Research Reports of the Research Institute of Industrial Safety, RIIS-SRR-90, 1990

6. A-Cモデルによるシステム的安全性評価

佐藤吉信*

6. Systematic Safety Assessment Using an A-C Model

by Yoshinobu SATO*

Abstract: The strategy for ensuring the safety of man-machine systems is:

1) To incorporate a fail-safe mechanism, and if this is not feasible, 2) To apply a fault-tolerant configuration, and 3) To execute equalitative and quantitative systems analyses.

In this paper, first of all, the concept of hazard-space and hazard-sets is introduced in accordance with the A-C model hazard-production theory, and the definition of a fail-safe system and a fault-tolerant system is generalized, which results in the system condition for structuring the fail-safe mechanism in a system.

Next, an actual man-machine system, which consists of aged workers and movable lifters for supporting the workers, is assumed. And the main hazards of lifters to the workers, which are produced during the operation of lifters, are identified, and hazard-control systems are structured using an A-C model. The applicability of a fail-safe mechanism to the hazard-control systems is explored systematically, and three design tactics for the hazard-control systems are presented. Then, qualitative and quantitative systems analyses are implemented using fault-tree analisis, and how to obtain the optimam design tactics is shown. Finally, the effectiveness of the hazard-control systems is assessed by evaluating the statistically-expected-number of occurrences of the system failures (top event of the fault-tree) and compared with the residual risks of other systems.

6.1 緒　言

系の安全化を図る一連の活動すなわち系の安全計画は，災害の再発を防止するための事後安全計画と，潜在的に発生の可能性のある災害を事前に予防する事前安全計画とに大別できる。系統的な安全計画の実施手順はFig. 6.1のようになろう。

新しい装置・機械・作業方法を導入するに際しては，事前安全計画が系統的方法論に基づいて適切に実施されなければならない。事前安全計画では，Fig. 6.1にみるように，まずデータ収集に基づいて，新しい装置・機械・作業方法を導入する系内に生ずる潜在危険が同定される。以下順次，潜在危険抑制手段の概念化(基本設計)，それらの抑制手段の条件下での定性的安全性解析，定量的安全性解析，… と実施される。

このような事前安全計画において，安全性評価に課せられる範囲は，主として手順1,2,3,4, すなわち，

1. 潜在危険の同定
2. 潜在危険抑制措置の検討
3. 定性的安全性解析
4. 定量的安全性解析

である[1,2]。

ここで，潜在危険の同定とは，系内にどのような故障や異常が発生し，その結果どのような毀損が生じうるかを帰納的に予測しみきわめる作業を意味する。

次に，同定された潜在危険に対してその抑制措置が検討される。潜在危険抑制措置の構成過程は，多相安全設計として体系化される。多相安全設計は，戦略

*機械研究部，Mechanical Safety Research Division

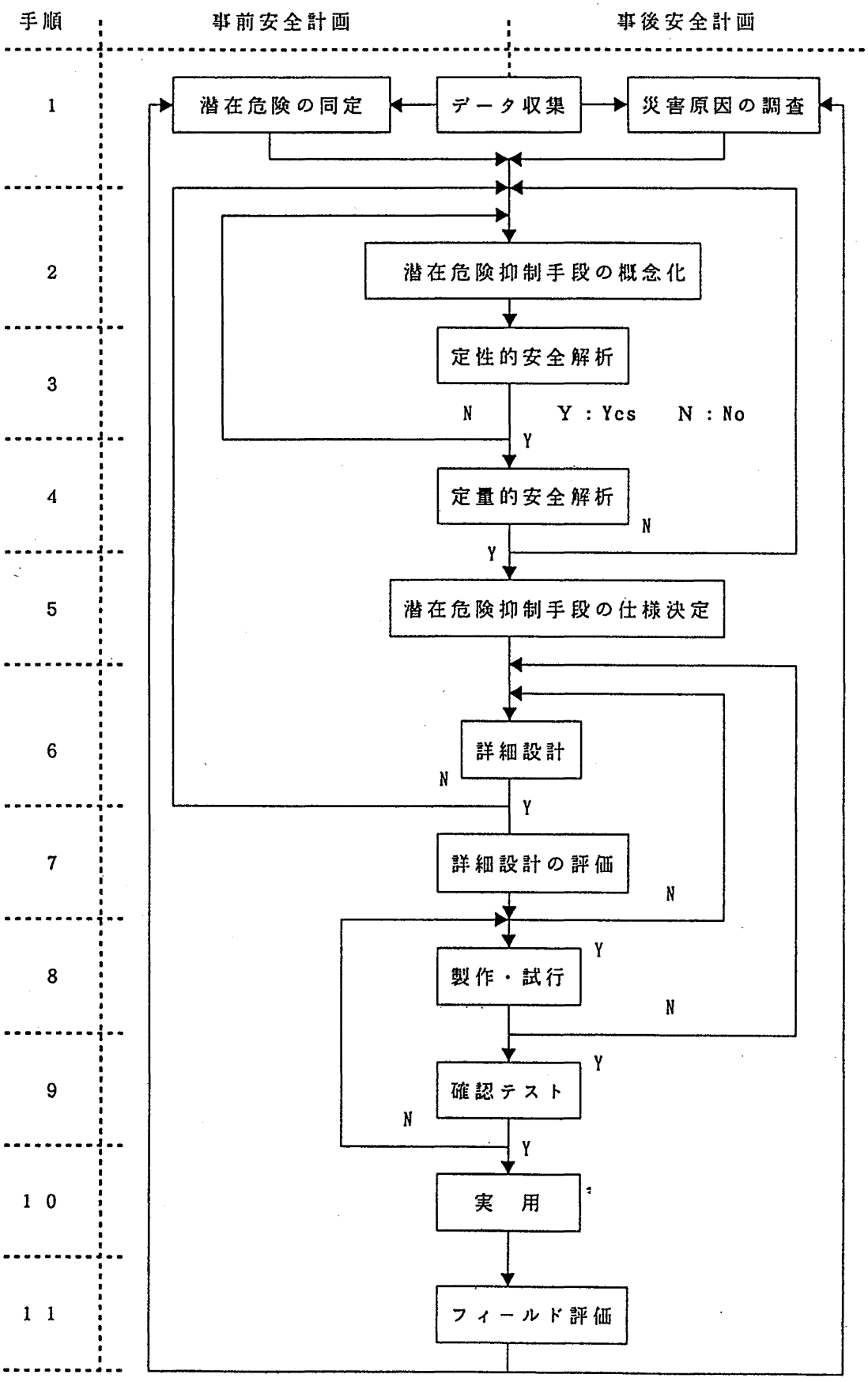


Fig. 6.1　Procedure of safety program.
安全計画の実施手順

的多相安全設計と戦術的多相安全設計を順次検討して実施される。ここで，戦略的多相安全設計とは系に潜在危険の抑制原理を系統的に適用する設計過程であり，戦術的多相安全設計とは系に潜在危険制御系を構成して系のフェール・セーフ・システム化やフォールト・トレラント・システム化を図る設計過程である[3]。

さらに，それらの潜在危険抑制措置の条件下での系の定性的安全性解析および定量的安全性解析が実施され，検討された潜在危険抑制措置から最善のものが選択される。また，安全性解析の結果によっては，再び手順 (2) に戻って潜在危険抑制措置を再構成しなければならないこともありうる。

安全性解析によって，潜在危険抑制措置構築のための詳細設計条件が与えられる。

事前安全計画は，機器の 1) 組み立て・設置，2) 運用，3) 移動，4) 廃棄など，そのライフサイクル全般にわたって実施されるのが理想であり，その過程で新しい機器を導入することにより減ずるリスクと新たに生ずるリスクとが比較・評価されなければならない。

本報告は，昇降リフタ等移動機構を高齢者による作業系に導入した時の安全性を，主として機器の運用時を対象として評価する。

6.2 潜在危険の集合論的表示とフェール・セーフ・システムの定義および構成条件

安全工学の基本的術語である「潜在危険」や「フェール・セーフ・システム」の用語は，今日ではマスコミなどジャーナリズムをはじめ多方面で使用されるようになった。例えば，フェール・セーフ・システム（元来，鉄道信号の分野で用いられ，信号系統に発生した障害が列車を停止させる方向に収束するような系の構成方法を意味していた）の用語は，近年では原子力プラントや航空機の設計など広範な分野で使用されている。しかしながら，ある種の冗長系を構成することをフェール・セーフ・システムと呼ぶなど，その意味するところが各分野で異なっており，各種工学体系間を横断する安全論議にしばしば混乱が生じている[4]。

JIS では，フェール・セーフを「部品の故障が人体障害を起こさないような設計上の配慮」と定義している[5]。大方の専門家にとって，フェール・セーフの本質が系の Inherence（事象の収束を工学的な機能に頼らず，自然法則すなわち自然に収束する方向に任せること）な安全構造の構築であることについては，異存のないことであろう。JIS の定義は，このフェール・セーフの本質を汲んでおらず，辞書的意味としてはともかくとして，安全工学上不十分である。

また，論理回路の分野では，「ある論理系において，故障が生じても，誤り出力があらかじめ決められた安全側の出力に限られる時，その論理系はフェール・セーフである」と定義されている[6]。この定義をそのまま機械系，化学系，あるいは人間の挙動などが混在する一般の系に拡張するには無理がある。そこでは，まず，1) 故障とは何か，2) 出力とは何か，3) 安全側とは何か，ということが問題となる[7]。

一方，潜在危険は，米国など先進国では，術語としていくつかに定義され[8,9]，専門用語としてある程度慎重さをもって使用されている。しかし，わが国では，潜在危険の術語は，佐藤等の定義があるものの[10,11]，一般的にはさほど神経質には扱われていない。潜在危険とフェール・セーフ・システムは互いに密接に関連しており，それらの基本的術語が系統的に論ぜられる必要がある。

そこで，本節では，A-C モデルから新たに潜在危険集合の概念を導出することにより，フェール・セーフ・システムを異なる工学体系間に一般化して定義して，フェール・セーフ・システムの構成条件を明らかにする。

6.2.1 潜在危険集合

潜在危険同定の方法論，潜在危険の抑制原理および潜在危険制御系（以下，H-制御系）の構成法則は，A-C モデルと作用鎖の解離法則として体系化されている[12–29]。ここで，A-C モデルを拡張して，系の潜在危険集合を次のように定義する：

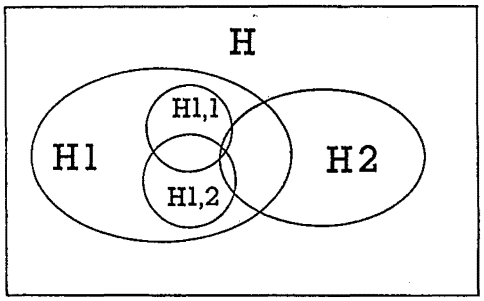
［定義 6-1］系において，潜在危険を単連鎖からなる作用連鎖で同定した時，それらの作用を発生させるその作用連鎖中の全変化，および直接原因作用から最も離れた作用を発生させる変化を直接または間接的に誘発させる系の全変化からなる集合を，その作用連鎖が同定する潜在危険集合とする。

定義より，系の全潜在危険集合（潜在危険空間）は系の全変化集合として定義され，これを集合 H で表すものとする。

ここで，例えば次の 2 本の作用連鎖（単連鎖）：

$$X(x)a \xrightarrow[0]{} W(\cdot) \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots (6\text{-}1)$$

$$X(y)f \xrightarrow[0]{} W(\cdot) \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots (6\text{-}2)$$



H　：全潜在危険集合
H1　：潜在危険集合 [X (x) a $\xrightarrow[0]{}$ W (·)]
H2　：潜在危険集合 [X (y) f $\xrightarrow[0]{}$ W (·)]
H1,1：潜在危険集合 [A (a) a $\xrightarrow[1]{}$ X (x) a $\xrightarrow[0]{}$ W (·)]
H1,2：潜在危険集合 [B (b) f $\xrightarrow[1]{}$ X (x) a $\xrightarrow[0]{}$ W (·)]

Fig. 6.2　Hazard-space and hazard-sets.
潜在危険の集合論的表示

すると，H1 は作用鎖$[a \xrightarrow[0]{}]$を発生させる要素X中の全変化集合x，および要素Xに結合して変化x_i $(\in x)$を誘発させる全作用連鎖中の全変化集合からなる変化集合として定義される。H2 も同様である。

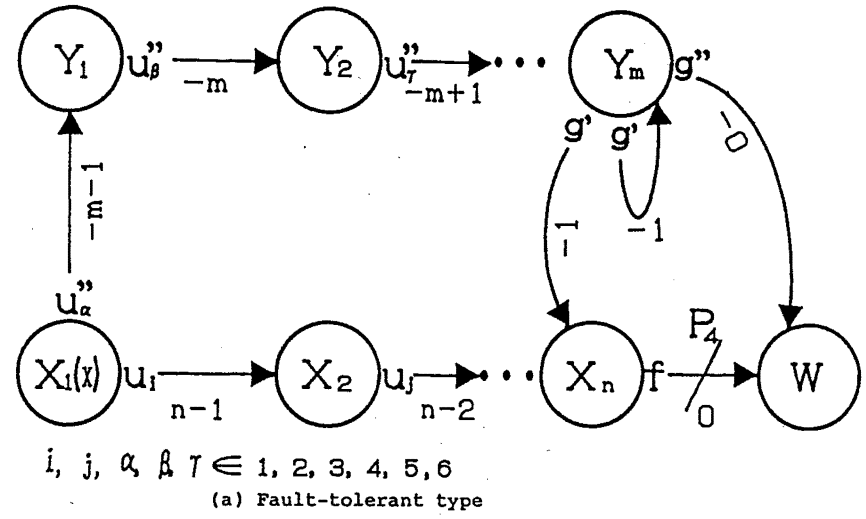
さらに，次の作用連鎖：

$$A(a)a \xrightarrow[1]{} X(x)\ a \xrightarrow[0]{} W(\cdot) \cdots\cdots\cdots\cdots (6\text{-}3)$$

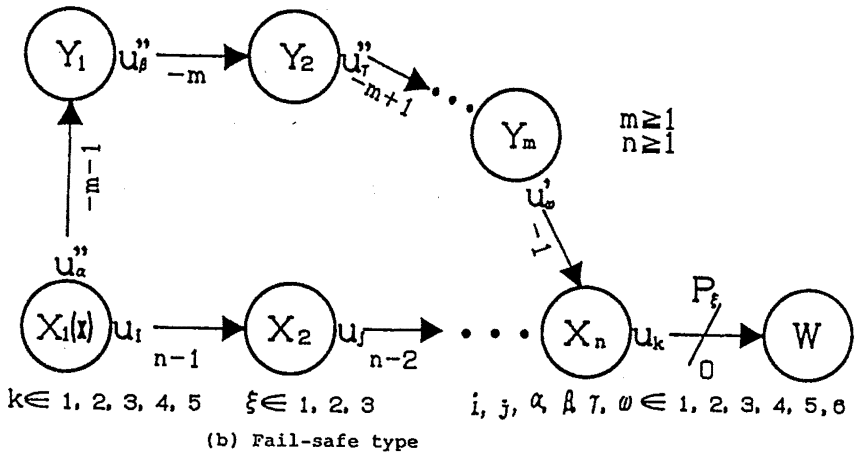
$$B(b)f \xrightarrow[1]{} X(x)\ a \xrightarrow[0]{} W(\cdot) \cdots\cdots\cdots\cdots (6\text{-}4)$$

で同定される潜在危険集合を，それぞれ H1,1, H1,2 と定義すると，系の全潜在危険集合 H，部分潜在危険集合 H1, H2, H1,1, H1,2 との関係は，Fig. 6.2 のように図示される。

H が枠内の全空間を占め，部分潜在危険集合がそれぞれの楕円および円内の領域を占める。領域の重なが同定する潜在危険集合を，それぞれ H1, H2 とする。



(a) Fault-tolerant type



(b) Fail-safe type

Fig. 6.3　Schematic representations of fault-tolerant and fail-safe dissociations.
フェールセーフとフォールトトレラント形解離を行う H-制御系の図式表現

り合う部分は，それらの作用連鎖が共に誘発される変化集合領域を示している。

6.2.2 フォールト・トレラント・システムとフェール・セーフ・システムの定義

Fig. 6.3 は，ある毀損を要素 W に生じさせる潜在危険が，要素X_1の故障xを引き金として，X_1, X_2, $\cdots$と次々と作用を伝播させることにより発現しようとする時，H-制御系が作用連鎖を途中で解離して毀損を防ぐ場合の図式表現である。図中 (a) では，作用鎖$[f \xrightarrow[0]{}]$が解離原理P_4で，(b) では，作用鎖$[u_k \xrightarrow[0]{}]$が解離原理P_ξ ($\xi \in 1,2,3$) で解離されている。

ここで，フォールト・トレラント・システムとフェール・セーフ・システムを次のように定義する：

［定義 6-2］ある潜在危険集合xの任意の変化（故障）x_iが系に発生することにより発現する作用連鎖，または，潜在危険集合yの任意の変化（故障）y_jが系に発生することにより発現する反転連鎖を解離原理P_4で解離して毀損を防止できれば，系はxとその毀損（xが引き起こす作用連鎖すなわちその潜在危険），または，yとその毀損（yが引き起こす反転連鎖すなわちその潜在危険）に関してフォールト・トレラント・システムである。また，解離原理P_4による解離をフォールト・トレラント形解離という。

［定義 6-3］同様に，解離原理P_ξ ($\xi \in 1,2,3$) で解離して毀損を防止できれば，系はxとその毀損（xが引き起こす作用連鎖すなわちその潜在危険），または，yとその毀損（yが引き起こす反転連鎖すなわちその潜在危険）に関してフェール・セーフ・システムである。また，これらの解離をフェール・セーフ形解離という。

以上の定義から，フェール・セーフ・システムやフォールト・トレラント・システムを論ずる場合，まず，議論の適用範囲としての潜在危険集合を明確にしなければならないことがわかる。これは，一般的には（イ）同一の系の同一の潜在危険集合に関し，ある変化（故障）部分集合に対してはフェール・セーフ・システムが構成できるが別の変化（故障）部分集合には構成できない，（ロ）同一の系の同一の変化（故障）部分集合でも，異なる潜在危険に対して同時にはフェール・セーフ・システムを構成できない，場合が多いからである。

そこで，次節では，H-制御系による危険回避時における系の状態遷移について考察し，さらにこれに基づきフェール・セーフ・システムの構成条件を明らかにする。

6.2.3 被制御要素の状態遷移

潜在危険は，H-制御系が被制御要素のエネルギ状態や化学的性質を制御する，すなわち作用鎖（反転作用鎖）を解離することにより抑制される。ある作用鎖が発現しようとする時，例えば H-制御系が被制御要素のエネルギ状態を高エネルギ状態 H から低エネルギ状態 L に移行させることにより作用鎖を解離させる時：

(1) Fig. 6.4(a) に示すように，あらかじめ予定されていたある時間内とエネルギ・レベル内で無秩序に H から L に遷移させればよい：

(2) Fig. 6.4(b) のように，ある時間内で，例えばフィードバック制御によって，外乱などに応じて定まるポイント A, B, $\cdots$などを通過させるなど，秩序をもって遷移させなければならない；

場合とがある。前者には，プラント容器のリリーフ弁開閉前後における，容器内の内部エネルギの状態遷移が典型的な例としてあげられる。後者には，気象学的外乱下での，航空機の着陸時における機体の運動エネ

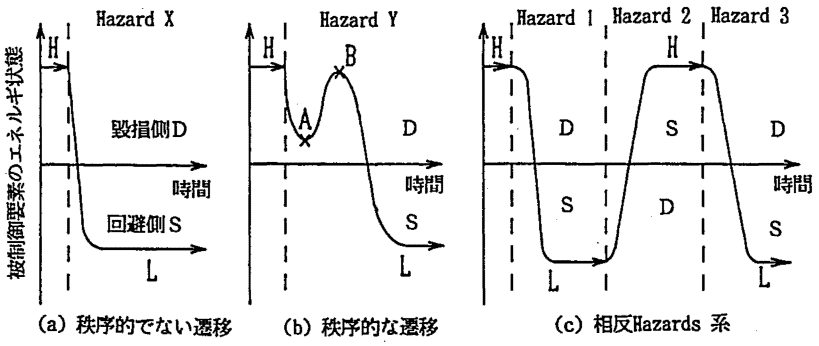


Fig. 6.4 Transition of a system-element for hazard-control.
危険回避のための被制御要素の状態遷移

ルギの状態遷移が典型的な例としてあげられる。

無秩序な状態遷移は原理的に単方向制御作用鎖からなるH-制御系でも遂行されうるが，フィードバック制御などのような秩序をもった状態遷移は，外依複方向作用鎖が必要となるため，単方向制御作用鎖のみで構成されるH-制御系では実現できない。したがって，要素の状態遷移と制御作用鎖との関係が次の定理として得られる：

［定理 6-1］無秩序な状態遷移は，単方向制御作用鎖のみで構成されるH-制御系で原理的に実現可能である。他方，フィードバック制御による状態遷移は，外依複方向作用鎖で構成される制御連鎖を含むH-制御系によってのみ実現される。

［定義 6-4］Fig. 6.4(c) に示すように，系内に複数の潜在危険が次々と発現しようとし，しかもH-制御系による要素の状態遷移の方向が各潜在危険で異なる場合がある。このような潜在危険を相反潜在危険と定義する。

$f''(f')$ の作用鎖は，1方向のみの状態遷移を可能とするので，相反潜在危険に関して次の定理を得る：

［定理 6-2］H-制御系の構成要素のうち，相反潜在危険に共通して対応しなければならない要素は，少なくとも一方の潜在危険に対して能動形抑制（解離）作用鎖を構成しなければならない。

6.2.4　フェール・セーフ・システムの構成条件

Fig. 6.3 の抑制要素Y_2に故障y_j $(\in y)$ が発生し，$[Y_2 u_{\nu''} \xrightarrow[-m+1]{}]$が$[Y_2(y_i)\overline{u_l} \xrightarrow[m-1]{}]$と反転する場合を考える。$u_{\nu''}$が能動形 $(\gamma \in 1,2,\cdots,5)$ の時，$\overline{u_l}$は$\overline{f}$となり，$u_{\nu''}$がf''の時能動形反転作用$\overline{u_l}$ $(l \in 1,2,\cdots,5)$ の少なくともひとつが生ずる。これらの反転作用のうち，能動形反転作用はフェール・セーフ形解離で解離される。もし解離されるならば，系は故障yと毀損に関してフェール・セーフ・システムである。このようにして，次のフェール・セーフ・システム構成定理を得る：

［定理 6-3］機能停止形の抑制（解離）作用を行うH-制御系構成要素にはフェール・セーフ・システムが，能動形抑制（解離）作用を行うH-制御系構成要素にはフォールト・トレラント・システムがそれぞれ原理的に構成可能である。

フィードバック回路を構成する外依複方向制御作用鎖は，能動形抑制作用鎖のみで構成される。したがって，フィードバック回路を機能させるH-制御系構成要素にはフォールト・トレラント・システムを構成しなければならない。また，相反潜在危険に対処するH-制御系が同一のH-制御系構成要素で構成される場合，その構成要素には少なくとも1つの潜在危険に対してフォールト・トレラント・システムを構成する必要がある。

6.3　潜在危険の同定

次の作用連鎖で同定される潜在危険を有する昇降リフタ等移動機構を設定する：

$$DRe \xrightarrow[3]{} ESa \xrightarrow[2]{} DRa \xrightarrow[1]{} La \xrightarrow[0]{} H(\cdot) \quad \cdots (6\text{-}5)$$

$$L(l)e \xrightarrow[2]{} He \xrightarrow[1]{} Ma \xrightarrow[0]{} H(\cdot) \quad \cdots\cdots\cdots (6\text{-}6)$$

$$L(l)e \xrightarrow[2]{} H(h)e \xrightarrow[1]{} H(h')a \xrightarrow[0]{} H(\cdot) \quad \cdots\cdots (6\text{-}7)$$

$$L(l)e \xrightarrow[1]{} H(h'')f \xrightarrow[0]{} H(\cdot) \quad \cdots\cdots\cdots\cdots (6\text{-}8)$$

記号の定義

(1) 系の要素

L　：リフタ
DR：リフタの駆動部
ES：駆動エネルギ源
H　：高齢作業者
M　：周辺機器・装置

(2) 作用鎖

$e \xrightarrow[3]{}$, $e \xrightarrow[2]{}$, $e \xrightarrow[1]{}$ ：存在形態形作用が要素間で授受される。

$a \xrightarrow[2]{}$, $a \xrightarrow[1]{}$, $a \xrightarrow[0]{}$ ：エネルギ伝播形作用が要素間で授受される。

$f \xrightarrow[0]{}$ ：機能不履行形作用が要素間で授受される。

(3) 要素の変化

$(\cdot)$　：高齢作業者の傷害
(l)　：リフタの停止故障
(h)　：高齢作業者の転落
(h')：位置エネルギの運動エネルギ変換
(h'')：高齢作業者に急病の発生

各作用連鎖に対して，次の災害のシナリオが想定される：

作用連鎖 (6-5) では，リフタの駆動部が作動する状態となり$[DRe \xrightarrow[3]{}]$，駆動エネルギ源よりエネルギが供給される$[ESa \xrightarrow[2]{}]$。すると，駆動部がリフタを動作させ$[DRa \xrightarrow[1]{}]$，動作中のリフタに作業者が押され$[La \xrightarrow[0]{}]$，傷害が発生する。

作用連鎖 (6-6) では，リフタが故障で途中停止し$[L(l)e \xrightarrow[2]{}]$，搭乗している作業者$[He \xrightarrow[1]{}]$に周辺装置が接触し$[Ma \xrightarrow[0]{}]$，傷害が発生する。

作用連鎖 (6-7) では，リフタが故障で途中停止し$[L(l)e \xrightarrow[2]{}]$，搭乗している作業者が降りようとした時$[H(h)e \xrightarrow[1]{}]$，転落して$[H(h')a \xrightarrow[0]{}]$，傷害が発生する。

作用連鎖 (6-8) では，リフタが故障で途中停止した時$[L(l)e \xrightarrow[1]{}]$，高齢作業者に急病が発生し$[H(h'')f \xrightarrow[0]{}]$，救出が遅れる。

以上の作用連鎖により同定される潜在危険を，それぞれ Hazard 1, Hazard 2, Hazard 3, Hazard 4 と定義する。

この他，リフタの倒壊や破壊による潜在危険も考えられるが，本報では省略する。

6.4 H-制御系の構成

Hazard 1 において，作用鎖$[ESa \xrightarrow[2]{}]$は，次のような制御連鎖から構成される H-制御系によりフェール・セーフ形解離で解離される：

$$H(h)u_i'' \xrightarrow[-6]{} SRu_j'' \xrightarrow[-5]{} PRu_k'' \xrightarrow[-4]{}$$
$$ARu_l' \xrightarrow[-3]{} ESa \overset{P_\xi}{\not\rightarrow_2} DR \quad \cdots\cdots\cdots\cdots (6\text{-}9)$$

記号の定義

(1) 系の要素

H ：高齢作業者
SR ：H-制御系検出部
PR ：H-制御系処理部
AR ：H-制御系出力部
ES ：リフタの駆動エネルギ源
DR ：リフタの駆動部

(2) 作用鎖

$u_i'' \xrightarrow[-6]{}$, $u_j'' \xrightarrow[-5]{}$, $u_k'' \xrightarrow[-4]{}$ ： 抑制作用 u_i'', u_j'', $u_k''(i,j,k \in 1,2,3,4,5,6)$ が要素間で授受される。

$u_l' \xrightarrow[-3]{}$ ：解離作用 u_l' $(l \in 1,2,3,4,5,6)$ が要素間で授受される。

$a \overset{P_\xi}{\not\rightarrow_2}$ ：作用a が解離原理P_ξ $(\xi \in 1,2,3)$ で解離される。

(3) 要素の変化

(h) ：危険域に作業者の存在

この H-制御系は典型的なインタロッキング機構を構成している。すなわち，高齢作業者がリフタと干渉する危険域に存在する時，H-制御系の検出部が高齢作業者からの抑制作用$[u_i'' \xrightarrow[-6]{}]$に基づき処理部に作用する$[u_j'' \xrightarrow[-5]{}]$。すると，出力部が，処理部からの抑制作用$[u_k'' \xrightarrow[-4]{}]$に基づき，リフタの動力源に作用して$[u_l' \xrightarrow[-3]{}]$，動力が遮断される。

この人間—機械系は，潜在危険集合h に関してフェール・セーフ・システムとなっている［定義 6-3］。

ここで，H-制御系は，定理 6-1 の意味で動力源の状態遷移を無秩序に行うことができる。したがって，制御連鎖 (6-9) を構成する抑制および解離作用鎖は，すべて単方向制御作用鎖として構成されるので，いずれもf''(機能停止形抑制作用) またはf'(機能停止形解離作用) とできる。その時，制御連鎖 (6-9) は次のように書き換えられる：

$$H(h)e'' \xrightarrow[-6]{} SRf'' \xrightarrow[-5]{} PRf'' \xrightarrow[-4]{}$$
$$ARf' \xrightarrow[-3]{} ESa \overset{P_1}{\not\rightarrow_2} DR \quad \cdots\cdots\cdots\cdots (6\text{-}10)$$

ここで，例えば検出部に故障$y(\in Y)$ が生じ，抑制作用鎖が反転すると，制御連鎖 (6-10) は次の反転連鎖を形成して，解離は実現されない：

$$H(h)e'' \xrightarrow[-6]{} SR(y)\bar{b} \xrightarrow[-5]{} PR\bar{b} \xrightarrow[-4]{}$$
$$AR\bar{e} \xrightarrow[-3]{} ESa \xrightarrow[2]{} DR \quad \cdots\cdots\cdots\cdots (6\text{-}11)$$

ここで，反転作用$[\bar{b} \xrightarrow[-5]{}]$は故障$y$に対するフェール・セーフ機能$FS$により次のようにフェール・セーフ形解離で解離され，再び元の作用鎖の解離が可能となる：

$$FSe' \xrightarrow[-6]{} SR(y)\bar{b} \overset{P_1}{\not\rightarrow_5} PRf'' \xrightarrow[-4]{}$$
$$ARf' \xrightarrow[-3]{} ESa \overset{P_1}{\not\rightarrow_2} DR \quad \cdots\cdots\cdots\cdots (6\text{-}12)$$

すると，系は潜在危険集合Yに関してフェール・セーフ・システムとなる［定義 6-3］。同様のことが処理部および出力部にもあてはまる。

ここで，制御連鎖 (6-9) で定義される H-制御系を C と置く。C に故障$y(\in Y)$ が発生してリフタが誤停止する潜在危険を検討する。故障yは次のように Hazard 2 を誘発する：

$$C(y)u_i \xrightarrow[3]{} L(l)e \xrightarrow[2]{} He \xrightarrow[1]{}$$
$$Ma \xrightarrow[0]{} H(\cdot) \quad \cdots\cdots\cdots\cdots\cdots\cdots (6\text{-}13)$$

Hazard 3 および Hazard 4 についても同様である。

作用連鎖 (6-13) において，作用u_i $(i \in 1, 2, 3, 4,$

5, 6) は，制御連鎖 (6-9) の解離作用u_l' ($l \in 1, 2, 3, 4, 5, 6$) が，

(イ)　$u_l' = u_6'$ ($\equiv f'$) の時，$u_i = u_6$ ($\equiv f$) となるので，作用連鎖 (6-13) は：

$$C(y)f \xrightarrow[3]{} L(l)e \xrightarrow[2]{} He \xrightarrow[1]{}$$
$$Ma \xrightarrow[0]{} H(\cdot) \cdots\cdots\cdots\cdots\cdots\cdots (6\text{-}14)$$

(ロ)　$u_l'(l = 1,2,3,4,or\ 5)$ の時，$u_i = u_5(\equiv e)$ となるので，作用連鎖 (6-13) は：

$$C(y)e \xrightarrow[3]{} L(l)e \xrightarrow[2]{} He \xrightarrow[1]{}$$
$$Ma \xrightarrow[0]{} H(\cdot) \cdots\cdots\cdots\cdots\cdots\cdots (6\text{-}15)$$

作用鎖$[C(y)f \xrightarrow[3]{}]$はフォールト・トレラント形解離により，作用鎖$[C(y)e \xrightarrow[3]{}]$はフェール・セーフ形解離によりそれぞれ解離される。

したがって，インタロッキング機構を Hazard 1 に対してフェール・セーフ・システムとした場合，Hazard 2 および Hazard 3, Hazard 4 に対してはフェール・セーフ・システムを構成できない。逆に，インタロッキング機構を Hazard 2 および Hazard 3, Hazard 4 に対してフェール・セーフ・システムとした時は，Hazard 1 に対してフェール・セーフ・システムを構成できない。また，すべての潜在危険に対してフォールト・トレラント・システムを構成することは原理的に可能である。すなわち，Hazard 1 に対して，Hazard 2, Hazard 3 および Hazard 4 はインタロッキング機構に関して相反潜在危険となっている。以上の議論の結果を Table 6.1 にまとめて示す。

6.5　定性的解析

全節までに潜在危険の同定と H-制御系の検討が行われた。本節では，それら潜在危険による毀損生成論理をフォールトツリー[30]を用いて定性（決定論）的に解析することにより最小カット集合を求める。

Table 6-1　Design tactics for H-control systems
H-制御系の基本設計方策

Plan	Fail-safe	Fault-tolerant
1	Hazard I	
2	Hazard 2, 3 and 4	
3		Hazard 1, 2, 3, and 4

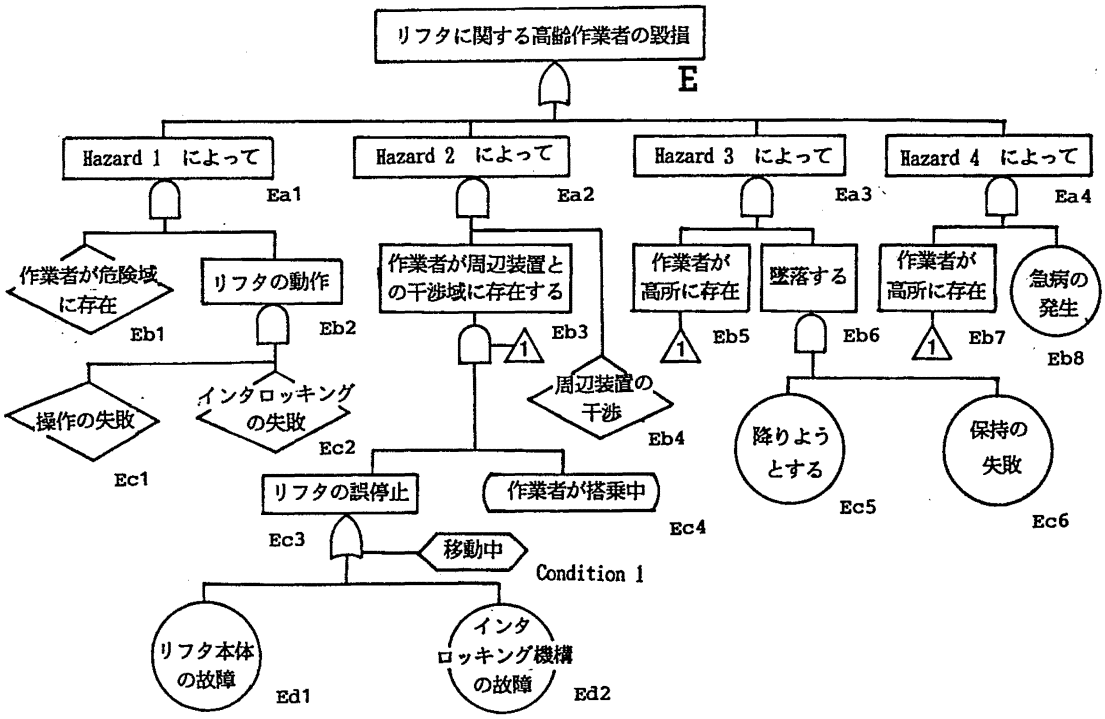


Fig. 6.5　A fault-tree for the loss of aged workers resulting from lifters.
昇降リフタによる高齢作業者の毀損に関するフォールトツリー

6.5.1 毀損生成論理のフォールトツリー

頂上事象を「リフタに関する高齢作業者の毀損」(E：事象識別記号，以下同様) とするフォールトツリーは，Fig. 6.5 のように展開される。

頂上事象「リフタに関する高齢作業者の毀損」(E) は，事象「Hazard 1」(Ea1),「Hazard 2」(Ea2),「Hazard 3」(Ea3),「Hazard 4」(Ea4) のいずれかにより発現する。

事象「Hazard 1」(Ea1) は,「作業者の危険域に存在」(Eb1) および「リフタの動作」(Eb2) 事象が共に成立することにより生起する。事象 Eb2 は,「操作の失敗」(Ec1) および「インタロッキングの失敗」(Ec2) 事象が共に成立することにより生起する。

事象「Hazard 2」(Ea2) は,「作業者が周辺装置と干渉する空間に存在する」(Eb3) および「周辺装置の干渉」(Eb4) 事象が共に成立することにより生起する。事象 Eb3 は,「リフタの誤停止」(Ec3) および「作業者がリフタへ搭乗して移動中」(Ec4) により生ずる。事象 Ec3 は,「リフタが移動中」(Condition 1) を条件として「リフタ本体の停止故障」(Ed1) または「インタロッキング機構の誤停止故障」(Eb2) のいずれかにより生起する。

事象「Hazard 3」(Ea3) は,「作業者が高所に存在」(Eb5) および「墜落する」(Eb6) 事象が共に成立することにより生起する。事象 Eb5 は，事象 Eb3 下の転出ゲート (No. 1) に連結される。事象 Eb3 は,「作業者がリフタから降りようとする」(Ec5) および「落ちないように保持することの失敗」(Ec6) が共に成立することにより生起する。

事象「Hazard 4」(Ea4) は,「高齢作業者が高所に存在」(Eb7) および「高齢作業者に急病の発生」(Eb8) が共に生ずることにより生起する。事象 Ea4 は，事象 Eb3 下の転出ゲート (No. 1) に連結される。

6.5.2 最小カット集合

最小カット集合を求めるアルゴリズムには，Semanderes のアルゴリズム，Fussell のアルゴリズム，および Vesely and Narum のアルゴリズム等があり，それぞれのアルゴリズムから ELRAFT，MOCUS，PREP などのコンピュータプログラムが開発・市販されている。

Fussell のアルゴリズムにより次の最小カット集合 C_i $(i = 1, 2, 3, \cdots, 7)$ が得られた：

$$C_1 = \{Eb1,\ Ec1,\ Ec2\} \cdots\cdots\cdots\cdots\cdots\cdots (6\text{-}16)$$

$$C_2 = \{Ed1,\ Ec4,\ Eb4\} \cdots\cdots\cdots\cdots\cdots\cdots (6\text{-}17)$$

$$C_3 = \{Ed2,\ Ec4,\ Eb4\} \cdots\cdots\cdots\cdots\cdots\cdots (6\text{-}18)$$

$$C_4 = \{Ed1,\ Ec4,\ Ec5,\ Ec6\} \cdots\cdots\cdots\cdots (6\text{-}19)$$

$$C_5 = \{Ed2,\ Ec4,\ Ec5,\ Ec6\} \cdots\cdots\cdots\cdots (6\text{-}20)$$

$$C_6 = \{Ed1,\ Ec4,\ Eb8\} \cdots\cdots\cdots\cdots\cdots\cdots (6\text{-}21)$$

$$C_7 = \{Ed2,\ Ec4,\ Eb8\} \cdots\cdots\cdots\cdots\cdots\cdots (6\text{-}22)$$

6.6 定量的解析

6.6.1 定量的評価のためのアルゴリズム

系の安全性を評価するうえで，最も一般的な指標は，毀損すなわちフォールトツリー頂上事象の統計的期待発生回数である。

前節で求めたフォールトツリー (Fig. 6.5) の頂上事象の任意の時刻 t に置ける単位時間当たりの統計的期待発生回数$w\{E\}_{(t)}$は，

$$w\{E\}_{(t)} = \sum_{i=1}^{7} w\{C_i\}_{(t)} \pm o\left(\sum_{\substack{i,j=1 \\ i\neq j}}^{7} w\{C_i \cap C_j\}_{(t)}\right) \cdots\cdots\cdots (6\text{-}23)$$

ここで，$w\{C_i\}_{(t)}$および$w\{C_i \cap C_j\}_{(t)}$ $(i, j = 1, 2, 3, \cdots, 7)$ は，(6-16) ～ (6-22) で与えられた最小カット集合およびその積集合の任意の時刻 t における単位時間当たりの統計的期待発生回数である。

6.6.2 基本事象の定量化と頂上事象の統計的発生率評価アルゴリズム

基本事象に関して次の仮定を置く：

(1) 作業者は，平均a_1[回／時間] 危険域に立ち入り，そこに平均b_1^{-1}[時間] とどまる。

(2)「操作の失敗」(Ec1) 事象の発生率は平均q_1[回／時間] (Constant) である。

(3) インタロッキング機構の MTTF (Mean Time To Failure) はa_2^{-1}[時間] (Constant) であり，故障状態は平均b_2^{-1}[時間] 後に修復される。

(4) インタロッキング機構の故障は，誤出力故障 (誤って出力してしまう故障) と欠出力故障 (出力すべき時に出力しない故障) からなり，イン

タロッキング機構のフェールセーフ度γを次のように定義する：

$\gamma \equiv$ 誤出力故障率／全故障率 ……(6-24)

ただし，

全故障率＝（誤出力故障率＋欠出力故障率）

(5) 作業者は，移動のためリフタへ平均a_3[回／時間] 搭乗し，その移動には平均b_3^{-1}[時間] 要する。

(6) リフタ本体の停止故障の MTTF はa_4^{-1}[時間] であり，故障状態は平均b_4^{-1}[時間] 後に修復される。

(7) 事象 Eb3 の条件下で周辺装置の干渉が発生する確率は，p_1 (Constant) である。

(8) リフタの誤停止の条件下で作業者がリフタから降りようとする確率は，q_2 (Constant) である。

(9) 作業者がリフタから降りようとする条件下で，落ちないように保持することに失敗する確率は，q_3 (Constant) である。

(10)高齢作業者のリフタに搭乗中の急病の発生率は，q_4 (Constant) である。

以上の条件より：

（イ）事象 Eb1 の生起は，定数発生率$a_1, b_1/(b_1 - a_1)$ [時間$^{-1}$] と修復率b_1の指数分布でモデル化される（仮定 1）。

（ロ）事象 Ec2 の生起は；①インタロッキング機構を Plan 1 (Table 6.1) とすると，定数発生率γa_2と修復率b_2の指数分布で，② Plan 2 では，定数発生率$(1-\gamma)a_2$と修復率b_2の指数分でそれぞれモデル化される（仮定 3,4）。

（ハ）事象 Ed1 は，定数発生率a_4と修復率b_4の指数分布でモデル化される（仮定 6）。

（ニ）事象 Ed2 の生起は；① Plan 1 では，定数発生率$(1-\gamma)a_2$と修復率b_2の指数分布で，② Plan 2 では，定数発生率γa_2と修復率b_2の指数分布でモデル化される（仮定 3,4）。

（ホ）事象 Ec4 の生起は，定数発生率$a_3 b_3/(b_3 - a_3)$と修復率b_3の指数分布でモデル化される（仮定 5）。

（ヘ）さらに，実際に最小カット集合が成立するためには，事象 Ec2 が Eb1 に，事象 Ec4 が Ed1 および Ed2 に，事象 Ec4 が Eb8 にそれぞれ先立って生起しなければならない。

基本事象の発生順序に依存するフォールトツリー頂上事象の統計的発生回数評価アルゴリズムは，佐藤等によって研究されている[15,16]。

系を T 時間運用した場合の頂上事象の統計的期待発生回数 W(0,T) は，式 (6-23) から：

$$W(0,T) = \int_0^T w\{E\}_{(t)} dt \quad \cdots\cdots\cdots\cdots (6\text{-}25)$$

これは，佐藤のアルゴリズム[15,16]を用いて：

① Plan 1 に対して；

$$\begin{aligned} W(0,T) &= \gamma q_1 a_2 a_1 (T - 1/b_2)/b_2 \\ &+ p_1 a_3 a_4 (T - 1/b_3)/b_3 \\ &+ (1-\gamma) p_1 a_3 a_2 (T - 1/b_3)/b_3 \\ &+ q_2 q_3 a_3 a_4 (T - 1/b_3)/b_3 \\ &+ (1-\gamma) q_2 q_3 a_3 a_2 (T - 1/b_3)/b_3 \\ &+ q_4 a_3 a_4 (T - 1/b_3)/b_3 \\ &+ (1-\gamma) q_4 a_3 a_2 (T - 1/b_3)/b_3 \end{aligned}$$

ただし，

$$a_i/b_i \ll 1, T > b_i \ (i = 1,2,3,4) \cdots\cdots\cdots (6\text{-}26)$$

② Plan 2 に対して；

$$\begin{aligned} W(0,T) &= (1-\gamma) q_1 a_2 a_1 (T - 1/b_2)/b_2 \\ &+ p_1 a_3 a_4 (T - 1/b_3)/b_3 \\ &+ \gamma p_1 a_3 a_2 (T - 1/b_3)/b_3 \\ &+ q_2 q_3 a_3 a_4 (T - 1/b_3)/b_3 \\ &+ \gamma q_2 q_3 a_3 a_2 (T - 1/b_3)/b_3 \\ &+ q_4 a_3 a_4 (T - 1/b_3)/b_3 \\ &+ \gamma q_4 a_3 a_2 (T - 1/b_3)/b_3 \end{aligned}$$

ただし，

$$a_i/b_i \ll 1, T > b_i^{-1} \ (i = 1,2,3,4) \cdots\cdots (6\text{-}27)$$

6.6.3　系の最適設計

ここで，インタロッキング機構の基本設計上，Plan 1 と Plan 2 でどちらが優れているかを検討しよう。

式 (6-26) と式 (6-27) はそれぞれ次のように変形される：

$$W(0,T)_{\text{Plan 1}} = \gamma X + (1-\gamma) Y + Z \quad \cdots (6\text{-}28)$$

$$W(0,T)_{\text{Plan 2}} = (1-\gamma)X + \gamma Y + Z \quad \cdots(6\text{-}29)$$

ここで,

$$X = q_1 a_2 a_1 (T - 1/b_2)/b_2$$

$$Y = p_1 a_3 a_2 (T - 1/b_3)/b_3 + q_2 q_3 a_3 a_2 (T - 1/b_3)/b_3 + q_4 a_3 a_2 (T - 1/b_3)/b_3$$

$$Z = p_1 a_3 a_4 (T - 1/b_3)/b_3 + q_2 q_3 a_3 a_4 (T - 1/b_3)/b_3 + q_4 a_3 a_4 (T - 1/b_3)/b_3$$

通常, $\gamma \ll 1$ であるから, 式 (6-28) および式 (6-29) より,

(イ) $X > Y$では,

$$W(0,T)_{\text{Plan 1}} < W(0,T)_{\text{Plan 2}}$$

(ロ) $Y > X$では,

$$W(0,T)_{\text{Plan 1}} > W(0,T)_{\text{Plan 2}}$$

となる。

頂上事象の発生回数は少ない方が望ましい。そこで, $X > Y$なら Plan 1 が, $Y > X$なら Plan 2 が系の優れた設計法となる。

6.6.4 他の系とのリスクの比較

前節までに導入した$q_1, a_2, a_1 \cdots$など基本事象の統計量は, 実際の系の設定条件や使用環境条件によって異なってくる。したがって, 新しい系の設計にあたっては, 安全性評価アルゴリズムの検討のみにとどまることなく, それら統計量に関するデータの収集も重要となる[31,32]。安全性評価のアルゴリズムは, どのようなデータを収集すべきかをも示唆してくれる。ここでは, 次のような平均的と考えられる系の設定条件に対して残存リスクを評価する:

$a_1 = 1$ [回／時間], $b_1^{-1} = 3.6$ [秒]
$q_1 = 2 \times 10^{-3}$ [回／時間]
$a_2^{-1} = 10^4$ [時間], $b_2^{-1} = 30$ [分]
$\gamma = 10^{-4}$
$a_3 = 1$ [回／時間], $b_3^{-1} = 36$ [秒]
$a_4^{-1} = 10^4$ [時間], $b_4^{-1} = 30$ [分]
$p_1 = 10^{-3}$
$q_2 = q_3 = 10^{-2}$
$q_4 = 3 \times 10^{-7}$

これより,

$$X = 10^{-7} \times (T - 1/2),$$

$$Y = 1.1 \times 10^{-9} \times (T - 10^{-2})$$

を得るので, Plan 1 が優れた設計となる。Plan 1 を採用した時の系の運用時の極大残存リスク (生ずる災害のすべてを死亡災害とした残存リスク) R_{MAX}は, 式 (6-28) より:

$$R_{\text{MAX}} = W(0,1)_{\text{Plan 1}} = 2.2 \times 10^{-9}$$

[DEATH/HOUR · COMPONENT]

これは, 代表的系の運用時残存リスク：商用発電原子炉の苛酷事故 10^{-9} [ACCIDENT/HOUR · COMPONENT]; 産業用ロボットに打たれる事故 10^{-9} [ACCIDENT/HOUR · COMPONENT]; 自動車の死亡事故 10^{-7} [DEATH/HOUR · COMPONENT] などと比較しても遜色がないといえる。

6.7 結　言

本報では, 昇降リフタ等移動機構の安全性についてその運用時を対象として評価した。まず, 複雑な系におけるフェール・セーフ・システムについて, 潜在危険集合の概念を導入して定義し, その構成条件を明らかにした。次に, A-C モデルを用いて当該作業系に生ずる潜在危険を同定し, H-制御系 (インタロッキング機構) を基本構成して各潜在危険集合に対するフェール・セーフ・システムの適用性を明らかにした。そして, 系の定性的および定量的解析を行い, インタロッキング機構の最適設計方針決定の方法を示した。さらに, 系の具体的な設計使用を設定して残存リスクを求めた。これを他の代表的な系の残存リスクと比較しても, 当該作業系の安全性に遜色がないことが分かった。

(平成 2 年 11 月 30 日受理)

参考文献

1) H.W. Heinrich, D. Petersen and N. Roos: Industrial Accident Prevention, McGRAW-

HILL, BOOK CO., New York, p.130, (1980)
2) H. Ozog: Hazard identification, analysis and control, Hazard Prevention, May/June, pp.11–18, (1985)
3) 佐藤：産業安全今後の課題—機械システムに求められる多相安全設計—, 機械学会誌, Vol. 93, No. 863, p.848, (1990 Oct.)
4) 奥村：コンピュータを用いたフェール・セーフなシステム, 情報処理, Vol. 22, No. 9, p.863, (1981)
5) JIS ハンドブック安全, 日本規格協会, 東京, p.21, (1988)
6) 平山, 渡辺, 浦野：フェールセーフ理論系の構成理論, 電子通信学論文集, Vol. 52(C), No. 1, p.33, (1969)
7) 佐藤, 井上：ロボットの安全性について, 機械学会誌, Vol. 90, No. 827, pp.105–109, (1987)
8) W.G. Johnson: MORT Safety Assurance Systems, Marcel Dekker, INC., New York, p.247, (1980)
9) H.E. Roland and B. Moriarty: System Safety Engineering and Management, John Wiley & Sons, Inc., New York, p.6, (1983)
10) 佐藤, 井上：人間—ロボット系の安全性評価（作用—変化と作用連鎖モデルによる潜在危険の同定）, 機械学会論文集（C 編）, Vol. 51, No. 468, pp.2188–2195, (1985)
11) Y. Sato and K. Inoue: Safety assessment of human-robot systems (Hazard identification based on the action-changes and action-chains models) Bull. JSME, Vol. 29, No. 250, pp.1356–1361, (1986)
12) H. Kumamoto, Y. Sato and K. Inoue: Engineering Risk and Hazard Assessment (Hazard identification and safety assessment of human-robot systems), CRC Press, Inc., Boca Roton, Florida, pp.61–80, (1988)
13) 佐藤, 井上, 熊本：人間—ロボット系の安全性評価（災害発生機構の解析のための論理モデル—その 1）, 機械学会論文集（C 編）, Vol. 52, No. 474, pp.823–832, (1986)
14) Y. Sato, K. Inoue and H. Kumamoto: The safety assessment of human-robot systems (Logic models for the analysis of the accident-causing mechanisms-Part 1), Bull. JSME, Vol. 29, No. 256, pp.3618–3625, (1986)
15) 佐藤, 井上, 熊本：人間—ロボット系の安全性評価（順序依存形故障論理の定量化について）, 機械学会論文集（C 編）, Vol. 52, No. 475, pp.1110–1117, (1986)
16) Y. Sato, K. Inoue and H. Kumamoto: The safety assessment of human-robot systems (On the quantification of consecutive failure logic), Bull. JSME, Vol. 29, Nol. 257, pp.3945–3951, (1986)
17) 佐藤：新技術を用いたシステムに生ずる潜在危険の評価, RIIS-SRR-86, No. 1, pp.103–117, (1986)
18) Y. Sato, H. Kumamoto and K. Inoue: On hazard identification and analysis of human-robot systems, Proc. Japan-U.S.A. Symp. Flexible Automation, pp.679–684, Osaka, (1986)
19) 佐藤, 井上, 熊本：人間—ロボット系の安全性評価（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）, 機械学会論文集（C 編）, Vol. 52, No. 482, pp.2754–2763, (1986)
20) Y. Sato, K. Inoue and H. Kumamoto: The safety assessment of human-robot systems (Evaluation of hazard control measures for an industrial robot handling work pieces), JSME Intr., Jour., Vol. 30, No. 260, pp.350–356, (1987)
21) Y. Sato, K. Inoue and E.J. Henley: Hazard assessment of industrial-robots, Proc. U.S.A.-Japan Symp. Flexible Automation, Vol. 2, pp.703–707, Minneapolis, (1988)
22) 佐藤, 井上：人間—ロボット系の安全性評価（潜在危険制御系の構成原理）, 機械学会論文集（C 編）, Vol. 54, No. 505, pp.2164–2173, (1988)
23) 佐藤, 井上：ヒューマン・インターフェースにおける安全計画, 第 4 回 HIS 論文集, pp.215–225, 東京, (1988)
24) Y. Sato, K. Inoue and E.J. Henley: The safety assessment of human-robot systems (Architectonic Principles of hazard-control

systems), JSME Intr. Jour., Vol. 32, Nol. 1, pp.67–74, (1989)

25) Y. Sato, E.J. Henley and K. Inoue: Architectionics of hazard-controls systems for robotics, Proc. Intr., Conf. Advanced Mechatronics, pp.415–420, Tokyo, (1989)

26) 佐藤, 井上:人間—ロボット系の安全性評価 (移動ロボットにおける潜在危険制御系の構成について), 機械学会論文集 (C 編), Vol. 55, No. 518, pp.2663–2671, (1989)

27) Y. Sato and K. Inoue: On the quantification of consecutive failure logic, Procs. Intr. Symp. Reliability and Maintainability, Tokyo, pp.552–557, (1990) June

28) Y. Sato, E.J. Henley and K. Inoue: An action-chain model for the design of hazard-control systems for robots, IEEE Trans. Reliab., Vol. 39, No. 2, pp.151–157, (1990)

29) Y. Sato, E.J. Henley and K. Inoue: Structuring hazard-control systems for autonomous mobile robots, Proc. Japan-U.S.A. Symp. Flexible Automation, Vol. 1, pp.111–118, Kyoto, (1990) July

30) 井上監修:FTA 安全工学, 日刊工業新聞社, 東京, (1979)

31) IEEE Std 500, Reliability Data, p.115, (1983)

32) 厚生省大臣官房統計情報部編:人口動態統計, (財) 厚生統計協会, Vol. 1, pp.179–183, (1990)