)q_2a_2b_2/\{b_2-(1-q_1)q_2a_2\},\quad \mu_1=b_2$$
$$\lambda_2=a_1b_1/(b_1-a_1),\quad \mu_2=b_1$$

として得られる。

Case 3：同様に，このカットの ${W_3}^*_{(0,t)}$ は，式(18)において，

$$\lambda_1=a_3b_3/(b_3-a_3),\quad \mu_1=b_3$$
$$\lambda_2=a_2b_2/(b_2-a_2),\quad \mu_2=b_2$$

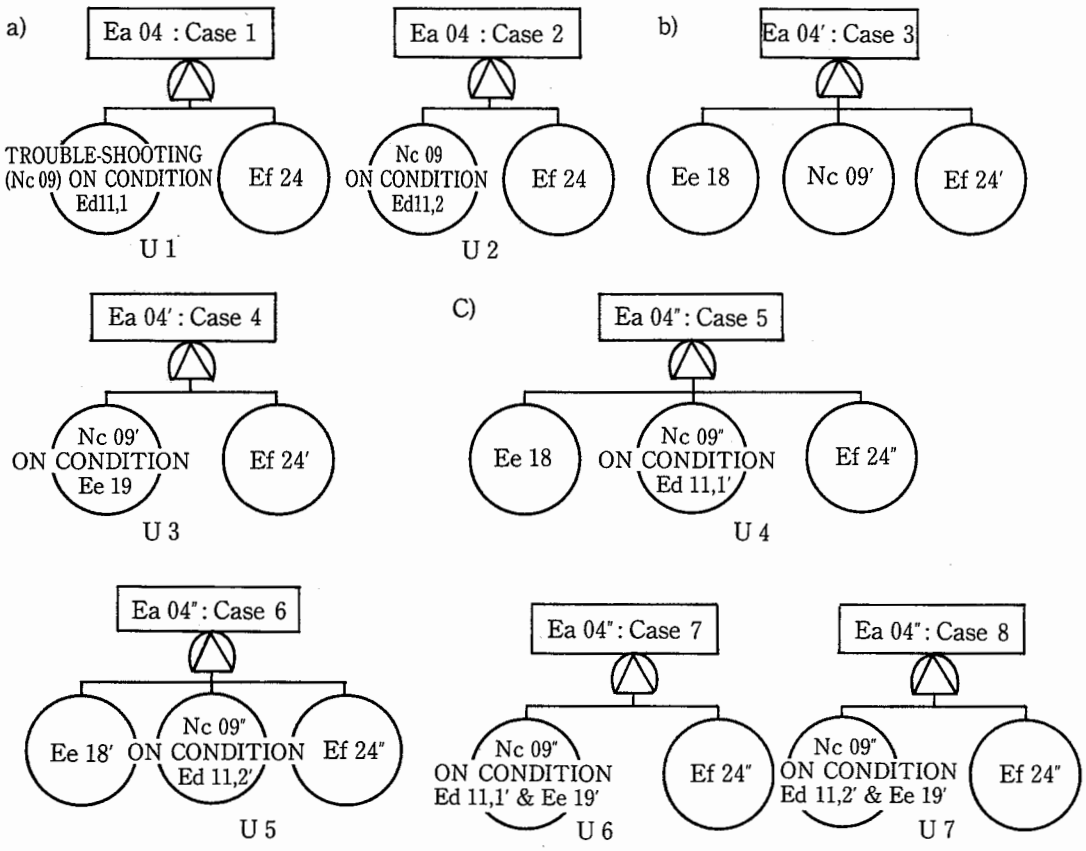


Fig.4　Representation of minimal cut sets using Priority-AND gate.
Priority-AND ゲートによる最小カット集合の記述

$$\lambda_3 = a_1 b_1/(b_1 - a_1),\quad \mu_3 = b_1$$

として与えられる。

Case 4：同様に，このカットの $W_4^*{}_{(0,t)}$ は，式(17)において

$$\lambda_1 = p_1 a_2 b_2/(b_2 - p_1 a_2),\quad \mu_1 = b_2$$
$$\lambda_2 = a_1 b_1/(b_1 - a_1),\quad \mu_2 = b_1$$

として与えられる。

Case 5：同様に，このカットの $W_5^*{}_{(0,t)}$ は，式(18)において

$$\lambda_1 = a_3 b_3/(b_3 - a_3),\quad \mu_1 = b_3$$
$$\lambda_2 = q_1 a_2 b_2/(b_2 - q_1 a_2),\quad \mu_2 = b_2$$
$$\lambda_3 = a_1 b_1/(b_1 - a_1),\quad \mu_3 = b_1$$

として得られる。

Case 6：同様に，このカットの $W_6^*{}_{(0,t)}$ は，式(18)において

$$\lambda_1 = a_3 b_3/(b_3 - a_3),\quad \mu_1 = b_3$$
$$\lambda_2 = (1-q_1) q_2 a_2 b_2/\{b_2 - (1-q_1) q_2 a_2\},\quad \mu_2 = b_2$$
$$\lambda_3 = a_1 b_1/(b_1 - a_1),\quad \mu_3 = b_1$$

として得られる。

Case 7：同様に，このカットの $W_7^*{}_{(0,t)}$ は，式(17)において

$$\lambda_1 = q_1 p_1 a_2 b_2/(b_2 - q_1 p_1 a_2),\quad \mu_1 = b_2$$
$$\lambda_2 = a_1 b_1/(b_1 - a_1),\quad \mu_2 = b_1$$

として与えられる。

Case 8：同様に，このカットの $W_8^*{}_{(0,t)}$ は，式(17)において

$$\lambda_1 = (1-q_1) q_2 p_1 a_2 b_2/\{b_2 - (1-q_1) q_2 p_1 a_2\},\quad \mu_1 = b_2$$
$$\lambda_2 = a_1 b_1/(b_1 - a_1),\quad \mu_2 = b_1$$

として与えられる。

(17)　(18)
(ただし，$i=1,2,4,7,8$, $j=3,5,6$ とする)

8. 頂上事象の期待発生回数による停止機構の潜在危険抑制力の評価

停止機構の潜在危険抑制力を，各場合の頂上事象の期待発生回数を求めることによって評価しよう。ここでは，系に以下の具体的な数値を設定する：a_1(ワークの平均加工数)$=20\ \mathrm{h}^{-1}$，b_1^{-1}(マニプレータの動作時間)$=9$ s；a_2(異常処理作業期待発生回数)$=10^{-2}\ \mathrm{h}^{-1}$，$b_2^{-1}$(危険域にとどまる平均時間)$=12$ s；q_1(停止操作を怠る確率)$=q_2$(完全停止の確認を怠る確率)$=3\times$

$$W^*_{i(0,t)}=\left(\frac{\lambda_1}{\lambda_1+\mu_1}\right)\left(\frac{\lambda_2}{\lambda_2+\mu_2}\right)\left\{\mu_2 t-\frac{\lambda_2 e^{-(\lambda_2+\mu_2)t}}{\lambda_2+\mu_2}+\frac{\mu_2 e^{-(\lambda_1+\mu_1)t}}{\lambda_1+\mu_1}+\frac{\lambda_2 e^{-(\lambda_1+\mu_1+\lambda_2+\mu_2)t}}{\lambda_1+\mu_1+\lambda_2+\mu_2}\right.$$
$$\left.+\frac{\lambda_2}{\lambda_2+\mu_2}-\frac{\mu_2}{\lambda_1+\mu_1}-\frac{\lambda_2}{\lambda_1+\mu_1+\lambda_2+\mu_2}\right\} \quad \cdots\cdots(17)$$

$$W^*_{j(0,t)}=\int_0^t w^*_{(\tau)}d\tau=\left\{\prod_{i=1}^{3}\left(\frac{\lambda_i}{\lambda_i+\mu_i}\right)\right\}\left[\left\{\left(\frac{\mu_2}{\mu_1+\mu_2}\right)t+\frac{\mu_2 e^{-(\lambda_1+\mu_1)t}}{(\mu_2-\lambda_1)(\lambda_1+\mu_1)}+\frac{\lambda_2 e^{-(\lambda_2+\mu_2)t}}{(\lambda_2-\mu_1)(\lambda_2+\mu_2)}\right.\right.$$
$$\left.-\left(\frac{\lambda_1}{\lambda_1+\lambda_2}+\frac{\mu_1}{\mu_1+\mu_2}+\frac{\mu_1}{\lambda_2-\mu_1}+\frac{\lambda_1}{\mu_2-\lambda_1}\right)\frac{e^{-(\mu_1+\mu_2)t}}{\mu_1+\mu_2}-\frac{\lambda_2 e^{-(\lambda_1+\mu_1+\lambda_2+\mu_2)t}}{(\lambda_1+\lambda_2)(\lambda_1+\mu_1+\lambda_2+\mu_2)}\right\}\mu_3$$
$$+\left\{-\frac{\mu_2 e^{-(\lambda_3+\mu_3)t}}{(\mu_1+\mu_2)(\lambda_3+\mu_3)}+\frac{\mu_2 e^{-(\lambda_1+\mu_1+\lambda_3+\mu_3)t}}{(\mu_2-\lambda_1)(\lambda_1+\mu_1+\lambda_3+\mu_3)}+\frac{\lambda_2 e^{-(\lambda_2+\mu_2+\lambda_3+\mu_3)t}}{(\lambda_2-\mu_1)(\lambda_2+\mu_2+\lambda_3+\mu_3)}\right.$$
$$-\left(\frac{\lambda_1}{\lambda_1+\lambda_2}+\frac{\mu_1}{\mu_1+\mu_2}+\frac{\mu_1}{\lambda_2-\mu_1}+\frac{\lambda_1}{\mu_2-\lambda_1}\right)\frac{e^{-(\mu_1+\mu_2+\lambda_3+\mu_3)t}}{\mu_1+\mu_2+\lambda_3+\mu_3}-\frac{\lambda_2 e^{-(\lambda_1+\mu_1+\lambda_2+\mu_2+\lambda_3+\mu_3)t}}{(\lambda_1+\lambda_2)(\lambda_1+\mu_1+\lambda_2+\mu_2+\lambda_3+\mu_3)}\Big\}\lambda_3$$
$$-\left\{\frac{\mu_2}{(\mu_2-\lambda_1)(\lambda_1+\mu_1)}+\frac{\lambda_2}{(\lambda_2-\mu_1)(\lambda_2+\mu_2)}-\left(\frac{\lambda_1}{\lambda_1+\lambda_2}+\frac{\mu_1}{\mu_1+\mu_2}+\frac{\mu_1}{\lambda_2-\mu_1}+\frac{\lambda_1}{\mu_2-\lambda_1}\right)\frac{1}{\mu_1+\mu_2}\right.$$
$$\left.-\frac{\lambda_2}{(\lambda_1+\lambda_2)(\lambda_1+\mu_1+\lambda_2+\mu_2)}\right\}\mu_3-\left\{-\frac{\mu_2}{(\mu_1+\mu_2)(\lambda_3+\mu_3)}+\frac{\mu_2}{(\mu_2-\lambda_1)(\lambda_1+\mu_1+\lambda_3+\mu_3)}\right.$$
$$+\frac{\lambda_2}{(\lambda_2-\mu_1)(\lambda_2+\mu_2+\lambda_3+\mu_3)}-\left(\frac{\lambda_1}{\lambda_1+\lambda_2}+\frac{\mu_1}{\mu_1+\mu_2}+\frac{\mu_1}{\lambda_2-\mu_1}+\frac{\lambda_1}{\mu_2-\lambda_1}\right)$$
$$\left.\left.\times\frac{1}{\mu_1+\mu_2+\lambda_3+\mu_3}-\frac{\lambda_2}{(\lambda_1+\lambda_2)(\lambda_1+\mu_1+\lambda_2+\mu_2+\lambda_3+\mu_3)}\right\}\lambda_3\right] \quad \cdots\cdots(18)$$

(ただし，$i=1,2,4,7,8$, $j=3,5,6$ とする)

10^{-3} (怠りによる人的過誤確率[10])，p_1 (インターロックの駆動失敗確率)$=2\times10^{-6}$ demand^{-1}(リレーの open 側故障確率[11]または機械的構造の破壊による失敗確率)とする。

センサは，MTTF$(a_3^{-1})=3.33\times10^3$ h とし，

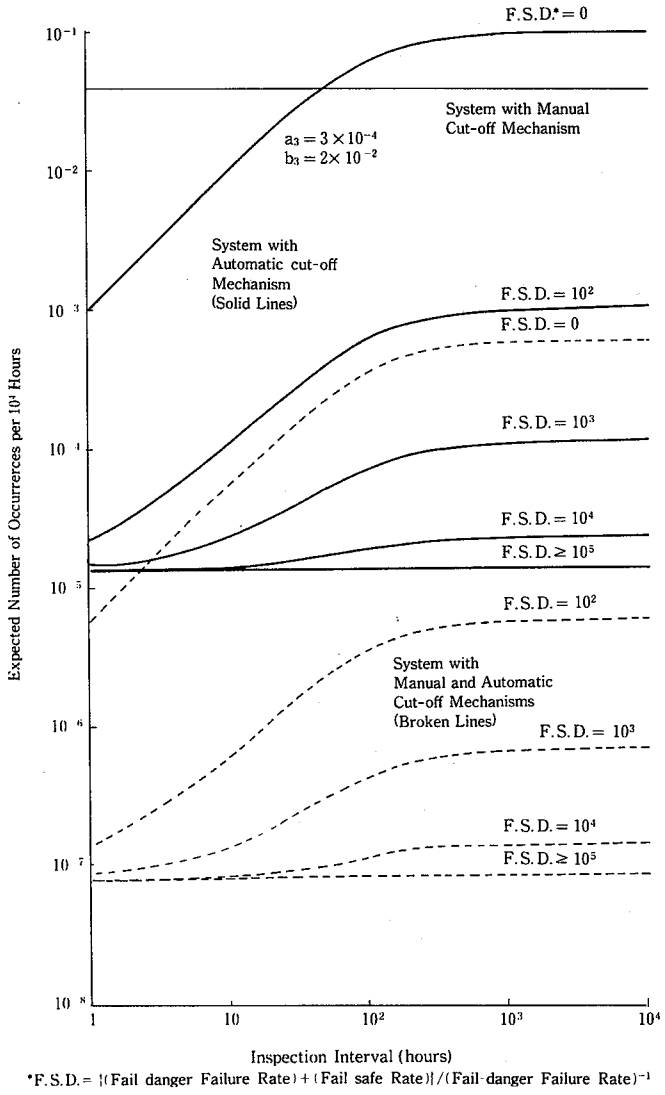
(フェイル・セイフ度)＝(危険側故障率
＋安全側故障率)/(危険側故障率)－1.0　(19)

で定義されるフェイル・セイフ度 $0,10^2,10^3,10^4,10^5$ の各場合のものが利用できるものとする。また，このとき定期点検が無い場合における故障持続時間の期待値を$(b_3^{-1}=)50$ h とし，危険側に故障中のセンサは定期点検によっても完全に新品のものと置き換えられるものとする。安全側に故障したときは，センサはただちに新品のものと置き換えられるがこの影響はわずかであり無視する。

手動停止機構，自動停止機構，そして手動と自動の両機構を備えた各系における頂上事象の 10^4 h あたりの期待発生回数が Fig. 5 のように得られる。

手動停止機構の系の期待発生回数を基準にとれば，フェイル・セイフ度 (F.S.D.)$=0$ のセンサを用いた自動停止機構の系では，点検間隔が 50 h 以上となると基準を満足しない。センサの F.S.D. を高めるとそれに応じて系の安全性は向上するが，F.S.D. がほぼ 10^5 となったところで飽和し，これ以上 F.S.D. を高めても安全性には変化が生じない。これは，センサの F.S.D. が高くなるに従って，相対的にセンサ以外の故障モードの影響が支配的となるためである。

手動停止機構の場合では，本報のような系が 10^4 存在



*F.S.D. = {(Fail danger Failure Rate) + (Fail safe Rate)}/(Fail-danger Failure Rate)$^{-1}$

Fig.5　Expected number of occurrences of top events per 10^4 hours for Fail Safe Degrees (F.S.D.) of sensors.
センサーの各フェイル・セイフ度に対する頂上事象の 10^4 h あたりの期待発生回数

し，それらが 10^4 h の連続自動運転を行うと，本報で特定した望ましくない頂上事象が 400 件近く発生することとなる。そして，そのうちの何割かは死亡や重傷災害につながることが考えられる。したがって，手動停止機構の場合には，必ずしも安全性が十分満足できるとは言いがたい。

本報のような条件にある人間—産業用ロボット系では，自動停止機構を備えることが望ましい。その際 F.S.D. を 10^5 まで高めることは，この場合非常に合理的である。

9. ま と め

本報では，産業用ロボットを用いた系を具体的に想定し，これまでに論じたモデルやアルゴリズムを用いて，そこで生ずる潜在危険を特定することにより災害発生機構を解析した。そして頂上事象の期待発生回数を求め，手動および自動停止機構によるロボットの人間に対する潜在危険抑制力を評価した。

いくつかのコメントが以下のように与えられる：

本報告では，手動停止の場合，10^4 h の連続自動運転として頂上事象の期待発生回数を求めている。現実には自動運転は種々の事情により中断される。しかし，式(17)からわかるように，事象の生起状態が非常に速く定常状態となり，例えば，1 h 以上この運転モードが継続されると，非定常状態の影響はほとんど無視できる。したがって，連続の 10^4 h は，各連続自動運転が 1 h 以上続くとき，それらの累積時間と考えてよい。

自動停止の場合では，点検から次の点検までの連続自動運転とし，その累積時間を 10^4 h としている。この場合でも一点検間隔内における中継回数がさほど多くなく，中断時間もあまり長くないとき，発生回数を多少高く見積もることとなるが本報での評価が許容されよう。中断時間が長い場合には，例えば，中断時間分の期待発生回数を差引くなどの工夫が必要である。

多重センサを用いる場合は，入力事象を増加させることにより，前報の式(4)，(5)から同様に頂上事象の期待発生回数を求めることができる。

謝　辞

本研究を遂行するに当たり，京大工・井上紘一教授，熊本博光氏および当研究所の先輩，同僚諸氏に御指導・御助言をいただいた。衷心より感謝する。

(昭和 61 年 11 月 25 日受理)

参考文献

1) 望月，産業用ロボットの導入と安全対策，(昭 59)，102，212，日本労働総合研究所
2) 加藤，からくりからマイ・ロボットへ，機械学会誌，87-792，(昭 59)，1245
3) 佐藤・杉本・前，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)，RIIS RR-32-5 (昭 59)，p.1～10
4) 同上 (第 2 報) RIIS RR-85-3，p.22～31
5) 同上 (第 3 報) RIIS RR-85-5，p.45～55

6) 文献4) のp.25～27
7) 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，51-468，C(昭60)，2188
8) 文献7）のp.2192
9) 文献4）のp.28
10) Henley, E.J. and Kumamoto, H., Reliability Engineering and Risk Assessment, (1981), 286 Prentice-Hall, Englewood Cliffs. New Jersey.
11) IEEE Std 500, RELIABILITY DATA, p.115