Research Reports of the Research Institute
of Industrial Safety, RIIS-RR-90, 1990
UDC 005-614-72.011.1-66.0

固有フェール・セーフ・システムの構成と多相安全設計について*

佐 藤 吉 信**

On the Structuring of an Inherently Fail-Safe System and Multiphasic Safety Design*

by Yoshinobu SATO**

Abstract: System safety engineers have developed and utilized the methods for identificsation, analysis and assessment of hazards and risks produced in a designed and assumed system, such as hazard-operability studies and fault-tree analysis. While, we have considered that the designing of systems involving hazard-control systems is a job as an expert in each technological field. In general, the systematization of designing is difficult because we can not express mathematically the knowledge of systems syntheisis.

Recently since systems are getting more complicated and flexible, the cause of large percentage of major hardware-failures that led to accidents has been hardly established. If the cause of accidents is unpredictable, this suggests that the most productive way of increasing safety and ameliorating risk is to mitigate the effect of an accident, i,e., to reduce its consequences. An automobile seat-belt, for example, does not prevent accidents, it, however, reduces risk of injury from an accident.

A hazard-control system (: the system which prevents damage, given that failures have occurred) materializes the seat-belt approach. The author has made efforts toward categorizing and systematizing the design of hazard-control systems in terms of an action-change and action-chain (A-C) model for hazard-control.

This paper systematizes the structuring of an inherently fail-safe system and describes the systematic procedure for multiphasic safety design based on the A-C model. The paper obtains the following results:

1. An entropy model for system state division is proposed. In the entropy model, the entropy of system elements with regard to energy, information, disorganization of shape, etc. divides system state into two states, ordered and disordered state. The ordered state evokes ordered-state actions between system elements. Disordered state produces a function-failure action. The entropy model clarifies the physical background of the A-C model. Next, the mode of system-state transition is divided into two modes, ordered and disordered transition. Only the ordered-state system-elements materialize the ordered transition. Then, an inherently fail-safe system is established by the following definition; if a failure in a system brings about a disordered system-transition from ordered state and if this transition prevents a damage which could be caused by a hazard, then the system is an inherently fail-safe system with regard to the failure and the hazard.

* この論文の一部の内容については，日本機械学会誌 Vol. 93, No. 863, 846 ～ 851 ページ，配管技術 Vol. 33, No. 1, 51 ～ 55 ページに掲載した。
** 機械研究部，Mechanical Safety Research Division

2. The paper generalizes hazard-restraint strategy as the following four principles; 1) exclusion or elimination of undesirable action source, 2) prevention of undesirable changes, 3) controls which prevent a system from transferring to a damage-producing systems phase, and 4) controls which transfer a system from a damage-producing system phase to a damaga-avoidable one. Principles 3) and 4) are materialized by hazard-control systems. Designing of fail-safe and fault-tolerant structures into hazard-control systems is hazard-restraint tactics. Multiphasic safety design is the implementation of the hazard-restraint strategy and tactics.

3. The paper defines the rules for structuring a fail-safe, fault-tolerant, and inherently fail-safe systems, and establishes the method of elaborate and systematic multiphasic safety design.

4. Examples involving a chemical batch-processing plant demonstrates the new technology and confirms its effectiveness.

Key Words: A-C model, Multiphasic safety design, Inherently fail-safe system, Fail-safe system, Fault-tolerance system, Chemical processing plant, Entropy model.

1. 緒　言

システム安全 (System Safety) の分野では，フォールト・ツリー・アナリシス (Fault-tree Analysis) やハザード・オペラビリティ・スタディー (Hazard-Operability Study) などの方法論が展開され，航空・宇宙開発，原子力開発，化学プラント，産業用ロボットなど現実の系に適用されてきた[1−4]。これらの方法論は，いずれも与えられた系に対して潜在危険の同定や解析，あるいはリスクの評価を行うためのものである。これにより，系の安全上の弱点あるいは改善点が指摘され，残存リスクが評価される。

一方，系の設計は，個々の技術体系におけるエキスパートの知識の集積として行われている。一般的に，それらの知識は，数学的に表現されにくいという特徴があるため，エキスパート・システムなど従来とは異なる方法論を用いた知識表現が試みられている[5]。事故を防止あるいは回避するための保護系 (Protection Systems)，防護系 (Safeguard Systems)，インターロッキング装置 (Interlocking Devices) などを含めた全般的な系の設計は各分野のエキスパートに任されてきたため，設計すなわち系の合成問題 (Systems Synthesis) にシステム安全が積極的に関与する機会は，ほとんどなかったといってよいであろう。

生産システム，交通システム，化学プラントなどの系は，ますます巨大化，複雑化，フレキシブル化しており，それらの系の計画・設計段階で安全性を先取りすることの重要性が増大している。例えば，次世代の商業用原子炉として固有安全炉 (Innovative Sodium-cooled Inherently Safe Fast Reactor)[6]が提案されている。固有安全炉にみるように，工学的な方法に頼らず，事象の自然な収束性を利用して事故を回避する設計方法を他の産業分野にも適用するのは安全上重要な方策の一つである。この実現のためには，先ず，固有安全の概念を明確にして，その構成法則を一般化する必要がある。それらの問題は全てシステム合成問題に帰着し，そのシステムズ・アプローチの展開がシステム安全の重要な課題であると考えられる。

筆者等は「作用－変化と作用連鎖モデル（Action-change and Action-chain Model，以下 A-C モデル)」を提案して，潜在危険制御系の構成問題に対するシステムズ・アプローチの確立を図ってきた[7−15]。本報では，A-C モデルを拡張して：

1) 系の状態遷移にエントロピ・モデルを導入して，固有安全すなわち固有フェール・セーフ・システム (Inherently Fail-safe System) を一般化して定義する；
2) 複雑な系の多相安全設計 (Multiphasic-safety Design) が大局的多相安全設計と局所的多相安全設計とに体系化されることを示す；
3) 固有安全すなわち固有フェール・セーフ・システムおよび工学的フェール・セーフ・システムの構成法則を明らかにする；

ことにより，システム合成問題のシステムズ・アプローチの確立に寄与することを目的としている。

なお，理論の展開に際しては，バッチ方式の化学プラントを例にあげて具体的な理解をはかる。

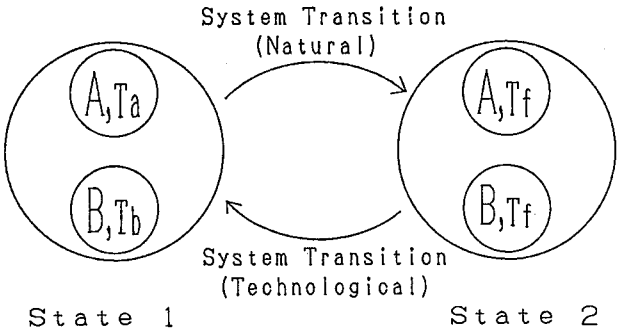

Fig. 1　Transitions of system state
システムの状態遷移

2. 系の状態遷移と固有フェール・セーフ・システム

2.1 エントロピ・モデル

系を構成する要素の毀損生成過程における状態変化は，電圧や温度あるいは運動量のような連続した物理量のみではなく，例えば，形状，情報なども含む。ここで，いくつかの要素から構成されるある系において，2組の要素からなる1個の閉じた系を想定することができる。この閉じた系は，情報，エネルギ，あるいは形状や物事の秩序性などに関してそれぞれエントロピ（Entropy：秩序性の数学的表現）を有する。

この閉じた系は，秩序性に関して2つの状態を取りうる。任意のエントロピに関してある基準値を設定したとき，その基準値よりも小さいエントロピ状態すなわち秩序的状態 (Ordered State) および基準値よりも大きなエントロピをもつ無秩序的状態 (Disordered State) である。

例として，Fig. 1に示すような，2つの要素A，Bからなる熱的に閉じた系を想定する。要素AとBは，それぞれ温度がT_aおよびT_bであるものとする。これを状態1(State 1) と呼ぶ。自然の成り行きにまかせると，要素A，B間で熱交換が行われ，十分な時間の後に両者は等しい温度T_fを持つとみなせるようになる。これを状態2(State 2) と呼ぶ。

状態1から状態2へと系が遷移する過程で，例えば要素AとBの間の温度差がある一定量T_d以上のとき，両者の間である量以上の熱エネルギの交換が行われる。もし熱エネルギの交換能力の観点から，温度差T_dを境界として，系をエントロピ的に分割するなら，温度差がT_d以上のとき，系は秩序的状態（所定の熱エネルギ交換能力のある状態）にあり，温度差がT_dよりも小さいなら系は無秩序的状態（所定の熱エネルギ交換能力がない状態）とみなすことができる。ここで，例えば，温度差がT_d以上のときに行われる熱エネルギの交換による事故を想定すると，秩序的状態が事故を発生させうる状態であり，無秩序的状態が事故を回避する状態となる。

2.2 固有フェール・セーフ・システム

物理的世界における事象の自然な収束性とは，事象がエントロピに関して秩序的状態から無秩序的状態へと遷移することと同義である。そこで，前節における状態1から状態2への遷移を（物理的世界に）固有な状態遷移 (Inherent System-transition) とよぶことにする。一方，状態2から状態1への遷移は，人工的 (Artificially) あるいは技術的 (Technologically) にのみ可能である。そこで，これを工学的な状態遷移とよぶ。

以上の観点から，固有フェール・セーフ・システムを次のように定義する：

［定義　1］もし，系におけるある変化（故障，異常，失敗，エラーなど）が，固有な状態遷移によって系を無秩序的状態へと遷移させ，かつ，これにより，ある潜在危険による毀損の生成が抑制されるならば，この系は，その変化とその潜在危険に関して固有フェール・セーフ・システムである。

2.3 作用とその物理的背景

系の秩序的な状態は，2つの要素間に，エネルギ（機械的，熱的など）の伝播作用，情報（信号，メッセージなど）の伝達作用，物質の転移（移動）作用，必要とされるエネルギ・情報・物質の供給を阻害する作用，形状や力あるいは質量などによる作用を引き起こす能力を有する。

一方，系の無秩序な状態では，その秩序的な状態で行われるはずであったエネルギの伝播，情報の伝達，物質の転移（移動），供給の阻止，形状や力あるいは質量などによる作用，及びそれらの複合された作用すなわち機能の履行が不可能となる。つまり，系の無秩序な状態では，2つの要素間において機能不履行作用が生ずる。

系の秩序状態と作用との関係を作用エントロピ・モデルということとする。すると，次ぎの系を得る。

［系　1］作用は，作用エントロピ・モデルから次のように分類・体系化される。

1. 秩序状態作用
   a. エネルギ伝播形
   b. 情報伝達形
   c. 作因物転移形
   d. 供給阻害形
   e. 存在形態形
2. 無秩序状態作用
   f. 機能不履行形

3. プラントの潜在危険同定例

Fig. 2 に示すようなあるバッチ・プラントの反応器では，設計・運用に欠陥があると，いくつかのタイプの災害が発生する可能性が考えられる。その一つとして，次のような災害に至るシナリオが考えられる：

反応器 R 内の反応物質群（気相状態の物質も含む）M の発熱反応により反応器内温度および圧力が上昇し，通常の反応温度θ_1を超えて温度がθ_2に達すると反応器が破壊することがある。反応過程で生成される反応生成物は，著しい毒性を有し，流出すると，プラント作業者や住民などに被害が発生する。

この特定の災害シナリオ（潜在危険：Hazard）は，A-C モデルにより，次の作用連鎖で同定される：

$$M(m)a \xrightarrow[3]{} M(m')\ a \xrightarrow[2]{} M(m'')\ a \xrightarrow[1]{}$$
$$R(\cdot)c \xrightarrow[0]{} E(\cdot) \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots (1)$$

系の要素とその変化

$M(m)$: 反応物質群（気相状態も含む）Mとその反応(m)
$M(m')$: 反応物質群とその温度θ_1への上昇(m')
$M(m'')$: 反応物質群とその温度θ_2への上昇(m'')
$R(\cdot)$: 反応器Rとその破壊$(\cdot)$
$E(\cdot)$: 被災者Eとその被害$(\cdot)$

作用の授受

$a \xrightarrow[3]{}$, $a \xrightarrow[2]{}$, $a \xrightarrow[1]{}$：エネルギ伝播形作用の授受
$c \xrightarrow[0]{}$：作因物転移形作用の授受

すなわち，反応物質群の発熱により$[M(m)a \xrightarrow[3]{}]$反応器内温度が$\theta_1$となり，さらに発熱反応の継続により$[M(m')a \xrightarrow[2]{}]$，温度が$\theta_2$となる。この結果，反応物質群の圧力・熱エネルギが反応器に作用して$[M(m'')a \xrightarrow[1]{}]$反応器を破壊する。これにより，反応器が有毒な物質を外部に放出するため$[R(\cdot)c \xrightarrow[0]{}]$，近傍にいた被災者 E が被災する。

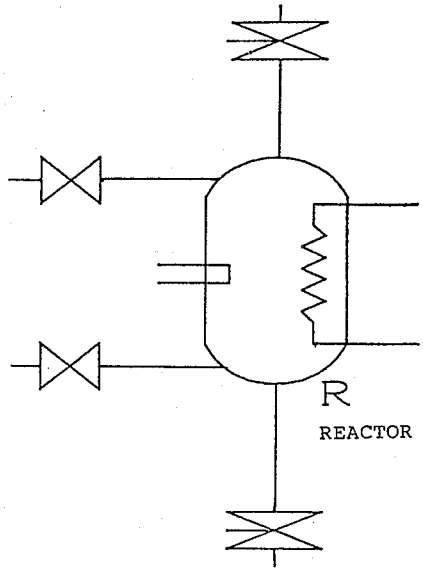

Fig. 2　A chemical reactor
反応器

系は，作用連鎖 (1) で同定される潜在危険を有し，この潜在危険を潜在危険 1 と定義する。

4. 潜在危険の抑制と多相安全設計

4.1　潜在危険抑制過程

A-C モデルから，潜在危険の抑制過程は，化学プラントに限らず，一般に次の潜在危険抑制原理として体系化される[16]：

(1) 作用源の排除
(2) 変化の抑制
(3) 系の毀損生成相遷移の禁止
(4) 系の毀損生成相からの遷移

潜在危険抑制過程 (1) は，人間または機器に望ましくない作用を行う要素を系から排除・隔離，またはそのエネルギー状態や化学的性質などが作用源とならない状態に限定して使用することを意味する。

(2) は，要素が機能を維持し，危険側への逸脱した挙動を行わないようにすることである。余裕をもった条件による系の設計・運用，品質管理，高信頼性要素の採用，高安全余裕，保全による信頼性の維持，教育・訓練によるヒューマン・エラーの防止，フール・プルーフなどによる危険側への変化の防止などによって達成される。

(3) における系の相とは，系の要素の状態モードにより定まる系の相を意味する。反応器が反応開始以前のモードにあるうちに，反応器の温度制御系が正常でないこと，又はそのまま反応開始後のモードへ遷移すると故障が生ずることが診断または予測できれば，系のこのモードへの遷移を禁止することができる。これは，異常診断，異常予測などによって達成される。

(4) は，系がすでに毀損の発生する相にあるとき，系の要素を制御することにより，毀損が回避される方向に系の状態を遷移させることを意味する。

潜在危険抑制原理 (3)，(4) は，ある条件下で系に発現しつつある作用連鎖をその途中で解離することによって災害を回避する機構，すなわち潜在危険制御系を構成することによって実現される。

4.2　多相安全設計

設計の各局面における意志決定問題すなわち多相安全設計問題は，各潜在危険抑制原理を現実化したものとして把握される。すなわち，「作用源を排除」する設計の実施を最も基本的な意志決定問題として，順次，「変化の抑制」，「系の毀損生成相遷移の禁止」，「系の毀損生成相からの遷移」の実施が連なる。このように，大局的な観点から 4 局面の設計方針を逐次策定し実行する活動を大局的多相安全設計 (Strategic Multiphasic-Safety Design) ということとする。

一方，「系の毀損生成相遷移の禁止」，「系の毀損生成相からの遷移」を実現する方策は，潜在危険制御系の構成によって実現されることはすでに述べた。潜在危険制御系は，フェール・セーフ・システム化，冗長化あるいは多重化（すなわち多重防護の考え方を実現させること）が可能である。それらの方策は，大局的方策内での局所的な多相安全設計であるとみなせるので，局所的多相安全設計 (Tactical Multiphasic-Safety Design) ということとする。

4.3　バッチ・プラントの大局的多相安全設計

前節で述べた方法論に従えば，バッチ・プラントの大局的多相安全設計例として次のようなものがあげられる：

(1) 作用源の排除設計
- ① 毒性物質を生成しないプロセスあるいは原材料の開発。
- ② プラント／反応器の隔離，無人化，遠隔操作。
- ③ 毒性物質は生成するが，発熱量の少ないプロセスまたは原材料の開発。

これらが実現しないとき，

(2) 変化の抑制と修復に適した設計
- ④ 反応器などの構造・強度および運転条件の安全余裕の拡大。
- ⑤ プラントを構成する個々のハードウエアおよびソフトウエアの高信頼性設計。
- ⑥ プラントの許容運転能力とバッチ処理における反応条件（反応速度，発熱量，生成物質など）の仕様を明確にする設計と運転管理。
- ⑦ オペレータのヒューマン・エラーを防止する操作盤またはインターフェースの設計。
- ⑧ 保全条件の明確化と保全作業を考慮した設計。

これらに加えて，

(3) 系の状態遷移を抑制する制御系の設計
- ⑨ プラントの異常を予測・検出してプロセスを開始させないようにするプラント異常診断インタロッキング系の構築。
- ⑩ 反応中の缶内温度をθ_1（$< \theta_2$）以下に制御する内部冷却系の構成。

さらに，リスク解析の結果，これらだけでは十分でないと評価されたとき，

(4) 系の状態を遷移させる制御系の設計
- ⑪ 緊急外部冷却系の構成。
- ⑫ 反応抑制剤による反応速度制御系など，緊急反応抑制系の構成。

ここで，⑨～⑫の各系は，4.1 節で述べた潜在危険制御系であり，局所的多相安全設計の対象となる。次章以下においては，局所的多相安全設計のシステムズ・アプローチについて論ずる。

5.　フェール・セーフ／フォールト・トレランス・システム

5.1　定義と構成条件

潜在危険制御系は，これまでに参考文献 7) ～ 15) などにその構成定理として体系化されてきた。本報告における以降の論理の展開において，予備知識として必要とされる定理を以下に述べる。各定理の記述に用いられる述語は，参考文献 7) に定義されている。

［定理　1］a, b, c, d または e 形の作用鎖は，解離原理P_1，P_2，P_3のいずれかにより，f形の作用鎖は解離原理P_4によってのみ解離される。

［定理　2］解離原理P_1, P_2, P_3はa', b', c', d', e'（および／または）f'形の解離作用により実現され，解離原理P_4は，g' & g''形の解離作用によってのみ実現される。

［定理　3］a', b', c', d', e', g' & g''形の解離作用，またはa'', b'', c'', d'', e''形の抑制作用が反転すると機能不履行($\overline{f}$) 形の反転作用が生じ，$f'(f'')$形の解離（抑制）作用が反転すると$\overline{a}$, $\overline{b}$, $\overline{c}$, $\overline{d}$, $\overline{e}$形の反転作用のうち少なくともひとつが生ずる。

［定理　4］抑制連鎖を構成する任意の要素に引金変化が発生すると，他に引金変化が発生していない条件下で，その要素からの抑制作用鎖が反転することにより，そこから反転連鎖が生成され，解離は実現されない。

［定理　5］$\overline{a}$, $\overline{b}$, $\overline{c}$, $\overline{d}$, $\overline{e}$形の反転作用鎖は解離原理P_1，P_2またはP_3によって，$\overline{f}$形の反転作用鎖は解離原理P_4によってのみ解離される。

［定理　6］定理４において生じた反転連鎖中のある反転作用鎖が解離されると，他に引金変化および反転連鎖が生じていない条件下で，そこから部分的に抑制連鎖が復活し，作用連鎖の解離が再び可能となる。

［定理　7］単方向制御作用鎖は任意の解離または抑制作用鎖によって構成され得るが，複方向制御作用鎖は$f'(f'')$形の解離（抑制）作用鎖では構成できない。

さて，フェール・セーフ・システムおよびフォールト・トレランス・システムは，個々の工学分野において独自に定義されており，電子回路，機械工学，化学工学，人間工学など各種工学体系を包括する共通基盤に立って定義されていないため，各分野ごとに概念の不整合があり，曖昧な術語となっている[17]。

そこで，各種工学体系を包括するA–Cモデルを基盤として，システム工学的観点からフェール・セーフ・システムおよびフォールト・トレランス・システムを次のように定義する：

［定義　2］系において，ある変化（ある故障）が，ある潜在危険（作用連鎖または反転連鎖）を発現させることにより，ある要素にある毀損をもたらしうるものとする。このとき，もし，潜在危険制御系が，作用鎖（または反転作用鎖）を：1) 解離原理P_1(作用源の制御)，P_2(作用径路の制御）またはP_3(作用源と作用経路の両者の制御）により解離することにより，その毀損を回避するなら，この系は，その変化（その故障）と潜在危険に関してフェール・セーフ・システムである；2) 解離原理P_4(不履行機能の代替制御)で解離し，その毀損を回避するなら，この系は，その変化（その故障）と潜在危険に関してフォールト・トレランス・システムである。

定義１，系１および定義２より，次の系を得る：

［系　2］固有フェール・セーフ・システムは，フェール・セーフ・システムの特別な場合，すなわち作用源や作用径路の制御が固有な状態遷移によって行われる場合である。

秩序状態作用（反転作用）鎖は解離原理P_1，P_2またはP_3で解離可能であり，無秩序状態作用（反転作用）鎖は解離原理P_4によってのみ解離可能であるので［系１および定理１］，次のフェール・セーフ／フォールト・トレランス・システム構成則を得る：

［構成法則　1］系にフェール・セーフ・システムを構成可能とする必要条件は，作用連鎖（反転連鎖）が少なくとも１本の秩序状態作用（反転作用）鎖を含むことである。それ以外では，フォールト・トレランス・システムを構成しなければならない。

5.2　状態遷移の秩序性

大局的多相安全設計過程 (4) を実現するには，潜在危険制御系が系の状態遷移を行なわなければならない。

差し迫った危険が，系の全体あるいは部分のエネルギ状態，形状，時空上の状態，化学的性質などの工学的状態遷移で回避できるのは，どの状態に遷移させたらよいか分かっている場合に限られる。

今，ある潜在危険（作用連鎖または反転連鎖）が徐々に発現して，系の状態が毀損を発生させる状態側Dにあるとき，これを，毀損が発生しない状態側Sに遷移させるには，２通りの場合が考えられる。

ひとつは，DからSへの遷移を許容時空間閾で無秩序に行ってよい場合すなわち無秩序な工学的状態遷移 (Disordered Transition) である。

他方は，例えば，系へ作用する外乱によってその時々に定まる時空領域をフィードバック制御などにより通過するなど，ある秩序をもって行わなければならない場合すなわち秩序的な工学的状態遷移 (Ordered Transition) である。

前者では，例えば，安全弁開閉時における弁の状態遷移，後者では，航空機が気象学的外乱条件下で着陸する際の機体運動エネルギの状態遷移があげら

れる。

5.3 相反潜在危険

前節までは，系内に単一の潜在危険が生ずる場合のみを議論してきた。一般的には，系内に異なる潜在危険が次々と発生し，しかも各々の潜在危険によって毀損回避のための状態遷移の方向が異なることもある。このような潜在危険に対して次の定義を行う：

［定義　3］状態遷移の方向が異なる潜在危険を互いに相反潜在危険 (Mutually Reciprocal Hazards) という。

すると，潜在危険制御系と相反潜在危険の関係が次のように得られる：

［系　3］同一の潜在危険制御系で相反潜在危険を抑制するとき，潜在危険制御系は，系の状態遷移を複数の側に行わなければならない。

5.4 情報処理系の構成法則

潜在危険制御系では，センサ，処理部および出力部からなるいわゆる情報処理系が構成される場合が多い。情報処理系はフェール・セーフあるいはフォールト・トレランス・システム化されるが，両者には故障物理の観点から大きな相違がある。前者は通常非対称誤り率をもつ論理素子で構成され，後者は冗長系による機能維持が基本となる。

一般的に，フェール・セーフ・システムは，フォールト・トレランス・システムに比して，構造が単純で冗長系の同時故障を心配する必要性が少ないなど安全上優れた利点をもつ。しかしながら，フェール・セーフ・システムの適用性は，抑制しようとする潜在危険そのもの，および潜在危険を構成する要素集合の性質に依存する。

すなわち，f''(機能停止) 形の無秩序状態抑制作用鎖は，単方向制御作用鎖のみ構成可能である［定理7］。従って，無秩序な状態遷移を行う情報処理系では，原理的にf''形の無秩序状態抑制作用を構成できる。情報処理系に故障が発生し，f''形の抑制作用が反転すると秩序状態反転作用が生ずる［定理3］。秩序状態反転作用は，解離原理P_1，P_2またはP_3で解離されるので［定理5］，定義2より原則的にフェール・セーフ・システムが構成可能である。

秩序的な状態遷移を行う情報処理系では，複方向制御作用鎖を構成しなければならず，f''形の無秩序状態抑制作用鎖を構成できないので［定理7］，これをフェール・セーフ・システムとして構成できない。

以上の議論から，次のような情報処理系の構成法則を得る：

［構成法則　2］情報処理系の内部故障に対して，フェール・セーフ・システムを構成できるのは，情報処理系が無秩序な状態遷移を行う場合に限られる。

［構成法則　3］相反潜在危険を回避する情報処理系では，少なくとも一方の潜在危険に対してフェール・セーフ・システムを構成できない。

6. バッチ・プラントの局所的多相安全設計

本章では，第4章で述べた大局的多層安全設計⑩および⑪を実現する潜在危険制御系を構成し，さらにこれに対して，どのような局所的多相安全設計が実施できるかを例示して方法論の理解を図る。

6.1 内部冷却系 INC

6.1.1 基本構成

作用連鎖 (1) において，作用鎖$[M(m')a \xrightarrow[2]{}]$は反応器の温度制御を行う内部冷却系 INC によって，次のように解離される［定理1,2］：

$$INCa' \xrightarrow[-3]{} M(m')a \overset{P_1}{\not\rightarrow_2} M \cdots\cdots\cdots\cdots\cdots\cdots (2)$$

$a' \xrightarrow[-3]{}$: エネルギ伝播形解離作用（解離の必要条件となる作用）a'が要素間で授受される。

$a \overset{P_1}{\not\rightarrow_2}$: 作用$[a \xrightarrow[2]{}]$が解離原理P_1(作用源の制御）で解離される。

6.1.2 反転連鎖とその解離

内部冷却系 INC により作用鎖が解離されると，潜在危険が抑制される。しかし，INC に変化（故障）x（$\in X$: 故障集合）が生ずると，制御連鎖 (2) は，次のように反転連鎖を形成して，作用鎖の解離が実現されない［定理3,4］：

$$INC(x)\overline{f} \xrightarrow[3]{} M(m')a \xrightarrow[2]{} M(m'')a \xrightarrow[1]{}$$
$$R(\cdot)c \xrightarrow[0]{} E(\cdot) \cdots\cdots\cdots\cdots\cdots\cdots (3)$$

$\overline{f} \xrightarrow[3]{}$: 機能不履行形反転作用$f$が授受される。

反転作用鎖$[\overline{f} \xrightarrow[3]{}]$は，$INC$の冗長系$INC'$により次のように解離され，これにより元の作用鎖の解離が再び可能になる［定理5,6］：

$$\{(INC'g' \xrightarrow[-4]{} INC(x)\overline{f} \overset{P_4}{\not\rightarrow_3}) \,\&\, (INC'g' \xrightarrow[-4]{}$$
$$INC'g'' \xrightarrow[-3]{})\} M(m')a \overset{P_1}{\not\rightarrow_2} M \cdots\cdots\cdots (4)$$

$g' \xrightarrow[-4]{}$, $g'' \xrightarrow[-3]{}$: 機能代替形解離作用g' & g''が要素間で授受される。

このとき，内部冷却系は，変化（故障）集合Xと当該潜在危険に対してフォールト・トレランス・システムである［定義２］。すなわち内部冷却系のフォールト・トレランス・システム化により局所的多相安全設計が施されたことになる。

6.2　外部冷却系EXCの局所的多相安全設計

6.2.1　基本構成

反応器温度制御系の不調や予測しなかった反応などにより，器内の温度がθ_1を超えて危険な状態になることもありうる。そこで，作用連鎖 (1) の作用鎖$[a \xrightarrow[1]{}]$を解離する外部冷却系EXCを次の制御連鎖で構成する［定理 1,2］:

$$M(m')u_i'' \xrightarrow[-5]{} IPSu_j'' \xrightarrow[-4]{} ARu_k'' \xrightarrow[-3]{}$$
$$Vf' \xrightarrow[-2]{} M(m'')a \overset{P_1}{\not\xrightarrow[1]{}} R \cdots\cdots\cdots\cdots (5)$$

$$M(m')u_i'' \xrightarrow[-5]{} IPSu_l'' \xrightarrow[-4]{} ESa'' \xrightarrow[-3]{}$$
$$PMa' \xrightarrow[-2]{} M(m'')a \overset{P_1}{\not\xrightarrow[1]{}} R \cdots\cdots\cdots (5)'$$

$$HEa' \xrightarrow[-2]{} M(m'')a \overset{P_1}{\not\xrightarrow[1]{}} R \cdots\cdots\cdots\cdots (5)''$$

系の要素

IPS：情報処理系
AR　：外部冷却系出力部
V　：バルブ
PM：ポンプ
ES　：ポンプ動力源
HE　：熱交換器

抑制作用鎖

$a'' \xrightarrow[-3]{}$, $a'' \xrightarrow[-2]{}$：エネルギ伝播形抑制作用（解離作用の必要条件となる作用）が要素間で授受される。

$u_i'' \xrightarrow[-5]{}$, $u_j'' \xrightarrow[-4]{}$, $Su_l'' \xrightarrow[-4]{}$　：　抑制作用u_i'', u_j'', $u_k''(i,j,k \in 1,2,\cdots,6)$が要素間で授受される。$u_l'' \equiv a''$(エネルギ伝播形)，$u_2'' \equiv b''$(情報伝達形)，$u_6'' \equiv f''$(機能停止形)

外部冷却系は Fig. 3 のように基本設計される。

すなわち，反応器内の温度がθ_1を超えると$[M(m')u_i'' \xrightarrow[-5]{}]$，センサおよび処理部からなる情報処理系が出力部に作用する$[IPSu_j'' \xrightarrow[-4]{}]$ことにより，出力部がバルブを開放する$[ARu_k'' \xrightarrow[-3]{}]$。また，情報処理系は，ポンプ動力源にも作用してこれを ON とする$[IPSu_l'' \xrightarrow[-4]{}]$。すると，バルブが開となり$[Vf' \xrightarrow[-2]{}]$，ポンプが反応器内容物を外部冷却ラインに循環させる$[PMa' \xrightarrow[-2]{}]$。また，熱交換器がこれを冷却する$[HEa' \xrightarrow[-2]{}]$。こうして，作用鎖$[M(m'')a \xrightarrow[1]{}]$が解離され，災害が未然に防止される。

6.2.2　固有フェール・セーフ・システム

潜在危険 1 に対して，バルブを開放する状態遷移は無秩序に行える。情報処理系は，内部での抑制作用をf''形とでき，その故障に関してフェール・セーフ・システムを構成可能とする［構成法則 2］。

情報処理系内部での抑制作用をf''形と構成したとき，例えば，断線故障が生ずると系は潜在危険 1 による毀損を回避する方向に固有な状態遷移で収束する。このような故障を固有安全故障ということとする。系は，潜在危険 1 と固有安全故障に関して固有フェール・セーフ・システムである［定義 1］。

6.2.3　2 次的潜在危険の同定

保全作業による開口部の閉め忘れや配管材料の劣化などにより，開口部が外部冷却ラインに存在することがある。むやみにバルブV_1またはV_2を開放すると，外部冷却ラインにたまたま存在する開口部 (l) から反応器内容物が流出する。この 2 次的な潜在危険は，次の作用連鎖で同定される。

$$Rc \xrightarrow[1]{} EXL(l)c \xrightarrow[0]{} E(\cdot) \cdots\cdots\cdots\cdots\cdots\cdots (6)$$

$c \xrightarrow[1]{}$, $c \xrightarrow[0]{}$：作因物転移形作用cが授受される。

これを，潜在危険 2 と定義する。

6.2.4　潜在危険制御系の構成

潜在危険 2 を抑制するために，次の制御連鎖により，通常バルブは閉じられる［定義 1,2］:

$$Mu_i'' \xrightarrow[-5]{} IPSu_m'' \xrightarrow[-4]{} ARu_n'' \xrightarrow[-3]{}$$
$$Ve' \xrightarrow[-2]{} Rc \overset{P_2}{\not\xrightarrow[1]{}} EXL \cdots\cdots\cdots\cdots\cdots\cdots (7)$$

$e' \xrightarrow[-2]{}$：存在形態形解離作用が要素間で授受される。

$c \overset{P_2}{\not\xrightarrow[1]{}}$：作用鎖$[c \xrightarrow[1]{}]$が，解離原理$P_2$(作用径路の制御）で解離される。

バルブの閉方向の状態遷移は無秩序におこなえる。従って，この場合，潜在危険を抑制する情報処理系

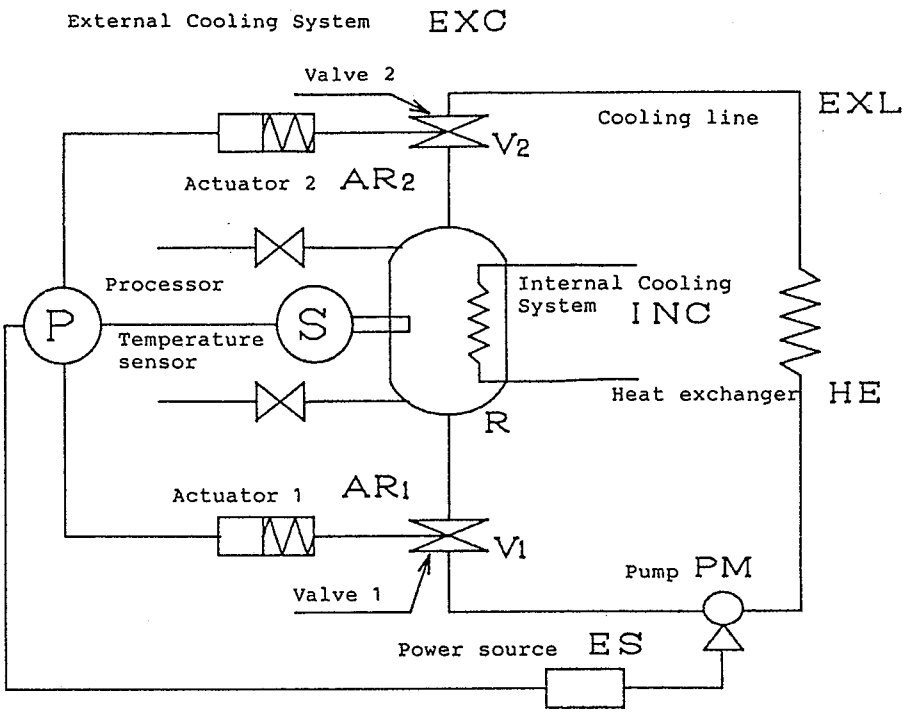

Fig. 3　Conceptualization of an emergency external-cooling-system
緊急外部冷却系の構成

は，その内部の故障に関してフェール・セーフ・システムを構成可能とする［構成法則 2］。

6.2.5　局所的多相安全設計

潜在危険 1 と潜在危険 2 とでは，バルブの開閉に関して，一方は開，他方は閉と状態遷移の方向が逆になっている。従って，定義 3 よりそれらは互いに相反潜在危険となり，外部冷却系における情報処理系は，一方の潜在危険のみにその内部の故障に関してフェール・セーフ・システムを構成可能である。［構成法則 3］。

すなわち，制御連鎖 (5)，(5)'，(7) における抑制作用u_j'', u_k'', u_m'', u_n''は，$f''(\equiv u_6''$ ：機能停止形)，$b''(\equiv u_2''$ ：情報伝達形)，$a''(\equiv u_1''$ ：エネルギ伝播形) のいずれかをとり，それらの可能な組合せは，Table 1 に示すようになる。

(s),(d),(s'),(d') をそれぞれIPSとARの潜在危険 1 に関する固有安全故障と危険側故障とする。すると，Table 1 の各構成法に対して，次のことが結論づけられる［構成法則 1 ～ 3］:

1. 全ての構成法 (Case No.1 ～ 9) において，(d),(d') および潜在危険 1 に関してフェール・セーフ・システムが構成可能である。このとき，(s),(s') は潜在危険 2 に対して危険側故障となる。
2. Case No.3,4 および 8 において，(s),(s') および潜在危険 2 に関してフェール・セーフ・システムが構成可能である。このとき，系は，(s),(s') に対する固有フェール・セーフ・システムの性質を失う。
3. Case No.2 と 7 では，(s) と潜在危険 2 に関してフェール・セーフ・システムが構成可能である。このとき，系は，(s) と潜在危険 1 に対する固有フェール・セーフ・システムの性質を失う。
4. 1 ～ 3 以外では，系はフォールト・トレランス・システムを構成しなければならない。

6.7　結　　言

複雑な系の計画・設計段階で，安全性を多相的に系に組みこむには，系統的方法論が必要である。システム安全は，現在までのところ，この多相安全設計問題すなわちシステム・シンセシス問題に無関心である。しかし，系がますます複雑化，巨大化，あるいはフレキシブル化しているので，これに対応するた

Table 1　Possible configurations of control actions
抑制作用の取りうる組合せ

Case Number	Control Actions			
	u''_j	u''_k	u''_m	u''_n
1	f''	f''	b''	a''
2	b''	f''	f''	a''
3	b''	a''	f''	f''
4	f''	a''	b''	f''
5	f''	a''	b''	a''
6	b''	f''	b''	a''
7	b''	a''	f''	a''
8	b''	a''	b''	f''
9	b''	a''	b''	a''

めにはこの方面の研究に力を注ぐ必要がある。

A-C モデルは，システム・シンセシス問題に対処するために展開されてきた方法論である。本研究では，A-C モデルに基づき，次ぎの知見を得た：

(1) 系の状態遷移をエントロピ・モデル化した。これにより，A-C モデルにおける作用の物理的背景が明確化され［系１］，固有フェール・セーフ・システムが定義された［定義１］。

(2) 多相安全設計の方法論を展開し，多相安全設計が大局的多相安全設計と局所的多相安全設計からなるとした場合には，後者が潜在危険制御系をフェール・セーフ／フォールト・トレランス・システム化することにより実現されることを示した。

(3) 各種工学体系を包括した一般化された形式でフェール・セーフ・システムの定義を試み，その構成条件を明らかにした［定義２，構成法則１］。

(4) 1) ～ 3) に基づき，系の状態遷移と潜在危険制御系における制御形式および相反潜在危険などの関係を考察した［定義３，系２］。その結果，系の状態遷移および相反潜在危険と潜在危険制御系情報処理部のフェール・セーフ・システム構成との関係が明らかにされた［構成法則2,3］。

さらに，以上の方法論をバッチ・プラントにおける固有フェール・セーフ・システムの構成と多相安全設計問題に事例的に適用して，本研究で得られた知見 1) ～ 4) が系統的なシステム・シンセシスに有効であることを確認した。

(平成３年４月 22 日受理)

参考文献

1) H. Kumamoto, Y. Sato and K. Inoue: Engineering Risk and hazard assessment (Hazard idetification and safety assessment of human-robot systems), (1988), 61–80, CRC Press, Inc., Boca Roton, Florida.

2) U.S.AEC.: Reactor Safety Study (WASH-1400), (1974).

3) 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），日機学論（Ｃ編），52–474 (1986), 823–382.

4) 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），日機学論文集（Ｃ編），152–482, (1986), 2754–2763.

5) G. Stephanopoulos and J.F. Davis, CACHE Monograph Series: Artificial Intelligence in Process Systems Engineering, Vol.2, (1990), 2–12, CACHE, Austin, Texas.

6) G.E. Apostolakis: Accident Sequence Modeling, (1988), 61–90, Elsevier Applied Science Pub. Ltd. New York.

7) 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），日機学論集（Ｃ編），151–468, (1985), 2188–2195.

8) 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），日機学論集（Ｃ編），154–505, (1988), 2164–2173.

9) 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），日機学論集（ｃ編），155–518, (1989), 2663–2671.

10) Y. Sato, E.J. Henley and K, Inoue: Architectonics of hazard-control systems for robotics, Proc. Intr, Conf. Advanced Mechatronics, (1989), 415–420.

11) Y. Sato, E.J. Henley and K, Inoue: An action-chain model for the design of hazard-control systems for robots, IEEE Trans. Reliab., 39–2, (1990), 151–157.

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

13) 佐藤・井上：自動車におけるヒューマン・エラー・バックアップ・システムの基本構成，日機学論集（C論），56–527, (1990), 1789–1796.

14) 佐藤吉信：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），日機学誌，93–863, (1990), 846–851.

15) 佐藤吉信：バッチ処理プラントの多相安全設計，配管技術，33–1, (1990), 51–55.

16) 参考文献 8) の 2165 ページ.

17) 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，22–9, (1981), 863.