Specific Research Reports of the National Institute
of Industrial Safety, NIIS-SRR-NO.24 (2002)
UDC 331.461:62-192:62-531:62-781:65.011.56

2. プログラマブルな電子制御装置を利用した安全制御システムの最適設計法に関する基礎的考察*

梅崎重夫**, 池田博康**, 斉藤　剛**, 杉本　旭***

2. The Basic Consideration on the Optimum Design Method of the Safety Control System Using Programmable Electronic Equipment*

by Shigeo UMEZAKI**, Hiroyasu IKEDA**,
Tsuyoshi SAITO** and Noboru SUGIMOTO***

Abstract: In the safety system using programmable electronic equipment, labor accidents may arise due to program bugs, troubles of electronic equipment, electro-magnetic noise effects, etc.. Therefore, countermeasures such as dualization of CPUs and installation of the self checking mechanism have recently been proposed in the industrial field. However, the safety of such control systems greatly depends on independence, redundancy, existence of the self checking mechnism and check intervals for elements of the safety system. The accident occurence rate was quantitavely examined according to the degree of redundancy and diversity, and the intervals of self checking for the programmable safety system. The allowable accident occurrence rate was assumed under 10^{-11}/hour.

Following results were obtained in this study:

(1) The allowable accident occurrence rate could not be achieved when the self checking mechanism for the sensor and the signal processing unit of programmable safety system had not been established, even if they had redundant and diverse CPUs. The self-checking mechanism was indispensable to the programmable safety system.

(2) The allowable accident occurrence rate could be achieved if the sensor and signal processing unit had triple redundant and diverse CPUs with the self checking mechanism. However, it was necessary that the self checking interval was about half an hour or less, and the non-reliability of these safety elements were less than 10^{-3}/hour to achieve the allowable accident occurrence rate.

(3) It was necessary to shorten the self checking interval within one minute when the safety system was composed by dual redundant and diverse sensors and signal processing units. However, the check interval of the memory within one minute might be difficult.

(4) The allowable accident occurrence rate could not be achieved when the non-reliability of programmable safety system was less than assumed value. As a result, the improvement of the reliability was indispensable to the realization of the high level safety system.

Keywords; Safety control, Programmable electronic equipment, Redundancy, Diversity, Self checking

---

* 本研究の一部は，日本機械学会第 18 回システムシンポジウム（平成 12 年 7 月 4 日）及び日本信頼性学会誌（平成 13 年 11 月号）に発表した。

** 機械システム安全研究グループ Mechanical and System Safety Research Group
*** 北九州市立大学　国際環境工学部　環境機械システム工学科 The University of Kita-kyuushu, Faculty of International Environmental Engineering, Dept. of Mechanical Systems and Environmental Engineering

1. はじめに

最近の機械設備では，プログラムを変更するだけで多様な作業に対応できる汎用機としての性能を備えているものも多い。このような機械では，プログラムを適切に組むことによって，機械の運用効率を向上させることも可能である。

また，安全の条件についても作業が変更になる毎にプログラムを随時変更しながらインタロックを組めれば，機械の運用上都合が良い。このような事情から，最近では，プログラマブル・ロジック・コントローラ (programmable logic controller，以下「PLC」と略す) などを利用した電子制御装置が，安全の制御にも広く利用されるようになってきた。

この装置では，プログラムに含まれるバグ（誤り），電子制御装置の故障，電磁ノイズの影響などによって，機械が止まらなくなったり，停止中の機械が突然不意作動を起こす場合がある。このため，最近では，電子制御装置の多重化や自動監視（セルフチェック）機構の設置によって，このような問題に対処する安全制御システムが提案されるようになってきた。しかし，現状では，このような制御システムの安全性は，システムを構成する要素間の独立性と冗長度，自動監視機構の有無とチェック間隔等に大きく依存するため，適切な設計を行わないと所要の安全性が得られない。

そこで，本報では，プログラマブルな電子制御装置に異種冗長化技術と自動監視技術を適用した安全確認システム（補足 1 参照）を対象に，異種冗長化の程度と自動監視機構のチェック間隔などがいかなる条件であれば，第 2.1 節に示した災害防止に関する目標値が満足できるかを定量的に検討した[1),2)]。

この検討過程では，蓬原・向殿・杉本・粂川らによって提案された安全の原理[3)]（安全か危険か分からない不確定なものは，すべて危険と見なす。補足 2 参照）が理論的基礎となっている。また，この検討過程で，機械設備の安全方策のあり方についても基礎的な考察を試みたので，参考として第 2.2 節に併記する。

2. 残存リスクの最小化を目的とした安全方策

2.1 災害防止に関する目標値

安全規格を作成する際の国際的なガイドラインである ISO/IEC ガイド 51 では，安全を「受け入れ不可能なリスクがないこと」(freedom from unacceptable risk) と定義している[4)]。

この定義に関しては許容可能なリスク (tolerable risk)[4)] との関係から様々な解釈が考えられている

Table 1　Rate of incident assumed in this study.
本研究で想定する災害発生率

被災の程度		災害防止に関する目標値	効果の推定
死亡または永久障害		10^{-11}回/h 以下	根絶
回復可能	重症	10^{-9}回/h 以下	従来の 1%以下
	軽症	10^{-7}回/h 以下	従来の 10%以下
	赤チン災害	除外	設定せず

が[5),6)]，少なくとも受け入れ不可能なリスク（この中には死亡災害や永久障害を残す災害のように，災害の発生自体が受け入れられないものを含む）に対しては，機械の設計・製造の段階で行う安全確認によって，無視可能なレベル[6)]まで低減する必要があると筆者らは考えている。

そこで，本報では，このレベルに対応する災害防止に関する目標値として，**Table 1** に示すように 10^{-11} 回/h 以下の災害発生率を設定した。

これは，我が国の 4000 万労働者が 1 年間（約 2000 時間）働いたときの災害発生件数の推定値を 1 件未満（この場合は 0.8 件）とする水準である。

また，国際規格である IEC61508[7)]では，安全性インテグリティレベルが 4 のシステムに対して危険側障害発生率を 10^{-9}～10^{-8}回/h とすることを要求しているが，この数値にハインリッヒの法則（補足 3 参照）に基づく回避失敗率（3.2 節参照。たとえば 1/300）を掛けて災害発生率を推定すると，概ね **Table 1** の水準になると考えられる。

ただし，**Table 1** では回復可能な災害（永久障害を残さない災害）に対しては現段階での災害発生状況を考慮し，現実的な目標値を参考値として示している。また，いわゆる赤チン災害は災害防止の対象から除外した。

2.2 これまでに実施されてきた対策

1) 確定的な安全方策

上記の目標値を達成する対策としてまず最初に考えられるのが，リスクゼロを目標とした確定的な安全方策の実施である。具体的には，安全確認システムを構成する要素に非対称誤り特性を持たせることによって，故障時に危険側の動作を機械に行わせない安全確認形インタロック（補足 1 参照）の適用が考えられる。

ここで，非対称誤り特性とは「あらかじめ定められ

た特定の故障状態しか生じない特性」と定義される。この特性は，システムを構成するすべての要素で発生する故障を一つずつ特定し，それぞれの故障が安全側(機械が停止する側）となるように設計されて，初めて実現できる。言いかえれば，この特性の実現にあたっては，安全確認システムの内部構造にまで及んだ徹底した検討が必要になる。以後，本報では，この特性を「構造的な非対称誤り特性」と呼ぶ。

2) 非確定的なリスク低減策

現実には，すべての場合に確定的な安全方策が実施できるわけではない。このため，実際の現場では，この方策に代わるものとして非確定的なリスク低減策も試みられてきた。

この典型例に，人間の誤りや機械の故障を減少させたり，安全確認システムの信頼性を向上させるなどの対策がある。しかし，本研究で定めた災害防止に関する目標値が少なくとも 10^{-11}回/h 以下であるのに対して，現実の人間側の誤り発生率は 10^{-1}～10^{-2}回/h，機械側の故障発生率は 10^{-3}～10^{-4}回/h 程度の場合もある(これについては，日本原子力研究所の機器故障率データベースや，A.D. Swain によるヒューマンエラーの評価 NUREG/CR-1278 などが参考になる)。したがって，単に人間の誤りや機械の故障を減少させたり，安全確認システムの信頼性を向上させただけでは，目標値の達成はほとんど不可能と言わざるを得ない。

ところで，伝統的な信頼性理論の体系では，上述のように人間や機械の信頼性を確率統計的に評価する分野のほかに，故障の原因を物性論的に解明しようとする分野が存在する。そして，前者が故障の発生率を問題とするのに対し，後者は故障が発生したときの故障に至るメカニズムや故障発生後の挙動（たとえば，安全側か危険側か）を問題にする。

この後者に関連する対策が非対称誤り特性の改善である。ただし，ここで言う非対称誤り特性とは本節の 1) で述べた構造的な特性とは異なる機能的な特性を意味する。具体的には，安全確認システムを構成するいずれかの要素が対称誤り特性を持つ場合でも，セルフチェック等の応用によってシステム全体としては機能的に非対称誤り特性を実現する方法をいう。この特性の具体的な実現方法は第 4 章で詳述する。以後，これを「機能的な非対称誤り特性」と呼ぶ。

機能的な非対称誤り特性の改善による効果は，非対称誤り率（発生するすべての故障のうち，危険側となる故障の比）で評価される。ただし，この指標による評価では，確率計算に特有の不確定性が含まれるため，既に述べた「安全の原理」に従って不確定性を根絶する必要がある。この具体的方法は第 2.4 節で詳述する。

2.3 従来の災害防止対策の問題点

以上の議論は，産業機械を対象とした災害防止対策に，以下の 5 種類があることを意味する。

① 確定的な安全方策
② 人間の誤りを減少させる対策
③ 機械の信頼性を向上させる対策
④ 安全確認システムの信頼性を向上させる対策
⑤ 安全確認システムの非対称誤り特性を機能的に改善させる対策

従来，我が国では，これらの対策が混然一体となって実施されてきた。そして，これらの対策の併用によって「結果的に労働災害が減少できれば良い」とされてきたのである。しかし，筆者らは，このような対策は少なくとも次の点で問題があると考える（**Fig. 1** 参照)。

1) 安全性の立証によるリスク排除の必要性

一般に，機械の安全性は安全方策の採用によってリスクを低減した後の残存リスクによって評価される。この場合，少なくとも残存リスク以外のリスク要因は，既に安全性が確認されていることの立証を必要とする。

しかし，従来の対策では，確定的な安全方策によって安全性の立証が可能である部分と，非確定的な対策によってリスクを低減せざるを得ない部分が混然一体となっているために，安全性の立証が可能な部分まで結果的には確率的なリスク評価に委ねざるを得ない（**Fig. 1(a)** 参照)。これでは，対策が完了したといっても安全性の立証が伴わないため，災害が発生しないという保証は得られない。

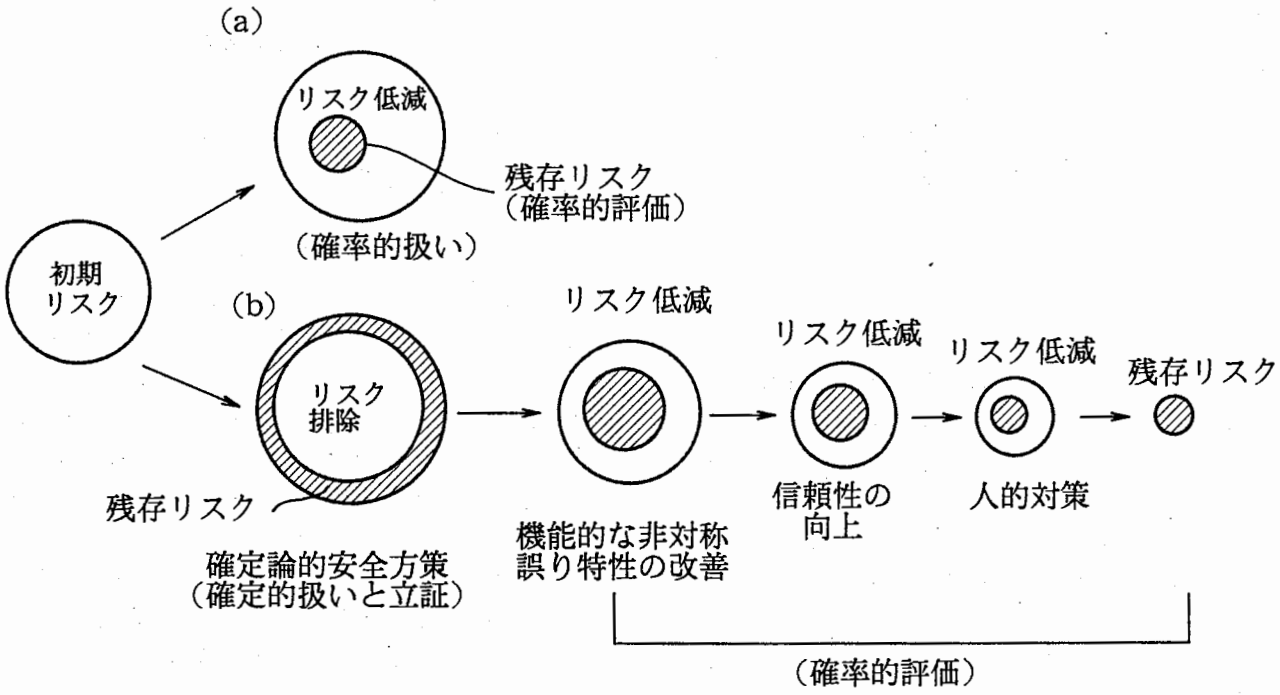
2) 確率的なリスク評価に含まれる不確定性の考慮

非確定的なリスク低減策では，確率的なリスク評価によってリスクを定量的に推定し，この値が所定の範囲内にあるときに「安全」と判断する。しかし，現実には災害発生率の推定値が 10^{-11}回/h 以下と判断されても，確率的なリスク評価に含まれる不確定性の方がこの数値と比較して桁違いに大きい場合もある。

したがって，非確定的なリスク低減策によって残存リスクの最小化を図るなら，まず残存リスクの推定値よりも残存リスクの確率的評価に含まれる不確定性を最小化する方が重要と考えられる。

2.4 筆者らが提案する評価手法と安全方策

Fig. 1(b) は，2.3 節で述べた問題点を考慮した上で筆者らが提案する災害防止対策である。この対策では，まず最初に確定的な安全方策の実施によってリスクの相当部分を排除した後に，なお残る残存リスクに対して非確定的なリスク低減策を実施する。



注) 斜線部分は，残存リスクを表す

Fig. 1　Safety measures proposed in this study.
本研究で提案する安全方策

ここで問題となるのが，非確定的なリスク低減策に含まれる不確定性である。そこで，本報では，この不確定性を排除するために，既に述べた安全の原理に従って「不確定を危険と見なす」処置を行い，次の対策を提案する。

1)　非対称誤り率に含まれる不確定性の排除

安全確認システムをプログラマブルな電子制御装置などの対称誤り特性を持つ素子で構成した場合，故障によって危険側となるか，安全側となるか予め予想がつかない。そこで，本報では安全側か危険側か予想できない不確定な故障は，安全の原理にしたがってすべて危険側とみなすことにする。

具体的には，安全確認システムの非対称誤り率η（回/回）に最悪値評価として$\eta = 1$を与えて，非対称誤り率の確率的評価に含まれる不確定性を排除する。ただし，非対称誤り率とは「発生するすべての故障に対する危険側となる故障の比」をいう。

2)　人間や機械の不信頼度に含まれる不確定性の最小化

後述の算定では，安全確認システムの故障発生率λ（回/h）には，想定できる最悪値の代表例として$\lambda = 10^{-3}$回/hを与えて確率的評価に含まれる不確定性を少なくする。

同様に，後述の算定では，機械の故障発生率α（回/h）に想定できる最悪値の代表例（補足4参照）として$\alpha = 10^{-3}$回/hを，人間の誤り発生率β（回/h）には$\beta = 10^{-1}$回/hを与える。

ただし，1) では不確定性が排除できるのに対し，2) では不確定性が排除できるわけではないから，2) によるリスク低減効果はあくまでも補助的なものと考えるべきである。

以上より，産業機械を対象とした安全方策は，次の優先順位に基づく包括的対策となる（補足5参照）。

①　確定的な安全方策（安全確認形インタロックの適用など）の実施によるリスクの排除と安全性の立証

②　安全確認システムの機能的な非対称誤り特性の改善（異種冗長化や自動監視等の応用）

③　人間や機械の不信頼度の改善（機械及び安全確認システムに対する高信頼化技術の適用，作業者の人的ミスを減少させる伝統的な労働安全手法の適用）

④　上記②及び③に対する確率的なリスク評価と残存リスクの確定

以上のような過程を経て，最終的に残存リスクが最小化できたという保証が得られ，対策が完了する。この過程で最終的に確定的対策と非確定的対策は融合され，包括的な安全方策が確立できる。

具体的には，①に対しては安全確認形インタロックを始めとする確定的な安全技術の適用が可能である。また，③及び④に対しては既存の信頼性技術や伝統的

な労働安全手法が適用可能である。これに対し，②を実現するための具体的対策は既に述べた「安全の原理」に従う必要があるため，新たな検討が必要である。これについては第3章で重点的に検討する。

3. 安全確認システムのリスク低減効果

3.1 システムの構成と状態遷移図

Fig. 2 に，安全確認システムの基本構成図を示す。ここで，$I(t)$ は運転命令ありのときを論理値1，運転命令なしのときを論理値0とする2値論理変数である。同様に，$A(t)$ は作業者が危険領域内に進入していないときを論理値1，進入しているときを論理値0，$W(t)$ は運転許可のときを論理値1，運転禁止のときを論理値0とする2値論理変数である。

また，Sは作業者が危険領域内に進入していないことを確認するセンサーであり，G は運転命令 $I(t)$ とセンサーからの許可信号 $A(t)$ の両方が論理値1であるときに機械の運転許可信号 $W(t)$ を発生する論理積演算要素（インタロック）である。

ここで，安全確認システムの故障発生率をλ（回/h），非対称誤り率をη（回/回）とすると，安全確認システムの状態遷移図は **Fig. 3** のようになる。

Fig. 3 で，$p_0(t)$ は時刻 t において安全確認システムが正常状態にある確率を意味する。これに対し，$p_K(t)$ と $p_S(t)$ は時刻 t において安全確認システムが故障状態にある確率を意味する。このうち，$p_K(t)$ は危険側故障の状態に対応し，$p_S(t)$ は安全側故障の状態に対応する。

ただし，正常状態とは，作業者が危険領域内に進入したときは直ちに機械を停止できる能力を安全確認システムが有している状態である。また，危険側故障の状態とは，作業者が危険領域内に進入したにもかかわらず，安全確認システムの故障によって機械を停止できなくなった状態である。さらに，安全側故障の状態とは，作業者が危険領域内に進入していないにもかかわらず，安全確認システムの故障によって $W(t)$ が論理値0となり，その結果，機械が停止した状態である。

Fig. 3 では，安全確認システムに危険側故障が発生したときは非修復系を構成し，安全側故障が発生したときは修復率μ（回/h）の修復系を構成するものと仮定している。これは，安全側故障の発生時には必ず機械が停止するために故障が検出可能であるのに対し，危険側故障の発生時には通常は機械が停止しないために検出が困難であることによる。

以上の関係は次式で表すことができる。

$$p_0(t+dt) = (1-\lambda\, dt)p_0(t) + \mu p_S(t)dt \qquad (1)$$

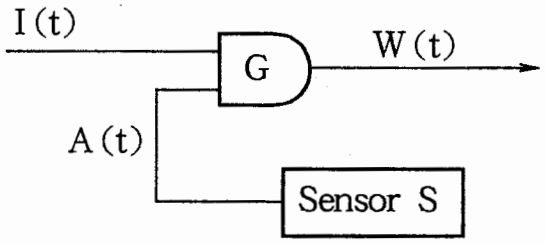


Fig. 2　Safety confirmation system.
安全確認システム

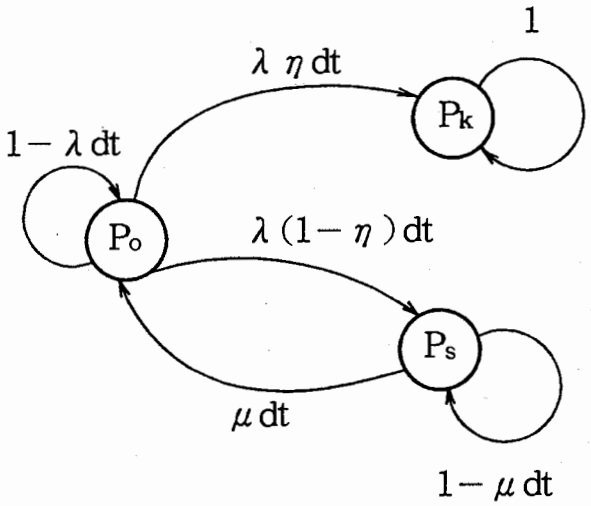


Fig. 3　State transition of safety confirmation system.
安全確認システムの状態遷移図

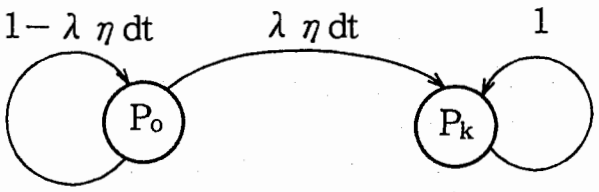


Fig. 4　Simplified state transition.
簡略化された状態遷移図

$$p_K(t+dt) = p_K(t) + \lambda\eta p_0(t)dt \qquad (2)$$

$$p_S(t+dt) = (1-\mu dt)\, p_S(t) + \lambda(1-\eta)p_0(t)dt \qquad (3)$$

ただし，$p_0(t)+p_K(t)+p_S(t) = 1$, $p_0(0) = 1$, $p_K(0) = 0$, $p_S(0) = 0$ とし，機械の停止時には迅速に修復が行われると仮定して **Fig. 3** を解くことにする。言い換えれば，安全側故障はすべて修復されるものと仮定する。

Fig. 4 は，このときの状態遷移図である。ここで，機械の迅速な修復が行われるための条件が$\mu dt = 1$ となることを考慮すれば，(1)～(3) 式は次式となる。

$$p_0(t+dt) = (1-\lambda\eta\, dt)p_0(t) \qquad (4)$$

$$p_K(t+dt) = p_K(t) + \lambda\eta\, p_0(t)dt \qquad (5)$$

ただし，$p_0(t)+p_K(t)=1$, $p_0(0)=1$, $p_K(0)=0$ とする。

これより，$p_0(t)$ 及び $p_K(t)$ は次式となる。

$$p_0(t)=\exp(-\lambda\cdot\eta\cdot t) \tag{6}$$

$$p_K(t)=1-\exp(-\lambda\cdot\eta\cdot t) \tag{7}$$

3.2 災害発生率の定量化

Fig. 2 の安全確認システムでは，

① 作業者が誤って危険領域内に進入し，かつ，

② そのときまでに安全確認システムが危険側故障を起こしていた場合に，

機械が停止できなくなって危険状態が発生する。

ここで，作業者が誤って危険領域内に進入する率をβ（回/h）とすると，安全確認システムが時刻 t までに危険側故障を起こしている確率は $p_K(t)$ で表されるから，時刻 t における危険状態の発生率 $r_K(t)$（回/h）は，①に関する指標βと②に関する指標 $p_K(t)$ の積となり，次のように表現できる。

$$\begin{aligned} r_K(t)&=\beta\cdot p_K(t)\\ &=\beta[1-\exp(-\lambda\cdot\eta\cdot t)] \end{aligned} \tag{8}$$

実際の安全確認システムでは，次の場合に危険状態が発生する。

(a) 作業者が危険領域内に進入したにもかかわらず，センサー Sが既に故障していたために作業者を検出できず，機械が停止しなかった場合

(b) 作業者が危険領域内に進入したにもかかわらず，論理積演算要素 G が既に故障していたために誤って運転許可信号 W(t) が論理値 1 となって，機械が停止しなかった場合

ここで，センサー Sの故障発生率をλ_S（回/h），非対称誤り率をη_S（回/回），論理積演算要素（インタロック）G の故障発生率をλ_G（回/h），非対称誤り率をη_G（回/回）とすると，センサー Sと論理積演算要素 G が時刻 t までに危険側故障を起こしている確率は (7) 式を利用して計算できるから，時刻 t での危険状態の発生率 $r_K(t)$（回/h）は次式となる。

$$\begin{aligned} r_K(t)&=\beta[1-\exp(-\lambda_S\cdot\eta_S\cdot t)]\\ &\quad+\beta[1-\exp(-\lambda_G\cdot\eta_G\cdot t)] \end{aligned} \tag{9}$$

実際の安全確認システムでは，仮に危険状態となったときでも，常に災害が発生するとは限らない。なぜなら，このようなときに作業者は危険状態に対して回避行動をとることで，災害から逃れる可能性があるからである。

そこで，本報では，前述した①，②とともに，③の作業者が災害を回避できる可能性（回避可能性）も考慮して，時刻 t における災害発生率を下式のように定めた。ここで，③に関する指標として回避失敗率 H_L（回/回）を導入すると，災害発生率 $r_H(t)$（回/h）は次式となる。

$$\begin{aligned} r_H(t)&=H_L\cdot r_K(t)\\ &=\beta H_L[1-\exp(-\lambda_S\cdot\eta_S\cdot t)]\\ &\quad+\beta H_L[1-\exp(-\lambda_G\cdot\eta_G\cdot t)] \end{aligned} \tag{10}$$

ただし，H_Lはシステムが危険状態となったときに，作業者が回避に失敗して実際に災害となる率であり，既に述べたハインリッヒの法則と呼ばれる偶然的要素に依存する。

3.3 冗長化とセルフチェックの必要性

(10) 式は，

① 安全確認システムで発生する故障やトラブルを減少させる高信頼化技術 (λ_Sやλ_Gの減少)

② 安全確認システムの非対称誤り特性を機能的に改善する安全性技術 (η_Sやη_Gの改善)

③ 及び作業者に対する教育・訓練によって人的ミスを減少させる伝統的な労働安全手法 (βや H_Lの減少) の併用

によって，災害防止に関する目標値を達成できる可能性を示している。

しかし，現実には，災害発生率の確率的評価に含まれる不確定性のために，目標値を達成したことの確認が困難な場合も生じる（たとえば，人間の不信頼度を訓練によって 10^{-11}回/h 以下にまで減少させたといっても，この数値自体が確定性に乏しいために，目標値を達成したことの確認は困難である)。そこで，本報では,「不確定を危険と見なす」安全の原理にしたがって上記のパラメータに対する最悪値評価を行い，この不確定性の最小化を図る。

Fig. 5 は，この考え方にしたがって，上記のパラメータに対して最悪値評価を実施したときの災害発生率 $r_H(t)$ を推定したものである。ここでは，最悪値として$\eta_S=1$, $\eta_G=1$, $\lambda_S=10^{-3}$回/h, $\lambda_G=10^{-3}$回/h, $\beta=10^{-1}$回/h, $H_L=1$ と仮定した。

この検討結果より，災害防止に関する目標値の実現には，次の 1), 2) で示す問題点に対する対処が必要であることが判明した。

1) 初期段階でのリスク低減効果の不足

このシステムでは，仮に上記①～③のリスク低減策の併用を図ったとしても，安全確認システムが **Fig. 2**

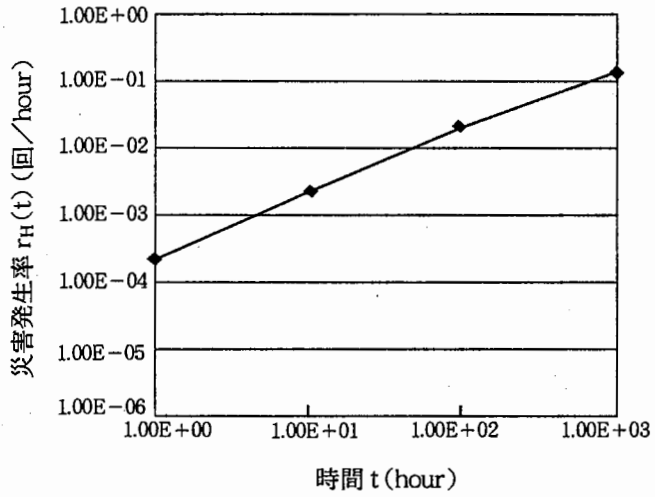


Fig. 5 Estimated rate of incident by single channnel safety confirmation system.
単一系の安全確認システムによる災害発生率の推定値

のような単一系である限りは，災害防止に関する目標値は達成できない。

そこで，安全確認システムの多重化を図ることによって，システムを運用する初期の段階で所定の確率までリスクの低減を図る。

2) 長期的運用時のリスク低減効果の維持

機械の長期的な運用にあたっては，予期しない故障によって災害が起きるおそれがある。このため，確定的な安全方策では，常時，安全確認を行うことによって，故障を瞬時に検出して機械を停止させる構成としている。

これに対し，非確定的なリスク低減策の中には，機械を運用する初期の段階で所定の確率までリスクの低減を図れたとしても，長期的な運用に対してまで初期のリスク低減効果を維持できないものがある。そこで，本報では，セルフチェックの応用によって安全確認システムに故障が発生していないことを定期的かつ自動的に監視するシステムを構成することにした。これにより，システムが長期にわたって運用された場合でも，所定のリスク低減効果を維持できるようにしている。

4. 非対称誤り特性の機能的改善によるリスク低減効果

4.1 機能的改善のための手法

前章の 1) に対する対策としてまず最初に考えられるのが，同種の安全確認システムの多重化である。しかし，単なる同種の多重化は，共通原因故障[7]（一つの事象を原因として，多重化された要素に同時に故障を起こすもの）の発生が懸念される。そこで，本報では，独立した異種のシステムの冗長化（以後，これを「異種冗長化」と呼ぶ）によって，共通原因故障を可能な限り少なくするようにした。ただし，完全な独立性の実現は容易でないので，ここでは完全独立の可能性を仮定して議論を進める。

また，異種冗長化では冗長化されたシステムの信頼性は改善されるが，故障でいつ危険な状態になるか分からないという問題は残る。そこで，本報では，異種冗長化された安全確認システムに故障が発生していないことを定期的かつ自動的にチェックする機構（以後，これを「自動監視機構」と呼ぶ）を適用し，故障を検出した場合には機械の運転を自動的に停止させることを仮定した。これにより，故障を解消しない限り機械が再起動できないため，機能的な方法によって非対称誤り特性の改善を図れる。

以下，安全確認システムの異種冗長化と自動監視機構の応用によって，既に述べた **Table 1** に示す目標値が達成できるかを定量的に検討する。

4.2 異種冗長化によるリスク低減効果

Fig. 6 に，異種冗長化された安全確認システムの基本構成を示す。ここでは，作業者が危険領域内に進入していないことを確認するセンサーを $S_N(N=1,2,3)$,

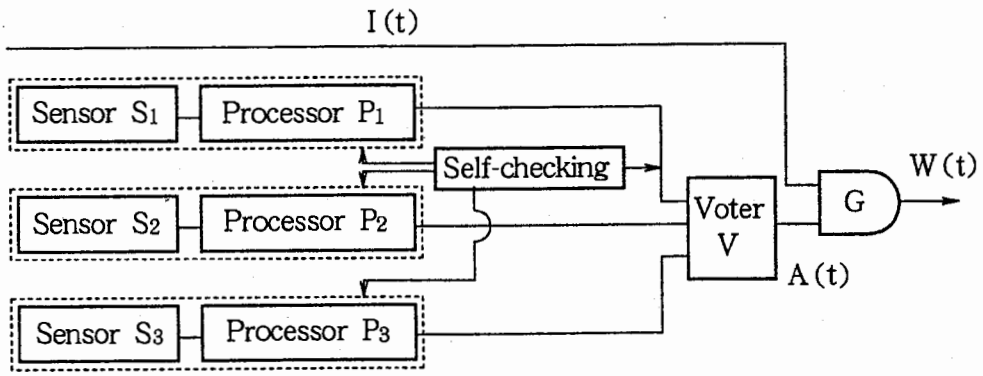


Fig. 6 Safety confirmation system with diversity and self-checking.
異種冗長化と自動監視を備えた安全確認システム

各センサーの信号処理要素（シグナル・プロセッサー）を $P_N(N=1,2,3)$ で表す。ただし，ここでは，センサー S_N及び信号処理要素 P_Nは，共通原因故障を生じない異種冗長化構成であると仮定する（この具体例に，信号処理要素 P_Nをアーキテクチャーの異なる三種類のハードウェアと，異なる設計者によって製作された三種類のソフトウェアの異種三重化構成とする方法などがある)。以後，S_Nと P_Nを一括して扱うためにこれらを総じて要素 SP_Nで表す。

また，要素 SP_Nからの信号がすべて「安全」を示す信号（論理値 1 の信号）を出力しているとき，安全確認信号 $A(t)$ を論理値 1 として発生する要素をボーター Vで表す。この要素では，信号処理要素 P_Nのいずれか 2 つの出力が不一致を生じたときは，センサー S_Nまたは信号処理要素 P_Nに故障が発生したものとして，安全確認信号 $A(t)$ を論理値 0 として機械を停止させる。

ここに，要素 SP_Nの故障発生率をλ_{SC}（回/h），非対称誤り率をη_{SC}（回/回），ボーター Vの故障発生率をλ_V（回/h），非対称誤り率をη_V（回/回）とすると，異種冗長化された N重系 $(N=1,2,3)$ の時刻 t における災害発生率 $r_H(t)$ は次式となる。

$$\begin{aligned} r_H(t) &= \beta\, H_L[1-\exp(-\lambda_{SC}\cdot\eta_{SC}\cdot t)]^N \\ &\quad + \beta\, H_L[1-\exp(-\lambda_V\cdot\eta_V\cdot t)] \\ &\quad + \beta\, H_L[1-\exp(-\lambda_G\cdot\eta_G\cdot t)] \end{aligned} \tag{11}$$

ただし，異種冗長化された N重系とは「独立した N 個の要素 $SP_1, SP_2, \cdots SP_N$がすべて危険側故障を起こしたときに，初めて安全確認システムが人体検知能力を失う」ものと仮定する。

逆に言えば，異種冗長化された三重系で仮に二個の要素 SP_Nが危険側故障を起こした場合でも，安全確認システムは人体検知能力を維持し続け，三個の要素 SP_Nがすべて危険側故障を起こしたときに安全確認システムは初めて人体検知能力を喪失する。このときの演算を行うのがボーター Vである。ここでは，**Fig. 6** のようなボックス形状でボーター Vを表現する。なお，(11) 式以降では，$N=1$ のときはボーターに関連する項は加算しない。

4.3 自動監視によるリスク低減効果

(11) 式は，安全確認システムを構成する要素の危険側故障によって災害発生率が時間とともに増大することを示している。すなわち，長時間の連続運転がなされる機械では，危険側故障が検出されないまま蓄積し，長期的には安全確認システムが機能喪失に至る事態が起こり得る。いま，このことを定量的に示すために，機械の全寿命を Tとすると，全寿命 T内での平均災害発生率 $R_H(T)$ は次式となる。

$$\begin{aligned} R_H(T) &= \left(\int_0^T r_H(t)dt\right)/T \\ &= (\beta/(N+1))H_L(\lambda_{SC}\cdot\eta_{SC}\cdot T)^N \\ &\quad + (\beta/2)H_L(\lambda_V\cdot\eta_V\cdot T) \\ &\quad + (\beta/2)H_L(\lambda_G\cdot\eta_G\cdot T) \end{aligned} \tag{12}$$

ただし，以後の議論を簡素化するために，

$$\lambda_{SC}\cdot\eta_{SC}\cdot T \leqq 1, \lambda_V\cdot\eta_V\cdot T \leqq 1, \lambda_G\cdot\eta_G\cdot T \leqq 1$$

と仮定している（補足 6 参照)。

(12) 式は，非対称誤り特性の実現を非対称誤り率の改善として機能的に行うならば，非対称誤り率がゼロでない限り機械の長期的使用によって安全確認システムの有効性が必ず喪失に向かうことを意味している。

従って，災害を根絶しようとするならば，構造的な非対称誤り特性を実現せざるを得ない。このため，筆者らは構造的な非対称誤り特性を持つ安全確認システムを安全確認形インタロックとして提唱してきた。しかし，安全確認システムを構成するすべての要素について構造的な非対称誤り特性を実現するのは現実に難しい。

そこで，本報では安全確認システムを構成する要素の正常性を定期的かつ自動的に監視する自動監視機構の採用によって，構造的な非対称誤り特性に準ずる状態が実現できないかを定量的に検討した。

ここで，センサー及び信号処理回路（シグナル・プロセッサー）SP_N，ボーター V，及び論理積演算要素 G の自動監視機構のチェック間隔を各々τ_{SC}，τ_V及び τ_G(h) とすると，自動監視機構を持つ安全確認システムの平均災害発生率 $R_H(\tau)$ は次式となる。

$$\begin{aligned} R_H(\tau) &= \left(\int_0^\tau r_H(t)dt\right)/\tau \\ &= (\beta/(N+1))H_L(\lambda_{SC}\cdot\eta_{SC}\cdot\tau_{SC})^N \\ &\quad + (\beta/2)H_L(\lambda_V\cdot\eta_V\cdot\tau_V) \\ &\quad + (\beta/2)H_L(\lambda_G\cdot\eta_G\cdot\tau_G) \end{aligned} \tag{13}$$

ただし，τはτ_{SC}, τ_V及びτ_Gの関数である。

4.4 機械の故障やトラブルの考慮

Fig. 6 のシステムでは作業者が危険領域内に進入したときだけでなく，機械の故障やトラブル（電源，油

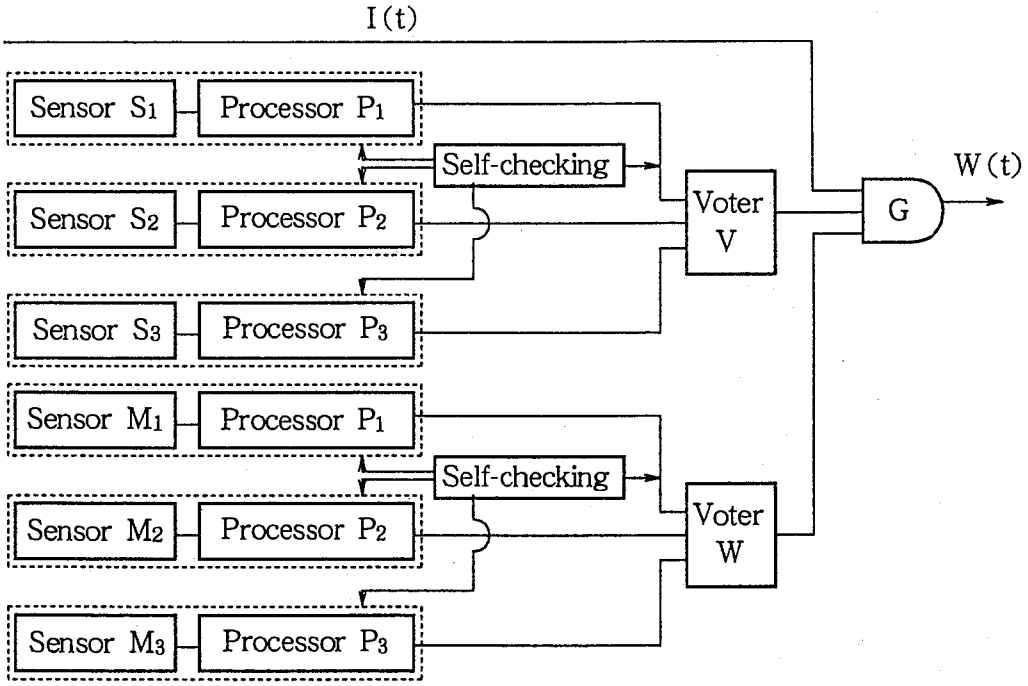


Fig. 7 Example of safety confirmation system considering trouble and malfunction of machinery.
機械の故障やトラブルを考慮した安全確認システムの例

空圧源等の駆動源の故障やトラブルを含む）に起因する暴走によっても災害が発生することがある。したがって，これらに対して安全確認システムを構成する必要がある。

Fig. 7 は，この点を考慮した安全確認システムの基本構成図である。ここでは，機械の故障やトラブルの発生率をα（回/h），機械に故障やトラブルが発生していないことを確認するセンサー及び信号処理回路（シグナル・プロセッサー）の故障発生率をλ_{MC}（回/h），非対称誤り率をη_{MC}（回/回）とする。

また，機械が故障やトラブルを発生していないことを確認するセンサー及び信号処理回路（シグナル・プロセッサー）を $MP_N(N=1,2,3)$, MP_Nからの信号がすべて「安全」を示す信号を出力しているとき，安全確認信号を発生する要素をボーターWで表す。この役割はボーターVと同様である。なお，MP_Nは **Fig. 6** と同様にセンサー M_Nと信号処理要素 P_Nの組み合わせを意味する。

さらに，ボーターWの故障発生率をλ_W（回/h），非対称誤り率をη_W（回/回），要素MP_NとボーターWの自動監視機構のチェック間隔を各々τ_{MC}, τ_Wとすると，平均災害発生率 $R_H(\tau)$ は次式で表すことができる。

$$R_H(\tau)=\left(\int_0^\tau r_H(t)dt\right)/\tau$$
$$=(\beta/(N+1))H_L(\lambda_{SC}\cdot\eta_{SC}\cdot\tau_{SC})^N$$
$$+(\beta/2)H_L(\lambda_V\cdot\eta_V\cdot\tau_V)$$
$$+(\alpha/(N+1))H_L(\lambda_{MC}\cdot\eta_{MC}\cdot\tau_{MC})^N$$
$$+(\alpha/2)H_L(\lambda_W\cdot\eta_W\cdot\tau_W)$$
$$+(\gamma/2)H_L(\lambda_G\cdot\eta_G\cdot\tau_G) \quad (14)$$

ただし，$\gamma=(\alpha+\beta)$ である。

5. リスク低減に関する定量的な検討結果

5.1 定量的検討を行うにあたっての仮定

次に，**Fig. 7** の安全確認システムに異種冗長化と自動監視を適用した場合の平均災害発生率 $R_H(\tau)$ を定量的に検討する。

この検討で使用する数値は，確率的なリスク評価に含まれる不確定性を最小化するために，安全の原理に従って以下の仮定を置いている。

1) センサー及びシグナル・プロセッサーは対称誤り特性を持つ要素（たとえば，プログラマブルな電子制御装置）で構成するものとし，このときの非対称誤り率の理論的な最悪値として$\eta_{SC}=1$回/回，$\eta_{MC}=1$回/回を設定した。
2) 1) の場合の自動監視機構のチェック間隔は，想定できる最悪値として，$\tau_{SC}=0.5$h, $\tau_{MC}=0.5$h を仮定した。これは，シグナル・プロセッサー P_N 間のメモリーの不一致検出に最悪値としてこの程度

Table 2　Effectiveness of redundancy, diversity and self-checking for safety confirmation system.
安全確認システムにおける冗長化，異種冗長化及び自動監視の効果

冗長化の程度と，自動監視機構の有無		平均災害発生率の推定値（回/h）		
		センサー及びシグナル・プロセッサは		
		異種のプログラマブルな電子制御装置で構成	安全確認形インタロックで構成	同種のハードワイヤードな制御装置で構成
自動監視機構なし	パラメーター	$\eta_{SC}=1$ 回/回, $\eta_{MC}=1$ 回/回, $T=10^3$h と仮定	$\eta_{SC}=10^{-3}$回/回, $\eta_{MC}=10^{-3}$回/回, $T=10^3$h と仮定	$\eta_{SC}=10^{-1}$回/回, $\eta_{MC}=10^{-1}$回/回, $T=10^3$h と仮定
	一重系	3.7×10^{-2}	5.0×10^{-5}	5.0×10^{-3}
	二重系	1.7×10^{-2}	——	3.3×10^{-4}
	三重系	8.5×10^{-3}	——	2.5×10^{-5}
自動監視機構あり	パラメーター	$\eta_{SC}=1$ 回/回, $\tau_{SC}=0.5$h, $\eta_{MC}=1$ 回/回, $\tau_{MC}=0.5$h と仮定	$\eta_{SC}=10^{-3}$回/回, $\tau_{SC}=10^{-5}$h, $\eta_{MC}=10^{-3}$回/回, $\tau_{MC}=10^{-5}$h と仮定	$\eta_{SC}=10^{-1}$回/回, $\tau_{SC}=10^{-3}$h, $\eta_{MC}=10^{-1}$回/回, $\tau_{MC}=10^{-3}$h と仮定
	一重系	2.5×10^{-5}	1.0×10^{-12}	5.0×10^{-9}
	二重系	8.4×10^{-9}	——	1.0×10^{-12}
	三重系	4.2×10^{-12}	——	1.0×10^{-12}

注）$\lambda_{SC}=10^{-3}$回/h, $\lambda_{MC}=10^{-3}$回/h, $\alpha=10^{-3}$回/h, $\beta=10^{-1}$回/h, $H_L=1$,
$\lambda_V=10^{-3}$回/h, $\eta_V=10^{-3}$回/回, $\tau_V=10^{-5}$h, $\lambda_W=10^{-3}$回/h,
$\eta_W=10^{-3}$回/回, $\tau_W=10^{-5}$h, $\lambda_G=10^{-3}$回/h, $\eta_G=10^{-3}$回/回, $\tau_G=10^{-5}$h

の時間が必要と考えためである。ただし，この場合は，万一チェック間隔が 0.5h を越えた場合，機械の運転を停止させる構成が必要である。

3) センサー及びシグナル・プロセッサーの不信頼度は，想定できる最悪値として，$\lambda_{SC}=10^{-3}$回/h, $\lambda_{MC}=10^{-3}$回/h を仮定した。

4) ボーター及びインタロックは確定的な安全方策を施した要素（たとえば，安全確認形インタロック）で構成するものとした。このとき，非対称誤り率は理論的にはゼロとなるが，ここでは予測不可能な危険側故障を考慮し，想定できる最悪値として，$\eta_V=10^{-3}$回/回，$\eta_W=10^{-3}$回/回，$\eta_G=10^{-3}$回/回を仮定した。

5) 4) の場合の自動監視機構のチェック間隔には，想定できる最悪値として$\tau_V=10^{-5}$h，$\tau_W=10^{-5}$h，$\tau_G=10^{-5}$h を仮定した。これは，約 30 msec に相当するチェック間隔であり，機械の緊急停止などを行うときに制御システムの処理時間として経験的に許容される応答遅れ時間に相当する。

6) ボーター及びインロックの不信頼度は，想定できる最悪値として，$\lambda_V=10^{-3}$回/h，$\lambda_W=10^{-3}$回/h，$\lambda_G=10^{-3}$回/h を仮定した。

7) 人間側の不信頼度は，想定できる最悪値として$\beta=10^{-1}$回/h を仮定した。

8) 機械側の不信頼度は，想定できる最悪値として$\alpha=10^{-3}$回/h を仮定した。

9) 危険回避の可能性は，回避の確定性が期待できないため，理論的な最悪値として $H_L=1$ を設定した。

5.2 検討結果

Table 2 は，**Fig. 7** の安全確認システムに異種冗長化と自動監視を適用した場合の平均災害発生率 $R_H(\tau)$ の変化を検討した結果である。ただし，センサー及びシグナル・プロセッサーはプログラマブルな電子制御装置で構成している。

ここでは，センサー及びシグナル・プロセッサーを安全確認形インタロックや同種のハードワイヤードな制御装置の多重化で構成する場合もあることを考慮し，これらを適用した場合の災害防止効果も参考値として示した。ただし，ここでは議論を簡単にするため，同種のハードワイヤードな制御装置では共通原因故障は発生しないものと仮定している。

Fig. 8 は，プログラマブルな電子制御装置を利用したセンサー及びシグナル・プロセッサーの非対称誤り率 η_{SC}，チェック間隔τ_{SC}及び不信頼度λ_{SC}の変化が，平均災害発生率 $R_H(\tau)$ に及ぼす影響を検討した結果である。

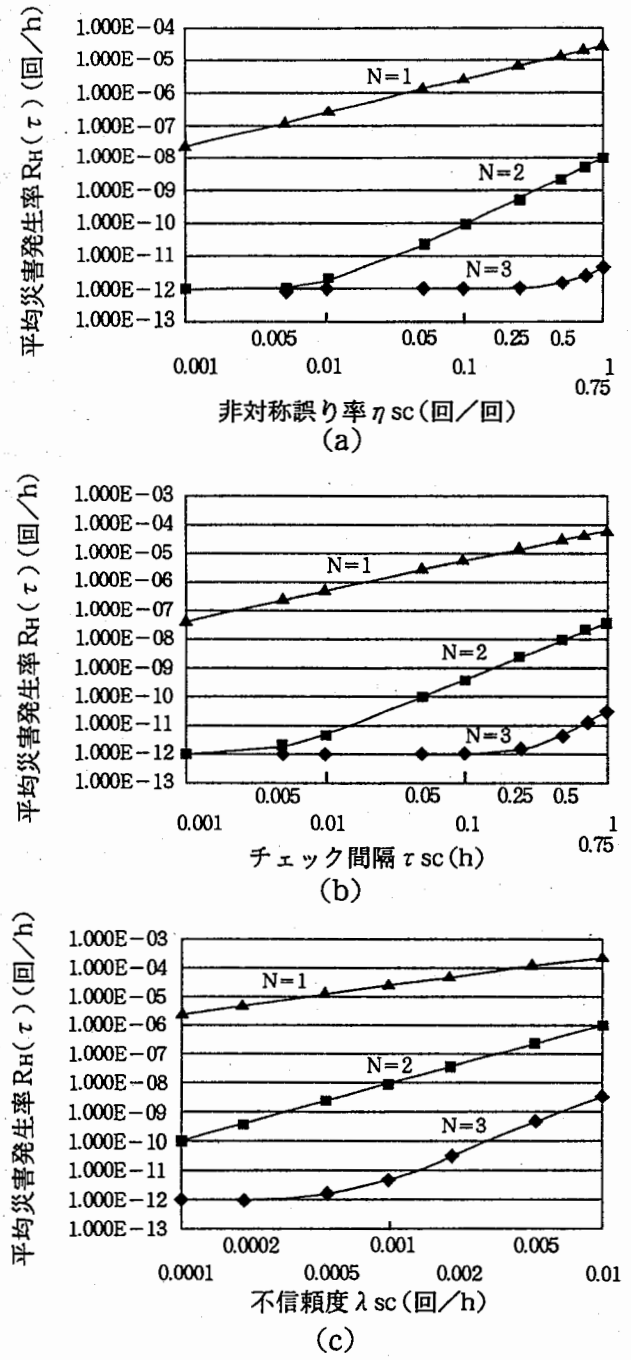


Fig. 8 Average rate of incident estimated in this study.
本研究で推定した平均災害発生率

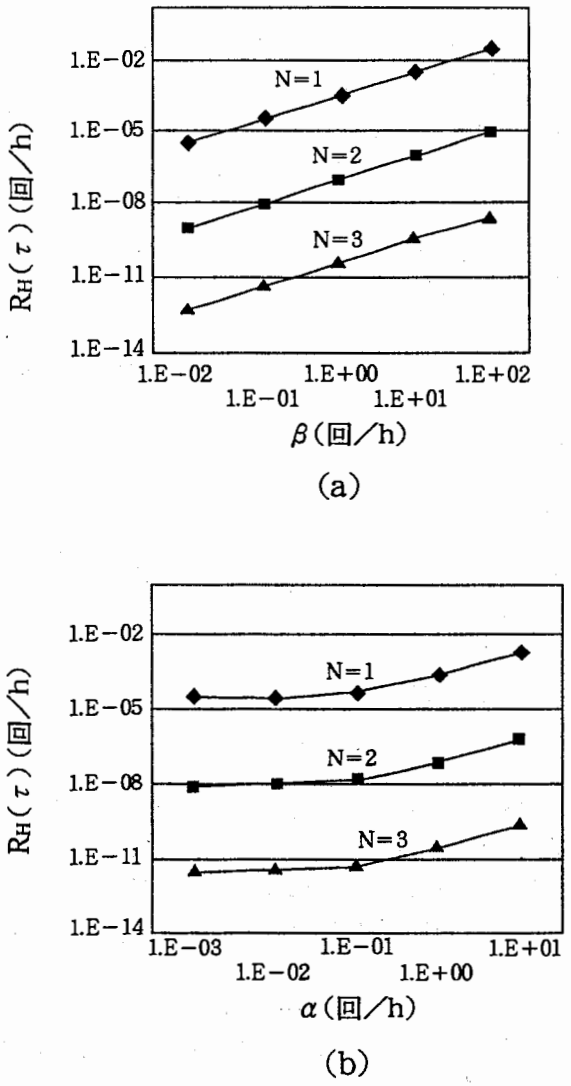


Fig. 9 Average rate of incident estimated in this study.
本研究で推定した平均災害発生率

Fig. 9 は，α及びβの変化が平均災害発生率 $R_H(\tau)$ に及ぼす影響を検討した結果である。

これらより，次のことが推察できる。

① 自動監視機構が設置されていない安全確認システムでは，異種冗長化された二重系や三重系であっても目標値を達成できない。したがって，自動監視機構は不可欠である（**Table 2** 参照）。

② センサー及びシグナル・プロセッサーを対称誤り特性を持つ要素（たとえば，プログラマブルな電子制御装置）で構成する場合は，センサー及びシグナル・プロセッサーを異種冗長化された三重化構成とし，自動監視機構のチェック間隔τ_{SC}を 0.5h 以下，かつ不信頼度λ_{SC}を 10^{-3}回/h 以下とすれば，目標値は達成できる（**Fig. 8(b), (c)** 参照）。

③ 上記②の条件の下で，異種冗長化された二重化構成によって目標値を達成しようとする場合は，自動監視機構のチェック間隔を 1 分に 1 回程度まで短縮する必要がある（**Fig. 8(b)** 参照）。しかし，メモリーチェック時間も考慮した場合，1 分に 1 回のチェックは困難なときもある。

④ 上記②の条件の下で，異種冗長化された三重化構成によって目標値を達成できるのは，αとβが一定の条件のとき (たとえば，$\alpha = 10^{-3}$回/h のとき$\beta \leqq 10^{-1}$回/h，$\beta = 10^{-1}$回/h のとき$\alpha \leqq 10^{-1}$回/h) である（**Fig. 9(a), (b)** 参照）。

また，$\alpha = 10^{-2}$回/h 以下ではβの寄与が大きくなるために，αを改善しても平均災害発生率は減少しない（**Fig. 9(b)** 参照）。

⑤　ボーター V，W及びインタロック G の故障に起因する災害発生率が一定値以下でないと（たとえば，$\beta/2\,(\lambda_V\eta_V\tau_V)+\alpha/2\,(\lambda_W\eta_W\tau_W)+\gamma/2\,(\lambda_G\eta_G\tau_G) \leqq 10^{-11}$), 目標値を達成できない。

また，参考として次のことが推察できる。

⑥　センサー及びシグナル・プロセッサーを安全確認形インタロックで構成する場合は，自動監視機構のチェック間隔が概ね 10^{-5}h 以下なら，冗長化を図らなくとも（一重系でも）目標値を達成できる（**Table 2** 参照）。

これに対し，センサー及びシグナル・プロセッサーを同種のハードワイーヤードな制御装置で構成する場合は，自動監視機構のチェック間隔が概ね 10^{-3}h 程度なら，二重化構成としなければ，目標値は達成できない（**Table 2** 参照）。

6.　おわりに

産業機械を対象とした災害防止対策では，残存リスクの最小化が不可欠である。しかし，現実には，確率的なリスク評価によって残存リスクを推定しても，この評価に含まれる不確定性の方が桁違いに大きい場合もある。

このため，本報では「不確定は危険と見なす」安全の原理にしたがって，安全確認システムの非対称誤り率ηに最悪値評価として$\eta = 1$ を与えるなどの方法によって，確率的評価に含まれる不確定性を最小化できる評価手法を提案した。また，残存リスクを最小化できる対策として，次の優先順位に基づく安全方策を提案した。

1)　確定的な安全方策（安全確認形インタロックの適用など）の実施によるリスクの排除と安全性の立証
2)　安全確認システムの機能的な非対称誤り特性の改善（異種冗長化や自動監視等の応用）
3)　人間や機械の不信頼度の改善（機械及び安全確認システムに対する高信頼化技術の適用，作業者の人的ミスを減少させる伝統的な労働安全手法の適用）
4)　上記 2) 及び 3) に対する確率的なリスク評価と残存リスクの確定

次に，本報では，これらの検討結果を基に，異種冗長化と自動監視技術を応用した安全確認システムが，機能的な方法による非対称誤り特性の改善によって残存リスクをどの程度まで低減できるかを数値例を用いて検討した。

その結果，センサー及びシグナル・プロセッサーを対称誤り特性を持つ要素（たとえば，プログラマブルな電子制御装置など）で構成したシステムでは，独立した異種三重系以上の冗長化と，少なくとも 30 分に一回以上のチェック間隔を持つ自動監視機構の採用によって，高リスクと判断される産業機械にも適用可能であることが推察された。

参考文献

1)　梅崎重夫·杉本　旭，安全性の評価指標と労働災害分析，日本ロボット学会第 6 回学術講演会 (1988), pp.367–370.
2)　梅崎重夫・井土伸彦・中村英夫，異種冗長化技術を応用した産業用機械の安全設計法の定量化に関する一考察，日本機械学会第 18 回設計シンポジウム (2000), pp.73–80.
3)　杉本　旭·蓬原弘一，安全の原理，機械学会論文誌，C 編，56–530 (1990), pp.2601–2609.
4)　Revision of ISO/IEC GUIDE51, Safety aspect – Guidelines for their inclusion standards (1997).
5)　松本俊次，リスクマネージメントで会社を守れ，工業調査会 (1999), p.202.
6)　向殿政男・蓬原弘一他，ISO 機械安全国際規格，日刊工業新聞社 (1999), p.7.
7)　IEC61508, Functional safety of electrical/electric/programable electric safety-related systems Part:1～Part:7 (1998).

[補足 1]

安全確認システムとは，安全が確認されているときに限って機械の運転を許可するシステムの総称であり，**Fig. 2** の構成を持つ。

このシステムでは，安全を確認するためのセンサーとインタロックが故障すると，危険な状態のときに機械を停止できなくなることがある。

そこで，センサーやインタロックの故障時には運転許可信号を発生させないフェールセーフ構造とする必要がある。これを安全確認型インタロックと呼んでいる。

[補足 2]

この原理[3]は，安全に関する状態に，従来考えられているように安全と危険の 2 種類だけでなく，安全とも危険とも判断のつかない不確定状態があり，この不確定状態を危険と見なす必要があることを言っている。

[補足 3]

ハインリッヒの法則とは，重大な災害 1 件の背後には，軽微な災害（たとえば，本報で言う赤チン災害など）29 件，ヒヤリ・ハット災害約 300 件が潜在してい

ることをハインリッヒが統計的に明らかにしたものである。

[補足 4]

ここで，最悪値と仮定した$\lambda = 10^{-3}$回/h，$\alpha = 10^{-3}$回/h，$\beta = 10^{-1}$回/hは，筆者のうちの一人が産業現場での経験に基づいて設定した代表例に過ぎない。したがって，極めて信頼性の低い機械や訓練の不十分な作業者は，この仮定を満足できないことがある。このため，本報では，**Fig. 8** と **Fig. 9** にλ，α，βが変動したときの平均災害発生率の推定値を併記した。

[補足 5]

この優先順位は欧州機械指令，ISO12100 などにも記載されている。しかし，安全の原理に基づき，不確定性の少ない順に高い優先度を与えようとする考え方は，明確に記載されていない。

[補足 6]

ここで，$\lambda_S \eta_S T \leqq 1$ が成立しない場合，(12) 式の近似式は成り立たず，$R_H(T)$ は次式で置き換えなければならない。

($N = 1$ の場合)

$$R_H(T) = \beta H_L[1 + (1/\lambda_{SC}\eta_{SC}T)\exp(-\lambda_{SC}\eta_{SC}T) - (1/\lambda_{SC}\eta_{SC}T)] + (\beta/2)H_L(\lambda_G \cdot \eta_G \cdot \tau_G) \quad \text{(A-1)}$$

($N = 2$ の場合)

$$\begin{aligned} R_H(T) = \beta H_L[&1 + (2/\lambda_{SC}\eta_{SC}T)\exp(-\lambda_{SC}\eta_{SC}T) \\ &- (1/2\lambda_{SC}\eta_{SC}T)\exp(-2\lambda_{SC}\eta_{SC}T) \\ &- (2/\lambda_{SC}\eta_{SC}T) + (1/2\lambda_{SC}\eta_{SC}T)] \\ &+ (\beta/2)H_L(\lambda_V \cdot \eta_V \cdot \tau_V) \\ &+ (\beta/2)H_L(\lambda_G \cdot \eta_G \cdot \tau_G) \end{aligned} \quad \text{(A-2)}$$

($N = 3$ の場合)

$$\begin{aligned} R_H(T) = \beta H_L[&1 + (3/\lambda_{SC}\eta_{SC}T) \\ &\exp(-\lambda_{SC}\eta_{SC}T) - (3/2\lambda_{SC}\eta_{SC}T) \\ &\exp(-2\lambda_{SC}\eta_{SC}T) + (1/3\lambda_{SC}\eta_{SC}T) \\ &\exp(-3\lambda_{SC}\eta_{SC}T) - (3/\lambda_{SC}\eta_{SC}T) \\ &+ (3/2\lambda_{SC}\eta_{SC}T) - (1/3\lambda_{SC}\eta_{SC}T)] \\ &+ (\beta/2)H_L(\lambda_V \cdot \eta_V \cdot \tau_V) \\ &+ (\beta/2)H_L(\lambda_G \cdot \eta_G \cdot \tau_G) \end{aligned} \quad \text{(A-3)}$$

(平成 14 年 1 月 10 日受理)