人間-ロボット系の安全性評価*

(第4報, 1台のハンドリング産業用ロボットの潜在危険抑制措置の評価)

佐藤吉信**, 井上紘一***, 熊本博光****

The Safety Assessment of Human-Robot Systems
(4th Report, Evaluations of Hazard Control Measures for an Industrial Robot
Handling Work Pieces)

by Yoshinobu SATO, Koichi INOUE, and Hiromitsu KUMAMOTO

An actual unmanned manufacturing station consisting of an NC machine and an industrial robot is assumed. The main hazards of the robot to a human, which occur for the troubleshooting in the automatic operation mode of the system, are enumerated using the "Action-Chains-Model". The Fault Trees of the accidents caused by the hazards are given as the subsets of the "Logic Models for the Analysis of the Accident-Causation-Mechanisms", and the minimal cut structures are represented with Priority AND Gates in consideration of the specifications of the basic events. Furthermore, the hazard controllability of a manual, an automatic, and a combined mechanism to cut off the power sources of the robot when human enters the site are evaluated by comparing the expected numbers of occurrences of the respective top events.

Key Words: Safety Engineering, Reliability Engineering, Safety Assessment, Industrial Robot, FTA, Kinetic Tree Theory

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實際上不可能である。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うん合することに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、安全性向上に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が生ずる。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、予測形安全性評価の第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ば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

* 昭和61年6月21日 東北支部秋田地方講演会において講演、原稿受付 昭和60年10月28日。

** 正員、労働省産業安全研究所 (〒108 東京都港区芝5-35-1)。

*** 正員、京都大学工学部 (〒606 京都市左京区吉田本町)。

**** 京都大学工学部。

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⁽⁶⁾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。

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 ロボットの自動運動モード 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ヤなどが図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、図1の位置①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①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、図1に示すような1箇所のみ存在する入口の

図1 産業用ロボットを用いた NC マシン無人加工ステーション各機配置図

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、金網外側の入口横に設置されている。

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、系の自動運転モードは自動的に解消されず、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⑩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⁾。図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、図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 ($f1^*$; 図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マシンからのワーク加工完了信号 ($b1$) により、マニプレータが作動し、危険域に存在する作業者 ($e1^{**}$) に対して直接原因作用が行われる ($a0$)。

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 ($f2^*$)、完全停止以前に侵入する ($e1^*$) 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 ($b1$)、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 ($a0$)。

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。

図2 作用-連鎖モデルによる潜在危険の特定

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 ($e1^{**}$)、センサシステムがその検知に失敗し ($f1^*$)、NC マシンの加工の完了信号により ($b1$)、マニプレータが作動し、作業者に対して直接原因作用が行われる ($a0$)。

この場合でも、センサ以外の他の要素の異常などによるものも想定されるが、本報では省略する。

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 4: 作業者が手動停止操作を怠り ($f1^*$) 危険域に侵入する ($e1^{***}$)。このとき、センサシステムがその検出に失敗し ($f1^{**}$)、NC マシンからの加工の完了信号により ($b1$)、マニプレータが作動し、作業者に対し直接原因作用が行われる ($a0$)。

Case 5: 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 ($f2^{**}$) 危険域に侵入する ($e1^{**}$)。このときセンサシステムがその検出に失敗し ($f1^*$)、NC マシンから、加工完了信号が送られ ($b1$)、マニプレータが作動し、作業者に対し直接原因作用が行われる ($a0$)。

4. 災害発生機構の Fault Tree

3章で図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、それぞれ図3のように Fault Tree 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、図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図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」(E_{b10}) 事象は、ワーク加工完了の「停止条件の解消」(E_{f22}) による動作信号 ($b1$)、インタロックによる自動停止機構の「不設置」(E_{e21}) 常起事象、および「停止のための操作を怠る: $f1^*$ 」($E_{a11,1}$) による「動力源の存在」(E_{a11}) 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: $a0$ 」(E_{a04}) は、「防護の不設置」(O_{a02}) 常起事象、「異常処理作業」(N_{c09}) のための「危険域に存在 $e1^{**}$ 」(E_{b12}) 事象、および「マニプレータの作動」(E_{b10}) 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」($E_{a11,2}$) のために「動力源が存在する」(E_{a11}) 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「検出ししない: $f1^*$ 」(E_{e18}) ことによるインタロック失敗論理、および手動停止機構の「不設置」($E_{a11,3}$) により動力源が常に存在する論理以外は、Case 1 と等価な論理となる。

Case 4 では、「停止のための操作を怠る: $f1^*$ 」($E'_{a11,1}$) ことによる「動力源の存在」(E'_{a11}) 論理以外は、Case 3 と等価な論理となる。

Case 5 では、「1 ブロックシーケンス運転完了以前」($E'_{a11,2}$) のために「動力源が存在する」(E'_{a11}) 論理以外は、Case 3 と等価な論理となる。

図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。

$$\text{Case 1: } C(x)_1 = \{E_{f22}, E_{a11,1}, E_{b12}\} \dots\dots (1)$$

$$\text{Case 2: } C(x)_2 = \{E_{f22}, E_{a11,2}, E_{b12}\} \dots\dots (2)$$

$$\text{Case 3: } C(x)_3 = \{E'_{f22}, E_{e18}, E'_{b12}\} \dots\dots (3)$$

$$\text{Case 4: } C(x)_4 = \{E'_{f22}, E'_{e18}, E'_{a11,1}, E'_{b12}\} \dots\dots (4)$$

$$\text{Case 5: } C(x)_5 = \{E'_{f22}, E'_{e18}, E'_{a11,2}, E'_{b12}\} \dots\dots (5)$$

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) 連続自動運転モードでは、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、図1に示された③→②→④→①→②→③の動作を平均 $a_1 \text{ h}^{-1}$ 行い、この動作持続時間は平均 $b_1 \text{ h}$ 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 $a_2 \text{ h}^{-1}$ 、また危険域内へとどまる時間の期待値は $b_2 \text{ h}$ 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、その故障モードは検出失敗側のみとする。また、センサ自体の自己診断機能や自己修復機能はなく、故障は非修復とし、その MTTF は $a_3 \text{ h}$ である。

条件(5) 侵入検出センサによる停止は、検出と同時にわれ、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(6) 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、操作してから侵入しようとする時間は無視できる。

条件(7) 作業者が事象 $E_{d11,1}$, $E_{d11,2}$, E_{e18} , $E'_{d11,1}$, または $E'_{d11,2}$ 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 $U_1 = \{\text{事象 } E_{d11,1} \text{ の条件下での事象 } N_{c09} \text{ の生起}\}$, $U_2 = \{\text{事象 } E_{d11,2} \text{ の条件下での } N_{c09} \text{ の生起}\}$, $U_4 = \{\text{事象 } E'_{d11,1} \text{ の条件下での } N'_{c09} \text{ の生起}\}$, および $U_5 = \{\text{事象 } E'_{d11,2} \text{ の条件下での } N'_{c09} \text{ の生起}\}$ として、次のように書き換えられる。

$$C(x)_1 = \{E_{f22}, U_1\} \dots\dots\dots (6)$$

$$C(x)_2 = \{E_{f22}, U_2\} \dots\dots\dots (7)$$

$$C(x)_3 = \{E'_{f22}, E_{e18}, N'_{c09}\} \dots\dots\dots (8)$$

(a) Cases 1 & 2*

* For System with Manual Cut Off Mechanism.

(b) Case 3**

** For System with Automatic Cut Off Mechanism.

(c) Cases 4 & 5***

*** For System with Manual and Automatic Cut Off Mechanisms.

図 3 作用連鎖の各 Case における災害発生論理の FT

$$C(x)_4 = \{E'_{f22}, E'_{e18}, U_4\} \dots\dots\dots (9)$$

$$C(x)_5 = \{E'_{f22}, E'_{e18}, U_5\} \dots\dots\dots (10)$$

これらのカットの生起には、前章の条件(5), (7)より

(i) 事象 E_{e18} , E'_{e18} がそれぞれ、事象 N_{c09} , U_4 , U_5 に先立って生起している

(ii) 事象 U_1 , U_2 , N_{c09} , U_4 , U_5 が、それぞれ事象 E_{f22} , E'_{f22} , E''_{f22} 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生起の正確な論理は、優先 AND ゲートを用いて、図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 E_{f22} , E'_{f22} , E''_{f22} の生起は、定数発生率 $a_1 b_1 / (b_1 - a_1) h^{-1}$ と修復率 $b_1 h^{-1}$ の指数分布でモデル化される。

仮定(2) 条件(2)より、事象 N_{c09} , N'_{c09} , N''_{c09} の生起は、定数発生率 $a_2 b_2 / (b_2 - a_2) h^{-1}$ と修復率 $b_2 h^{-1}$ の指数分布でモデル化される。

仮定(3) 条件(4)より、事象 E_{e18} , E'_{e18} の生起は、定数発生率 $a_3 h^{-1}$ と修復率 $b_3 = 0$ 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 カットの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 $q_1 a_2 b_2 / (b_2 - q_1 a_2) h^{-1}$ と修復率

$b_2 h^{-1}$ 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(11)において、

$$\lambda_1 = q_1 a_2 b_2 / (b_2 - q_1 a_2), \quad \mu_1 = b_2$$

$$\lambda_2 = a_1 b_1 / (b_1 - a_1), \quad \mu_2 = b_1$$

として与えられる。

Case 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 $(1 - q_1) q_2 a_2 b_2 / \{b_2 - (1 - q_1) q_2 a_2\} h^{-1}$ と修復率 $b_2 h^{-1}$ 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(11)において、

$$\lambda_1 = (1 - q_1) q_2 a_2 b_2 / \{b_2 - (1 - q_1) q_2 a_2\}, \quad \mu_1 = b_2$$

$$\lambda_2 = a_1 b_1 / (b_1 - a_1), \quad \mu_2 = b_1$$

として得られる。

Case 3: 同様に、このカットの $W_{3(0,t)}^*$ は、前報式(26)で、 $\mu_1 = 0$ として得られる式(12)において、

$$\lambda_1 = a_3$$

$$\lambda_2 = a_2 b_2 / (b_2 - a_2), \quad \mu_2 = b_2$$

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

として与えられる。

Case 4: 同様に、このカットの $W_{4(0,t)}^*$ は、式(12)において

$$\lambda_1 = a_3$$

$$\lambda_2 = q_1 a_2 b_2 / (b_2 - q_1 a_2), \quad \mu_2 = b_2$$

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

として得られる。

Case 5: 同様に、このカットの $W_{5(0,t)}^*$ は、式(12)において

$$\lambda_1 = a_3$$

図4 基本事象の生起順序を考慮した場合のカットの優先 AND ゲートによる表現

表1 各場合における頂上事象の10⁴hあたりの期待発生回数

CUT OFF MECHANISM	INSPECTION INTERVAL (HOURS)	EXPECTED NUMBERS OF OCCURRENCE OF TOP EVENTS PER 10 ⁴ HOURS			
		$Q_3 = 10^{-3} \text{ h}^{-1}$	$Q_3 = 10^{-4} \text{ h}^{-1}$	$Q_3 = 10^{-5} \text{ h}^{-1}$	$Q_3 = 10^{-6} \text{ h}^{-1}$
MANUAL		3.99×10^{-2}			
AUTO	50	1.64×10^{-1}	1.66×10^{-2}	1.67×10^{-3}	1.68×10^{-4}
	100	3.23×10^{-1}	3.32×10^{-2}	3.33×10^{-3}	3.34×10^{-4}
	200	6.25×10^{-1}	6.63×10^{-2}	6.67×10^{-3}	6.67×10^{-4}
	400	1.17	1.32×10^{-1}	1.33×10^{-2}	1.33×10^{-3}
	800	2.04	2.55×10^{-1}	2.61×10^{-2}	2.62×10^{-3}
MANUAL AND AUTO	50	9.81×10^{-4}	9.96×10^{-5}	9.97×10^{-6}	1.01×10^{-6}
	100	1.93×10^{-3}	1.99×10^{-4}	1.99×10^{-5}	2.00×10^{-6}
	200	3.74×10^{-3}	3.96×10^{-4}	3.99×10^{-5}	3.99×10^{-6}
	400	7.01×10^{-3}	7.87×10^{-4}	7.97×10^{-5}	7.98×10^{-6}
	800	1.22×10^{-2}	1.52×10^{-3}	1.56×10^{-4}	1.57×10^{-5}

$$\lambda_2 = (1 - q_1)q_2 a_2 b_2 / \{b_2 - (1 - q_1)q_2 a_2\}, \quad \mu_2 = b_2$$

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

として得られる.

$$W_{i(0,t)}^* = \left(\frac{\lambda_1}{\lambda_1 + \mu_1} \right) \left(\frac{\lambda_2}{\lambda_2 + \mu_2} \right) \left\{ \mu_2 t - \frac{\lambda_2 e^{-(\lambda_2 + \mu_2)t}}{\lambda_2 + \mu_2} + \frac{\mu_2 e^{-(\lambda_1 + \mu_1)t}}{\lambda_1 + \mu_1} + \frac{\lambda_2 e^{-(\lambda_1 + \mu_1 + \lambda_2 + \mu_2)t}}{\lambda_1 + \mu_1 + \lambda_2 + \mu_2} + \frac{\lambda_2}{\lambda_2 + \mu_2} - \frac{\mu_2}{\lambda_1 + \mu_1} - \frac{\lambda_2}{\lambda_1 + \mu_1 + \lambda_2 + \mu_2} \right\} \dots (11)$$

$$W_{j(0,t)}^* = \left(\frac{\lambda_2}{\lambda_2 + \mu_2} \right) \left(\frac{\lambda_3}{\lambda_3 + \mu_3} \right) \left[\left\{ t + \frac{\mu_2 e^{-\lambda_1 t}}{\lambda_1 (\mu_2 - \lambda_1)} + \frac{e^{-(\lambda_2 + \mu_2)t}}{\lambda_2 + \mu_2} - \left(\frac{\lambda_1}{\lambda_1 + \lambda_2} + \frac{\lambda_1}{\mu_2 - \lambda_1} \right) \frac{e^{-\mu_2 t}}{\mu_2} - \frac{\lambda_2 e^{-(\lambda_1 + \lambda_2 + \mu_2)t}}{(\lambda_1 + \lambda_2)(\lambda_1 + \lambda_2 + \mu_2)} \right\} \mu_3 + \left\{ -\frac{e^{-(\lambda_3 + \mu_3)t}}{\lambda_3 + \mu_3} + \frac{\mu_2 e^{-(\lambda_1 + \lambda_3 + \mu_3)t}}{(\mu_2 - \lambda_1)(\lambda_1 + \lambda_3 + \mu_3)} + \frac{e^{-(\lambda_2 + \mu_2 + \lambda_3 + \mu_3)t}}{(\lambda_2 + \mu_2 + \lambda_3 + \mu_3)} - \left(\frac{\lambda_1}{\lambda_1 + \lambda_2} + \frac{\lambda_1}{\mu_2 - \lambda_1} \right) \frac{e^{-(\mu_2 + \lambda_3 + \mu_3)t}}{\mu_2 + \lambda_3 + \mu_3} - \frac{\lambda_2 e^{-(\lambda_1 + \lambda_2 + \mu_2 + \lambda_3 + \mu_3)t}}{(\lambda_1 + \lambda_2)(\lambda_1 + \lambda_2 + \mu_2 + \lambda_3 + \mu_3)} \right\} \lambda_3 - \left\{ \frac{\mu_2 \mu_3}{\lambda_1 (\mu_2 - \lambda_1)} + \frac{\mu_3}{\lambda_2 + \mu_2} - \left(\frac{\lambda_1}{\lambda_1 + \lambda_2} + \frac{\lambda_1}{\mu_2 - \lambda_1} \right) \frac{\mu_3}{\mu_2} - \frac{\lambda_2 \mu_3}{(\lambda_1 + \lambda_2)(\lambda_1 + \lambda_2 + \mu_2)} \right\} - \left\{ \frac{-\lambda_3}{\lambda_3 + \mu_3} + \frac{\mu_2 \lambda_3}{(\mu_2 - \lambda_1)(\lambda_1 + \lambda_3 + \mu_3)} + \frac{\lambda_3}{\lambda_2 + \mu_2 + \lambda_3 + \mu_3} - \left(\frac{\lambda_1}{\lambda_1 + \lambda_2} + \frac{\lambda_1}{\mu_2 - \lambda_1} \right) \frac{\lambda_3}{\mu_2 + \lambda_3 + \mu_3} - \frac{\lambda_2 \lambda_3}{(\lambda_1 + \lambda_2)(\lambda_1 + \lambda_2 + \mu_2 + \lambda_3 + \mu_3)} \right\} \right] \dots (12)$$

(ただし, $i=1, 2$ $j=3, 4, 5$ $\lambda_1 \neq \mu_2$ 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 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} 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) = 3×10^{-3} (怠りによる人的過誤確率⁽¹⁰⁾). さらに4種類のセンサ; a_3^{-1} (センサのMTTF) = $10^3, 10^4, 10^5, 10^6 \text{ h}$

が利用できるものとし; センサの点検間隔を 50, 100, 200, 400, 800 h としたとき, 各場合における頂上事象の10⁴hあたりの期待発生回数が, 表1のように得られる. ただし, 点検によって, 故障したセンサは完全に新品と置き換えられるものとしている.

表1より, 自動停止機構では, 同じセンサでも点検間隔によって期待発生回数が大きく変わることがわかる. 点検間隔が2倍になると, 期待発生回数も約2倍となっている.

手動停止機構の系の期待発生回数を基準にとれば, 自動停止機構のみの系で, $a_3 = 10^{-3} \text{ h}^{-1}$ のセンサでは表1のいずれの点検間隔でもこれを満足せず, $a_3 =$

10^{-4} h^{-1} では点検間隔が100 h以下の場合で、他の二つのセンサでは表1のいずれの点検間隔でも満足する。 $a_3 = 10^{-6} \text{ h}^{-1}$ のようなセンサを用い、その保全状態も良好な自動停止機構を備えた系では、この停止機構のみでも、本報のような系での特定された潜在危険による異常モードに限定して言えば、基準よりもかなり安全性は上まわると言える。

しかしながら、現状では自動停止機構など、安全性に密接した関係を有する機器類の信頼性保証が義務づけられておらず、これが不明である場合も多い。また、基準の場合でも、本報のような系が 10^4 存在し、それらが 10^4 h の連続自動運転を行うと、本報で特定した潜在危険による望ましくない事象が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事が考えられる。したがって、手動停止機構の場合でも、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、手動と自動の二重の停止機構を備えることが望ましい。さらに、今後自動停止機構などの安全性に関連した機器の信頼性保証体制整備が重要な課題である。

9. ま と め

本報では、産業用ロボットを用いた作業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し、これによる災害発生機構を解析するとともに、頂上事象の期待発生回数を求めた。そして、手動および自動停止機構を用いた場合のロボットの人間に対する潜在危険抑制力を評価した。この手法は、広く適用が可能である。

本報では、センサの故障モードを欠報(非検出側)のみとしているが、実際に誤報モードをもつ場合も多い。誤報による修理活動によって、センサが更新される場合には、この影響も考慮しなければならない。しかし、誤報による修理の発生確率が、点検による修理の発生確率に比し十分小さいとき、この影響を無視してもよいであろう。

センサの故障を非修理系としているが、修理系の場合には式(12)のかわりに前報の式(26)を用いればよい。

センサの故障確率が、一作動要求あたりの不作動確

率で与えられる場合には、式(12)のかわりに式(11)を用いることができる。

本報では、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(11)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続く場合には、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断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。また、頂上事象やニアミス事象の生起によって、センサなどが更新されるのが普通で、点検間隔内での頂上事象の期待発生回数が1に近づくに従い、仮定(4)とのギャップの影響が増大し、本アルゴリズムはそのままでは適用困難となることに注意する必要がある。

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。

文 献

- (1) 現時点における産業用ロボットの定義および災害事例については、例えば、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、機誌、87-792, (昭59)、1245。
- (3) 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。
- (4) 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。
- (5) 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。
- (6) 文献(4)の829ページ。
- (7) 文献(3)の2192ページ。
- (8) 文献(3)の2189ページ。
- (9) 文献(4)の826ページ。
- (10) Henley, E. J. and Kumamoto, H., *Reliability Engineering and Risk Assessment*, (1981), 286, Prentice-Hall, Englewood Cliffs, New Jersey.

討 論

〔質問〕 中村 林二郎〔千代田工商(株)〕

地味な研究を一步一步着実に実施されていることに敬意を表す。

(1) 安全性は(A-危険性)であり、危険性は(被害の大きさ)×(頻度)の積算値であるから、頻度と被害の大きさ両面を考える必要がある。第4報の具体例で言うなら、ロボット自体および運搬物を含めた系の故障率または運搬品の寸法管理程度などが頻度を大きく支配し、ロボットの腕の柔らかさ、異物接触検知-停止システムなどにより、人の被害の大きさ(傷の程度)が変わる。

それらにより危険性を許容限度内に収めることが可能となる。これらの論文を法規制に利用するときには「法は一律とならざるを得ない」ので一方で過剰規制、他方で不安全なものとなる恐れがあるので注意を要する。

(2) 入口ドアとロボット動作停止-電源切断とをインタロックするほうが、ヒューマンエラーの影響を少なくし得るのではないか。

〔回答〕 (1) 安全とはリスクが小さい状態のことである。リスクは単位時間あたりの期待損失であり、(被害の大きさ)×(被害の発生頻度)と定義される。被害の大きさは、エネルギーや作用物などの作用や変化の大きさ、性質、伝わり方、受けとる側の状態に支配される。発現し得る作用や変化を被害が生じない程度の大きさと性質に限定設計することができれば、系は本質安全化される。系が本質安全化されない場合は、発生頻度が問題となり、これを抑制することが技術上の目標となる。第1報では、被害発生の必要条件となる作用が発現し得る潜在力を潜在危険として定義している。第2報では、作用の発現機構を論理モデル化し、作用の大きさ、性質、および作用を緩衝する防護の不適切を条件に災害が発生するとしている。ただし、作用とその被害の大きさとの関係についてはまだ立ち入っていない。本報では、本文で述べたような具体的な系を設定し、特定の潜在危険について、その発現力と抑制手段の抑制力とを評価している。ここでは、系の異常モードを、系の自動運転下で作業者が異常処理作業を行うことにより生ずる潜在危険に的をしぼっている。したがって、系としての完成された評価を得るためには、系のライフサイクル全般にわたったすべての異常モードについての評価をさらに行う必要がある。また本報のような系では、ロボット自体や運搬物を含

めた系の異常発生率が異常処理作業の発生頻度 a_2 を、ワークの重量などの影響が作業者の危険域にとどまる時間 b_2^{-1} を支配することとなる。

(2) 本報では、センサの故障モードを欠報のみとしているが、誤報がある場合でも、誤報による修理の発生確率が点検によるそれに比し小さいときはその影響を無視できる。センサについては、その回路上の構造をいわゆる fail safe (誤報側と欠報側の故障率の比を欠報側に小さい非対称なものとする) 化することにより、例えば本報で例示した $a_3=10^{-6} \text{ h}^{-1}$ よりもさらに小さな欠報側故障発生率を得ることもできよう。その場合には、欠報による異状モードよりも、論理モデルから、例えば「誤報による修理活動の生起」(N_{c10} : この場合は自動運転モードではなくなる)、「インタロックを人為的に無効とする」(E_{c20}) などの事象による潜在危険や他の異常モードによる潜在危険が相対的に重要となってくることが予想される。

〔質問〕 稲垣 敏之〔筑波大学電子・情報工学系〕

実際の状況設定と理論的厳密性を兼備した貴論文の成果の意義は大きい。今後も継続発展が望まれる。

(1) 6章1行め、事象 $U_1=\{E_{a11,1} \text{ の条件下での } N_{c09} \text{ の生起}\}$ なる定義は二とおりに解釈できる。条件つき事象としての解釈 $U_1=\{E_{a11,1}|N_{c09}\}$ と、同時事象としての解釈 $U_1=\{N_{c09} \text{ かつ } E_{a11,1}\}$ である。貴論文の意図は後者にあると思われるが、いかがか。

(2) 式(3)と(8)では、 E_{b12} と N'_{c09} は同義語か。

(3) 7・2節 Case 1 における事象 U_1 の発生率は、単純に考えれば $q_1 a_2 b_2 / (b_2 - a_2)$ かと思われた。貴論文での事象 U_1 の発生率導出の考え方をご教示願いたい。

(4) センサを定期点検すると、センサ信頼度関数はこの歯波形を描く。式(12)はセンサ信頼度が時間に関する単調減少関数となる場合に成立する式である。表1の結果を得るためにどのような処置をとられたか。

(5) 9章右欄8行め、「非定常状態の影響」は「運転開始(再開)時の初期状態の影響」という意味か。

〔回答〕 (1) ご指摘のとおりである。より正確な表現を期するために、 $U_1=\{E_{a11,1} \text{ の生起かつその条件下で } N_{c09} \text{ の生起}\}$ としたほうがよい。

(2) 本報では、系の異常モードとして、 E_{b12} が N'_{c09} によって生ずる場合を特定している。したがって、式(3)と(8)のカットセット表記上は同義である。し

かし厳密に言うと、式(8)のカットセットには基本事象の発生順序の条件が加味されていると考えていただきたい。これは、本文図4で示されている。すなわち、 E_{e18} の発生の後でしかも E_{f22} の発生の前で発生した N_{c09} のみが E_{b12} となる。

(3) N_{c09} すなわち E_{b12} を生起させようとする異常処理作業の単位時間あたりの期待発生回数を、十分時間の経過した定常状態で a_2 とし、 E_{b12} が生起しようとする条件下で停止操作を怠る確率を q_1 としている。事象 $U_1 = \{E_{b12} \cap E_{d11,1}\}$ であり、 U_1 の定常状態での単位時間あたりの期待発生回数を $w_1(\infty)$ とすれば、文献(5)113ページ、式(7)より、

$$Pr\{(t, t+dt] \text{ で } U_1 \text{ が発生}\} = w_1(\infty)dt \quad \dots (i)$$

また、

$$Pr\{(t, t+dt] \text{ で } U_1 \text{ が発生}\} = Pr\{(t, t+dt] \text{ で } E_{b12} \text{ が発生} \cap E_{d11,1}\} = (a_2 dt)(q_1) \quad \dots (ii)$$

でもあるので、式(i)および(ii)から

$$w_1(\infty) = q_1 a_2 \quad \dots (iii)$$

を得る。一方、基本事象は相互に独立としているので、このときの作業者が危険域にとどまる期待時間は変化がなく b_2^{-1} である。したがって、 $w_1(\infty) = [MTTF + MTTR]^{-1} = \lambda_1 \mu_1 / (\lambda_1 + \mu_1)$ から、定数発生率 $\lambda_1 = q_1 a_2 b_2 / (b_2 - q_1 a_2)$ と修復率 $\mu_1 = b_2$ を得る。

(4) センサの点検間隔を $T_1=50, T_2=100, \dots, T_5=800$ h とすると、各点検間隔内では連続自動運転として、 10^4 hあたりの頂上事象の期待発生回数 EN_i を

$$EN_i = (10^4 / T_i) \cdot W_i^*(0, T_i), \quad i=1, 2, \dots, 5$$

として求めている。

(5) ご指摘のとおりである。系の自動運転での k 番めの中断($k=0$ で開始)が終了し運転が再開される時、その持続時間を $T_k (>1 \text{ h})$ とすれば、延べ 10^4 hあたりの頂上事象の期待発生回数 $EN = \sum_{k=0}^n W_i^*(0, T_k)$ が $EN = W_i^*(0, T)$ として得られることを意味している。ただし、 $\sum_{k=0}^n T_i = T$ とする。