

## 二層 Cause-Effect モデルによるプラントアラーム変数選択法

化学産業におけるプラントの大規模化やプラント監視制御システムの高度化によりプラントアラームシステムの重要性が高まっている。適切なアラームシステムの設計のためには、膨大な数の測定変数の中からアラーム変数をシステムティックに選択する仕組みが必要である。本論文では、状態変数間の因果関係を表す二層 Cause-Effect (CE) モデルに基づき、識別したい異常原因を定性的に識別できるアラーム変数と管理範囲の組合せを網羅的に導出できるアルゴリズムを提案する。簡単なプロセスを例題に本手法の有用性を例示する。

## **Plant Alarm Signal Selection Based on a Two-Layer Cause-Effect Model**

The importance of plant alarm systems has grown with increases in the scale of plants and the sophistication of plant monitoring and control systems. In this paper, a two-layer cause-effect model is proposed that represents the cause-and-effect relationship between state variables. Using the proposed model, a derivation algorithm of sets of pairs of alarm variables and signs is proposed. The signs indicate the upper or lower limits of alarm variables. The derived sets of pairs are theoretically guaranteed to be able to qualitatively identify all assumed malfunctions. The proposed method using the two-layer cause-effect model was applied to a simple process, and the simulation results illustrated the usefulness of the method.

## 緒 言

化学産業におけるプラントの大規模化やプラント監視制御システムの高度化は、一人のオペレータが担当する監視領域を拡大させ、異常検知や異常診断業務の複雑化を招き、オペレータの判断ミスなどの人的要因によるプラント事故が多発する原因となっている。このような背景の中、オペレータによるプラント異常の早期検知を支援するヒューマンマシンインタフェースの一つであるプラントアラームシステムの重要性が高まっている。

プラントアラームシステムでは、品質、コストや安全などの監視目的に応じて上限値、下限値からなる管理範囲を持つアラーム変数が定められる。アラーム変数の値が管理範囲の上限値、下限値のいずれかから逸脱したとき、アラームシステムは音や警光灯による警報を出し、発報アラームの詳細情報をDCSの監視画面上に表示する。不適切なアラーム変数の選択や管理範囲の設定は、運転管理業務を妨害する迷惑アラームやアラームの洪水の原因となり、オペレータの誤判断や誤操作を引き起こす。迷惑アラームやアラームの洪水を防ぐためには、プラントの膨大な数の測定変数から監視目的に応じてアラーム変数を選択し、管理範囲を適切に設定しなければならない。

欧米では、不適切なアラームシステムの設計によるプラント事故の多発を機に、プラント安全に対する新たな法規制やガイドラインが定められている。米国の International Society of Automation (2009) は、標準的なアラームマネジメントライフサイクル(ANSI/ISA-18.2)を提唱している。欧州の Engineering Equipment and Materials Users' Association は、Publication No.191 (2007) の中で、アラームシステムが本来持つべき機能や目的を明確に定義し、標準化された設計方法や管理方法を通じて、オ

ペレータに有意な情報を何らもたらさないアラームを徹底的に合理化することを求めている。しかし、いずれもアラームマネジメントの理念の提唱が中心で、アラームシステムの具体的な設計法にまで踏み込んでいない。

Luo *et al.* (2007) は、異常伝播図に基づくアラーム変数候補の選択法を提案した。異常伝播図とは、アラームシステムによって識別したい異常原因が引き起こすプラント内部状態の正常状態からのズレ（兆候）の連鎖の定性的な順序関係をまとめたものである。異常原因が識別できるとは、アラーム発報時にいずれの異常原因が真の異常原因であるか区別できない状況が避けられることを意味する。この方法は非常に簡便ではあるが、得られたアラーム変数の候補によって、識別したい異常原因が必ず同定できることを理論的に保障できない。Takeda *et al.* (2010) は、プラント配管トポロジーに基づくプロセス変数や操作変数などの因果関係モデルである Cause-Effect (CE) モデルから、適切なアラーム変数群を導出する方法を提案した。この方法は、識別が必要であると想定された異常原因を定性的ではあるが理論的に識別可能なアラーム変数群を網羅的に導出できる。また、配管トポロジーに基づくプラント構造の CE モデルを知識ベースに用いることで、アラーム変数群の選択根拠が明確となり、知識ベースのメンテナンス性にも優れるという特徴を持つ。しかし、提案手法におけるアルゴリズムでは、アラーム管理範囲の上限値、下限値を区別していないため、アラーム変数群の選択後、各アラーム変数群の管理範囲として上限値、下限値のいずれか、もしくは両方にアラームの設定が必要なのかを再検討しなければならないという問題があった。

本論文では、アラーム変数と管理範囲の上下限の符号{+, -}の対をアラーム対と呼び、アラーム対の組合せをアラーム対集合と呼ぶ。想定する異常原因を定性的に識別でき

るアラーム対の組合せの集合をアラーム対集合族と呼ぶ。状態変数の正常範囲からのズレの因果関係を二層 CE モデルとしてモデル化し、二層 CE モデルを用いてアラーム対集合族をもれなく導出するアルゴリズムを新たに提案する。提案手法では、管理範囲の上限から逸脱したときに発報するアラームと、管理範囲の下限から逸脱したときに発報するアラームの二種類を区別するため、より精密なアラームシステム設計が可能になる。なお、アラームシステム設計は一般的にアラーム対集合族の選択から管理範囲のしきい値の調整までを指すが、本論文ではアラーム対集合族の選択のみを検討範囲とする。

本論文は4章からなる。1章では、アラーム対集合族の選択問題を定義する。2章ではプラントの状態変数の正常状態からのズレの因果関係を定性的に表現する二層 Cause-Effect (CE) モデルを説明する。3章ではアラームシステムの設計手順を説明し、プラントにおいて想定される異常原因を定性的に識別できるアラーム対集合族を導出するためのアルゴリズムを提案する。4章では、簡単なプロセスを対象に提案手法の有効性を例示する。最後に本論文を総括する。

## 1. アラーム対集合族の選択問題

Takeda *et al.* (2010) は、アラーム変数の選択問題を、プラントの監視制御システムにより監視可能なすべてのプロセス変数や操作変数などの測定変数の集合から、事前に想定するプラントの異常原因を定性的に識別可能なアラーム変数の集合を導出する問題として定式化した。しかし、定式化した問題の中で管理範囲の上限に対するアラーム設定と下限に対するアラーム設定を区別していないため、選択後にあらためて個々のアラームごとに管理範囲を検討しなければならないという課題があった。

そこで本論文では、測定変数が管理範囲の上限から逸脱したときに発報するアラームと、管理範囲の下限から逸脱したときに発報するアラームの二種類を区別する。プラントの測定変数を  $s$ 、測定変数の集合を  $S$  とする。測定変数  $s$  の管理範囲の上限に対するアラーム設定を  $\{+\}$ 、下限に対するアラーム設定を  $\{-\}$  と表記し、測定変数  $s$  と管理範囲の上下限の符号  $\{+, -\}$  の対  $s+$  または  $s-$  を測定対  $s_p$ 、測定対の集合を測定対集合  $S_p$  と定義する。また、プラントで想定しうる異常原因を、後述する二層 CE モデル上の状態変数  $i$  とその符号  $\{+, -\}$  の対  $i[+]$  または  $i[-]$  によって表し、これを異常原因対  $z (z \in Z)$  とよぶ。異常原因対  $z$  の中で、アラームシステムによって識別したい異常原因対を識別異常原因対  $c$  とし、その集合を識別異常原因対集合  $C$  と定義する。プラントでは、複数の異常原因が同時に発生することはないとする。アラームシステムによって識別したい識別異常原因対の集合は、事前に求められているとする。

本論文では、アラーム対の選択問題を、あらかじめ想定するすべての識別異常原因対  $c$  を定性的に識別できる測定対  $s_p$  の集合族であるアラーム対集合族  $A$  を求める問題として定式化する。異常原因対を識別できるとは、アラーム発報時に識別異常原因対の中のいずれが真の異常原因対であるか区別できない状況が避けられることを意味する。

## 2. 二層 CE モデル

アラーム対集合族  $A$  を選択するために、プラントの状態変数間の因果関係を表現する定性モデルである二層 Cause-Effect (CE) モデルを提案する。二層 CE モデルでは、プラントの状態変数の正常範囲からのズレを表す点として以下の二種類を定義する。

- $i+$ : 状態変数  $i$  の正常範囲からの大きな値 (+) 側への逸脱を表す点
- $i-$ : 状態変数  $i$  の正常範囲からの小さい値 (-) 側への逸脱を表す点

状態変数の正常範囲からのズレを表す点は、+層および-層のいずれか一方、もしくは両方に存在する。たとえば、ポンプや手動バルブなど、状態変数が正常領域に対して、+/-のいずれか一方にしかズレが発生しない場合は、片側の層のみに点を置く。状態変数の正常範囲からのズレの直接的な因果関係を、点間の有向枝で表現する。二層 CE モデルは、装置内の状態変数の因果関係やプラントの配管トポロジーなどの情報に基づいて作成することができる。

二層 CE モデルの簡単な例として、**Figure 1** のタンクシステムの二層 CE モデルを **Figure 2** に示す。タンクシステムの状態変数は、流入量  $F1$  および  $F2$ 、タンクの液位  $L$  および流出量  $F3$  である。たとえば、流入量  $F1$  が増加し正常領域より+側にずれた結果、タンクの液位  $L$  は上昇し正常領域より+側にずれるため、点  $F1+$  から点  $L+$  への因果関係を有向枝で結ぶ。

二層 CE モデルを用いることで、想定する異常原因が発生した場合の影響がプラントの状態変数にどのように伝播していくのかを定性的に調べることができる。たとえば、**Figure 1** のタンクシステムのすべての状態変数が正常かつ定常状態であるとき、 $F1$  の元圧が上昇するという異常原因が発生したとする。元圧が上昇した結果、 $F1$  が上昇し正常範囲から+側に逸脱する。このとき、二層 CE モデルの点  $F1+$  が発火したといい、二層 CE モデル上では網掛けの点で表す。アラーム変数に対応する点が発火した場合、発報することになる。 $F1+$  と  $L+$  は有向枝によって結ばれているため、 $F1+$  の発火の影響により  $L+$  が発火する。以後、**Figure 3** に示すように二層 CE モデルの有向枝を向きに沿って下ることで、元圧上昇によりプラント内の状態変数の変動が以下のステージのように進展することがわかる。

Stage 1: 元圧変動により、流入量  $F1$  が増加 ( $F1+$ )

Stage 2: 流入量  $F1$  増加により、タンク液位  $L$  が増加 ( $F1+ \rightarrow L+$ )

Stage 3: 液位  $L$  増加により、流出量  $F3$  も増加 ( $F1+ \rightarrow L+ \rightarrow F3+$ )

このように、二層 CE モデルを用いることで、想定する異常原因の影響がプラント内をどのように伝播していくのか定性的に調べることができる。次節では、この二層 CE モデルを用いて、想定する異常原因を理論的に識別できるアラーム対集合族の選択法を提案する。

### 3. アラーム対集合族の選択法

#### 3.1 アラームシステムの設計手順

アラームシステムの設計手順の流れを以下に説明する。対象とするプラントの二層 CE モデルおよび測定変数集合  $S$  は既知であるとする。なお、本論文では、以下の手順(b)アラーム対集合族の選択のみを検討の対象とする。

##### (a) 識別異常原因対の設定

- ① アラームシステムによって識別したいプラントのすべての異常原因(元圧上昇など)を列挙し、二層 CE グラフ上の点の中から各異常原因の表現に適切な点を選び、識別異常原因対  $c$  として割り付ける。
- ② 利用可能な測定対を全て用いても、要求されるすべての識別異常原因対を識別できない場合もある。この場合、いずれかの識別異常原因対の識別を諦める必要がある。そこで、諦める識別異常原因対の選択のために、異常原因の発生頻度とインパクトの大きさによるリスクマトリックス(EEMUA (2007))などに基づいて個々の識別異常原因

対  $c$  の重要度を決定する。

(b) アラーム対集合族の選択

- ③ プラントのすべての測定対  $s_p$  を二層 CE モデル上の点に割り付ける。
- ④ 二層 CE モデルを用いたアラーム対集合族選択アルゴリズムを用いて、識別異常原因対集合  $C$  に含まれるすべての識別異常原因対  $c$  を定性的に識別可能な測定対集合族を導出する。選択された測定対集合族をアラーム対集合族  $A$  とし⑥に進む。すべての識別異常原因対を識別できる測定対集合が存在しない場合は⑤に進む。アラーム対集合族の選択アルゴリズムは、3.2 で詳しく説明する。
- ⑤ 識別異常原因対の重要度を考慮して、識別異常原因対集合  $C$  の要素を減らし、④に戻る。

(c) 管理範囲の設定

- ⑥ アラーム対集合族  $A$  に含まれるアラーム対集合は、識別異常原因対集合  $C$  の要素として残った識別異常原因対  $c$  を定性的には識別できるアラーム対の組合せであり、アラーム変数と管理範囲の候補となる。各アラーム変数の管理範囲の設定値を EEMUA (2007) などの手法を用いて調整する。

### 3.2 アラーム対集合族の導出アルゴリズム

識別異常原因対集合  $C$  を定性的に識別可能とするアラーム対集合族  $A$  の選択アルゴリズムを以下に示す。

ステップ3にて後述するように、各アラーム変数の発報状態は、アラーム変数が正常な状態を含めて3種類に区分されるため、 $n$  個のアラーム変数の発報を仮定して表現される発報パターン(以下では仮定アラーム対発報パターンと呼ぶ)の数は  $3^n$  通りある。

各仮定アラーム対発報パターンの異常原因と考えられる原因対の集合を異常原因の候補対集合と呼ぶ。すべての仮定アラーム対発報パターンに対して得られたすべての異常原因の候補対集合の中で、他の異常原因の候補対集合の真部分集合にならない集合を異常原因の最大候補対集合と呼ぶ。異常原因の最大候補対集合の集合を異常原因の最大候補対集合族と呼ぶ。 $C$  の相異なる二つ以上の要素がいずれの異常原因の最大候補対集合にも同時に含まれないとき、アラーム対集合族  $A$  に含まれるアラーム対の集合により  $C$  のすべての要素は定性的に識別可能である。異常原因対を識別できるとは、アラーム発報時に識別異常原因対の中のいずれが真の異常原因対であるか区別できない状況が避けられることを意味する。

ステップ 1:  $C = \emptyset$  のとき、最初に想定した識別異常原因対集合  $C$  から識別異常原因対を重要度にもとづき諦めていったにも関わらず、測定点集合から生成可能なアラーム変数の組合せでは識別できない設定になっているとして計算を終了する。 $C \neq \emptyset$  のとき、 $A = \emptyset$  としてステップ 2 へ進む。

ステップ 2: 測定変数集合  $S$  のべき集合から空集合を除いて  $Q$  とする。

ステップ 3:  $Q$  の各要素をアラーム変数の組合せと仮定する。それぞれのアラーム変数の組合せにつき、すべての仮定アラーム対発報パターンを生成する。アラームの発報状態として以下の三種類を仮定し、それぞれ +、0、- の記号で表す。

- (+) アラーム変数が管理範囲の上限を逸脱してアラームが発報した状態
- (0) アラーム変数が管理範囲の中にあり、アラームが発報していない状態
- (-) アラーム変数が管理範囲の下限を逸脱してアラームが発報した状態

ステップ 4: すべての仮定アラーム対発報パターンに対する異常原因の最大候補対集合

族を導出する。具体的な導出方法を 3.3 で説明する。

ステップ 5: 識別異常原因対集合  $C$  と、 $Q$  の要素の中から  $C$  を識別可能であった要素それぞれに対するアラーム対集合族  $A$  を出力して計算を終了する。

(ステップ終わり)

### 3.3 二層 CE モデルを用いた最大候補対集合族の導出法

すべての仮定アラーム対発報パターンに対して、以下の手順によって識別異常原因対の候補対集合を導出する。

[識別異常原因対の候補対集合導出の手順]

仮定アラーム対発報パターンを一つ選んで考える。二層 CE グラフ上で該当の仮定アラーム対発報パターンにおいて発報を仮定しているアラーム対(以下では仮定発報アラーム対と呼ぶ)に対応する点のみを発火させる。発火した点から一つの点  $i$  を選び、点  $i$  から識別異常原因対に向かって、有向枝の向きとは逆方向に有向道をさかのぼって探索する(以下では、逆方向探索と呼ぶ)。有向道とは、点  $1 \rightarrow$  点  $2 \rightarrow \dots \rightarrow$  点  $n$  のように向きのそろった有向枝の列である。有向道の逆方向探索の途中でアラーム変数と仮定されていない状態変数の点までさかのぼった場合は、その点を発火させ有向道の逆方向探索を続ける。未発報と仮定したアラーム変数は、異常原因から異常が有向枝の向きに沿って伝播していないことを意味するため、有向道の逆方向探索の途中で未発報と仮定したアラーム変数までさかのぼった場合は、その点からの逆方向探索を打ち切る。

二層 CE モデルでは、有向道の逆方向探索の途中で、仮定発報アラーム対と逆符号のアラーム対に対応する点までさかのぼる場合がある。このとき、提案手法では、逆符号の点は発火させず、逆符号の点からの逆方向探索を打ち切る(後述の説明1参照)。同様

に、有向道の逆方向探索の途中で、すでに発火している点と同じ状態変数の逆符号の点までさかのぼる場合がある。提案手法では、各状態変数において、一旦いずれかの符号で発火した場合、同じ状態変数の逆符号の点に逆方向探索でさかのぼったとしても、逆符号の点は発火させず、逆符号の点からの有向道の逆方向探索は打ち切るとした(後述の説明2参照)。

有向道の逆方向探索結果から、異常原因の最大候補対集合族とアラーム対集合族を以下の方法によって導出する。仮定アラーム対発報パターンにおける全ての仮定発報アラーム対に対応する点から、ある識別異常原因対までの有向道を逆方向探索できれば、この識別異常原因対を異常原因の候補対集合に加える。その後、点  $i$  から逆方向探索された有向道以外の有向道上の点で、仮定アラーム対発報パターンに対応する仮定発報アラーム対の点以外の状態変数の発火の仮定はすべてリセットして、二層 CE モデル上のすべての有向道を逆方向探索するか、探索していない識別異常原因対がなくなるまで、有向道の逆方向探索を続ける。

すべての仮定アラーム対発報パターンに対して同様に有向道を逆方向探索する。有向道の逆方向探索の結果、次の2通りに対処がわかる(後述の説明3参照)。

①得られた異常原因の候補対集合が、いずれの異常原因の最大候補対集合の部分集合でもない場合:異常原因の候補対集合を異常原因の最大候補対集合として異常原因の最大候補対集合族に加え、該当のアラーム対集合をアラーム対集合族  $A$  に登録する。

②得られた異常原因の候補対集合が、いずれかの異常原因の最大候補対集合の部分集合である場合:すでにアラーム対集合族に含まれている当該の異常原因の最大候補対集合に対応するアラーム対集合  $a$  との和集合をアラーム対集合族  $A$  に登録し、 $a$  を

アラーム対集合族  $A$  から取り除く。(手順終わり)

[説明1]状態が振動する可能性のある変数へのアラーム設定は、アラームの洪水の原因となる。(説明1終わり)

[説明2]状態変数が振動する原因として、制御系やリサイクルなどトポロジーに起因するループ構造を持つ有向道の存在がある。一旦、状態変数の変動がループ内に入ると異常原因の特定は難しく、振動する状態変数から有向道の向きに下って辿りつく状態変数をアラーム変数に用いることは適切ではない。また、二層 CE モデルでは、異なる原因から発生する因果関係を有向枝として同時に表現しているため、二層 CE モデル上で異なった符号を持つ同じ状態変数の点が同時に発火する影響伝播が表現できてしまうが、現実のプラントでは、このような状態になることは少ない。(説明2終わり)

[説明3]複数の仮定アラーム対発報パターンから、同じ異常原因の候補対が逆方向探索される可能性がある。該当の異常原因の候補対において異常が発生した場合、有向枝の向きに沿って異常が伝播していくことで、状況として成立しうるアラーム対発報パターンを持つものが各アラーム対集合である。異常伝播の経路や到達状況は多様であり、複数のシナリオが成立すると考えられる。しかし、アラームシステムで検知を行う場合、いずれのシナリオに沿って異常が進行しているのかは分からない。よって、安全側を考慮して、いずれのシナリオに対しても発報できるアラームを設計することが望ましい。

また、異なった異常原因の候補対から有向枝の向きに沿って異常が伝播するシナリオにおいて、同一のアラーム対発報パターンとなる場合がある。そのアラーム対発報パターンから逆方向探索すると、これらの異常原因の候補対のいずれが真の異常原因かわからない異常原因の候補対集合となる。最大候補対集合は、ある仮定アラーム対発報パターンから逆方向探索して得られた異常原因の候補対集合であり、他の異常原因の候補

対集合の真部分集合にならない集合である。そのため、アラームシステムで検知を行う場合、最大候補対集合に含まれるいずれの候補対からのいずれのシナリオに沿って異常が進行しているかは分からない。よって、安全側を考慮して、該当するいずれのシナリオに対しても発報できるアラームを設計することが望ましい。すなわち、最大候補対集合に含まれるすべての候補対からのすべてのシナリオに沿ったアラーム対発報パターンを含むアラーム対集合が望ましい。

提案アルゴリズムでは、ある仮定発報アラーム対に対応する点から逆方向探索を行う際に、既に発火しているとした変数の逆符号の点に辿り着いた場合は逆方向探索を打ち切る仕組みとなっているため、同一アラーム変数において+側と-側の両方のアラーム対を用いるアラーム対集合は有向道の逆方向探索の対象外である。しかし、和集合として登録するためアラーム対集合には同時に含まれる可能性がある。(説明3終わり)

既に述べたように、アラーム変数の数が  $n$  のとき、仮定アラーム対発報パターンの数は  $3^n$  となるため、アラーム変数の数の増加と共に、異常原因の最大候補対集合族を導出するための有向道の逆方向探索は組合せ爆発を起こす。そこで、異常原因の最大候補対集合族の効率的な計算法として分枝限定法(Shibata and Matsuyama,1989)を用いた。ただし、提案手法では異常原因の最大候補対集合とともにアラーム対集合族  $A$  を探索する必要があるため、緩和問題において異常原因の候補対集合が得られなければ分枝操作を打ち切るという限定操作のみを採用した。

### 3.4 アルゴリズムの例説

Figure 1 のタンクシステムを例題として、提案するアルゴリズムにしたがってアラーム対集合族  $A$  の導出を説明する。タンクシステムの測定変数集合を  $S=\{F1,F3,L\}$ 、識別異常原因対の集合  $C=[F1+, F1-, L+, L-]$ とする。このとき、測定変数集合  $S$  のべき集合から空

集合を除いて、 $Q = \{F1\}, \{F3\}, \{L\}, \{F1, L\}, \{F3, L\}, \{F1, F3\}, \{F1, F3, L\}$ となる。

$Q$ から一つの要素 $\{F1, F3, L\}$ を取り出し、それぞれの測定変数をアラーム変数と仮定する。仮定アラーム対発報パターンの例として、 $\{F1+, F3+, L+\}$ を考える。それぞれを仮定発報アラーム対とする。二層 CE モデル上で仮定発報アラーム対  $F3+$ から有向道を逆方向探索すると、**Figure4(a)**に示すように、識別異常原因対  $L[+]$ にさかのぼれる。**Figures 4**では探索中の有向枝を太く、そうでない有向枝を薄く表示する。ここで  $L[+]$ が異常原因の候補対になれるかを考える。仮定アラーム対発報パターンは $\{F1+, F3+, L+\}$ なので、 $L[+]$ により仮定発報アラーム対  $F1+$ の発報を説明できなければならないが、 $L[+]$ から発報した仮定発報アラーム対  $F1+$ へ有向枝の向きに沿って下る有向道が存在しない。よって、 $L[+]$ は異常原因の候補対にならない。よって、仮定発報アラーム対  $F3+$ と  $L+$ の発報を説明できる変数を探すため、仮定発報アラーム対  $L+$ から引き続き逆方向探索を行う。**Figure4(b)**に示すように  $F3-$ にさかのぼれるが、仮定発報アラーム対  $F3+$ がすでに発報しているため、 $F3-$ は発火できない。よって、 $F3-$ からの有向道の逆方向探索を打ち切る。仮定発報アラーム対  $L+$ に戻り、別の有向道を逆方向探索すると、**Figure4(c)**に示すように識別異常原因対  $F1[+]$ にさかのぼれる。 $F1+$ は仮定発報アラーム対そのものであり、すでに仮定アラーム対発報パターンの全ての仮定発報アラーム対を含んだ有向道が得られている。よって、 $F1+$ から他の仮定発報アラーム対を説明できる有向道の存在を確認する必要がないため、この時点で  $F1[+]$ を異常原因の候補対集合に追加する。さらに、他の異常原因の候補対集合を探すため、 $L+$ からの有向道の逆方向探索を続ける。**Figure 4(d)**に示すように  $L+$ から  $F2+$ にさかのぼれるが、 $F2+$ は識別異常原因対ではなく、 $F2+$ に影響を与える有向道もない。よって、 $F3+$ からの逆方向探索の過程で仮定アラーム対発報パターン $\{F1+, F3+, L+\}$ に関わるすべての有向道を逆方向探索したので、有向道の逆

方向探索処理を終了する。異常原因の最大候補対集合族は空集合なので異常原因の候補対集合 $\{F1[+]\}$ を最大候補対集合族に加え、 $\{F1[+]\}$ に対応するアラーム対集合 $\{F1+, F3+, L+\}$ をアラーム対集合族 **A** に登録する。

すべての仮定アラーム対発報パターン( $3^3=27$  通り)についても同様に異常原因の候補対集合を探索すると、異常原因の最大候補対集合族は **Table 1** に示すように $\{\{F1[+]\}, \{F1[-]\}, \{L[+]\}, \{L[-]\}\}$ となる。**Table 1** における仮定アラーム変数の $\{+, 0, -\}$ は発報状態を意味し、 $\times$ は仮定アラーム対発報パターンに対応する異常原因対が、識別異常原因対以外の場合に起こりうる可能性があることを意味している。また、すべての仮定アラーム変数の状態が正常である場合、異常原因の候補対集合が存在しないことは自明である。アラーム対集合族 **A** の探索結果は、識別異常原因対  $F1[+]$  に対して $\{F1+, F3+, L+\}$ 、 $\{F1+, L+\}$ 、 $\{F1+\}$ の和集合 $\{F1+, F3+, L+\}$ 、識別異常原因対  $F1[-]$  に対して $\{F1-, F3-, L-\}$ 、識別異常原因対  $L[+]$  に対して $\{F3+, L+\}$ 、識別異常原因対  $L[-]$  に対して $\{F3-, L-\}$ となる。

**Q** の残りの要素 $\{F1\}$ 、 $\{F3\}$ 、 $\{L\}$ 、 $\{F1, L\}$ 、 $\{F3, L\}$ 、 $\{F1, F3\}$ についても同様にアラーム対集合族 **A** を求めると、最終的にアラーム対集合族 **A** と対応する識別異常原因対は **Table 2** のようになる。なお、 $\{F1\}$ 、 $\{F3\}$ 、 $\{L\}$ 、 $\{F3, L\}$ は、**C** に含まれる識別異常原因対を識別することができないため **Table 2** に含まれない。

(例題終わり)

## 4. ケーススタディ

### 4.1 問題設定

**Figure 5** に示すリサイクルを有する簡単なプロセスを用いて、提案手法の有効性を例示する。このプロセスでは、原料は系外からタンク1へフィードされ、タンク2を經由して系

外へと排出される。一部はタンク1へリサイクルされる。図中の  $P$ 、 $F$ 、 $L$ 、 $V$  は、それぞれ圧力、流量、液レベル、バルブ開度を表す状態変数であり、 $P1$  および  $P2$  を除くすべての状態変数が測定変数であるとする。このプロセスの二層 CE モデルを **Figure 6** に示す。ただし、タンク 1 からタンク 2 へ送るポンプは、タンク1の液レベル  $L1$  に応じて吐出圧が変化すると想定したため、ポンプは液レベル  $L1$  に縮退させた。

このプロセスで識別異常原因対として、フィード元圧上昇  $P1[+]$ 、フィード元圧下降  $P1[-]$ 、配管のつまり  $F2[-]$ 、 $V4$  バルブの異常開  $V4[+]$ 、 $V4$  バルブの異常閉  $V4[-]$  を想定した。アラーム対集合族  $A$  の選択問題は、以下の識別異常原因対集合  $C$  を完全に識別できるアラーム対の組合せの集合を測定対集合  $S_p$  から選ぶ問題となる。

$$C = \{P1[+], P1[-], F2[-], V4[+], V4[-]\}$$

$$S_p = \{F1+, F1-, F2+, F2-, F3+, F3-, F4+, F4-, L1+, L1-, L2+, L2-, V1+, V1-, V2+, V2-, V3+, V3-, V4+, V4-\}$$

#### 4.2 アラーム対集合族の選択結果

すべての識別異常原因対を識別できるアラーム対集合族  $A$  を探索したところ、344 通りのアラーム対の組合せが得られた。探索によって得られたアラーム対の組合せの数を、組合せの中に含まれるアラーム変数の数ごとに集計した結果を **Table 3** に示す。Table 3 より、10 個の測定変数の中から少なくとも三つの測定変数にアラームを設定すればすべての識別異常原因対を定性的に識別できることがわかる。すなわち、アラーム変数にいくつかなるアラームが発報しても、アラーム発報時に識別異常原因対集合の中のいずれが真の異常原因対であるか分からない状況が避けられる。

アラーム変数の数が最も少ないアラーム対の組合せのひとつは  $\{F1+, F1-, F2+, F2-, V4+, V4-\}$  であった。この組合せにおいて、想定した識別異常原因対とアラーム対の関係

を **Table 4** に示す。前報 (Takeda *et al.*, 2010) では、アラーム変数の選択までしかできなかったため、 $F1$ ,  $F2$ ,  $V4$  にアラームを設定すればよいことまでは分かっても、それぞれの識別異常原因対に対していずれの変数の+側および-側にアラームを設定すればよいかまでは分からなかった。

識別異常原因対  $F2[-]$ を識別するためには、 $F2[-]$ が異常原因となった場合にアラーム対  $F2-$ が発報し、それ以外が発報しないように設定すればよい。識別異常原因対  $P1[-]$ を識別するには、 $P1[-]$ が異常原因となった場合にアラーム対集合として  $F1-$ と  $F2-$ が発報し、それ以外が発報しないように設定すればよい。

## 結 言

プラントの配管トポロジーに基づく状態変数間の因果関係モデルである二層 CE モデルに基づき、想定する識別異常原因対を定性的に完全に識別することのできるアラーム対の組合せの集合をシステムティックに導出する手法を提案した。アラームシステムの設計者は、導出されたアラーム変数の管理範囲のしきい値をシミュレーションなどで調整するだけでよく、従来のような試行錯誤的なアラーム変数の選択および管理範囲の決定が不要になる。また、二層 CE モデルは配管トポロジーに基づくモデルであるため、アラームシステム設計の根拠情報が明確であり、メンテナンス性に優れる。

化学プロセスは、プラント内部にリサイクル流れを有することが多い。プラントのリサイクル流れは、二層 CE モデル上で強連結成分として表れるため、リサイクル構造の内部に存在する識別異常原因対を識別できるアラーム対集合族の選択は難しい。リサイクル構造の内部に存在する識別異常原因対を識別するためのアラーム対集合族選択法の提案が今後の課題である。

[謝辞]本研究は、日本学術振興会プロセスシステム工学第143委員会ワークショップ No. 28での活動成果の一部をまとめたものである。ここに謝意を表す。

## Nomenclature

$A$	= set of set of pair of alarm variables and signs	[—]
$c$	= assumed malfunction to be identified by alarm system	[—]
$C$	= set of $c$	[—]
$i$	= state variable	[—]
$n$	= number of alarm variables	[—]
$P$	= pressure	
$L$	= liquid level	[—]
$V$	= valve position	[—]
$F$	= flow rate	[—]
$Q$	= power set of $S$	[—]
$s$	= measuring point	[—]
$S$	= set of $s$	[—]
$z$	= assumed malfunction in a plant	[—]
$Z$	= set of $z$	[—]
<i>Subscript</i>		
$p$	= pair	[—]

## Literature Cited

- ANSI/ISA-18.2-2009 Management of Alarm Systems for the Process Industries Engineering Equipment and Materials Users' Association (EEMUA); ALARM SYSTEMS - A Guide to Design, Management and Procurement Publication No.191 2nd Edition, EEMUA, London (2007)
- Luo, Y., X. Liu, M. Noda and H. Nishitani; "Systematic design approach for plant alarm systems," *J. Chem. Eng. Jpn.*, **40**, 765—772 (2007)
- Shibata, B. and H. Matsuyama; "Evaluation of the Accuracy of the Fault Diagnosis System Based on the Signed Directed Graph", *Kagaku Kogaku Ronbunshu*, **15**, 395—402 (1989)
- Takeda, K., T. Hamaguchi and M. Noda; "Plant Alarm System Design based on Cause-Effect Model," *Kagaku Kogaku Ronbunshu*, **36**, 136—142 (2010)

## 図表一覧

**Fig. 1** Example tank system

**Fig. 2** Two-layer CE model of example tank system

**Fig. 3** Propagation of abnormal situation

**Fig. 4** Search of fault origin using two-layer CE model

**Fig. 5** Reaction process

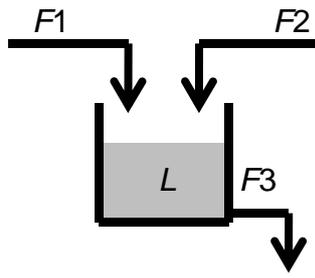
**Fig. 6** Two-layer CE model for reaction process

**Table 1** Sets of candidates for all pairs of alarm variables and signs

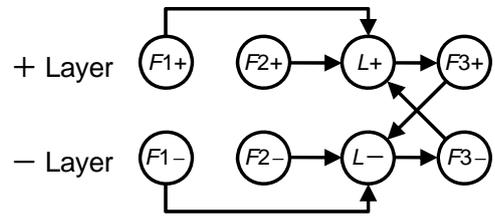
**Table 2** Sets of pairs of alarm variables and signs for each pair of origin variable and signs

**Table 3** Results of alarm variables selection

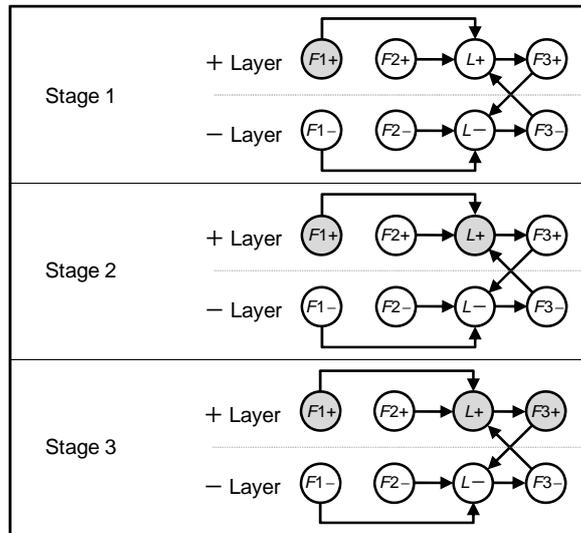
**Table 4** Pairs of alarm variables and signs for distinguished pairs of origin variables and signs



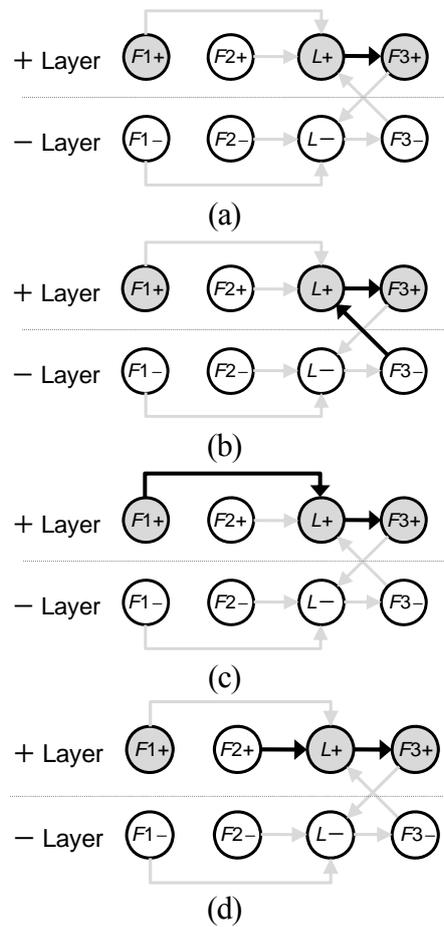
**Fig. 1** Example tank system



**Fig. 2** Two-layer CE model of example tank system

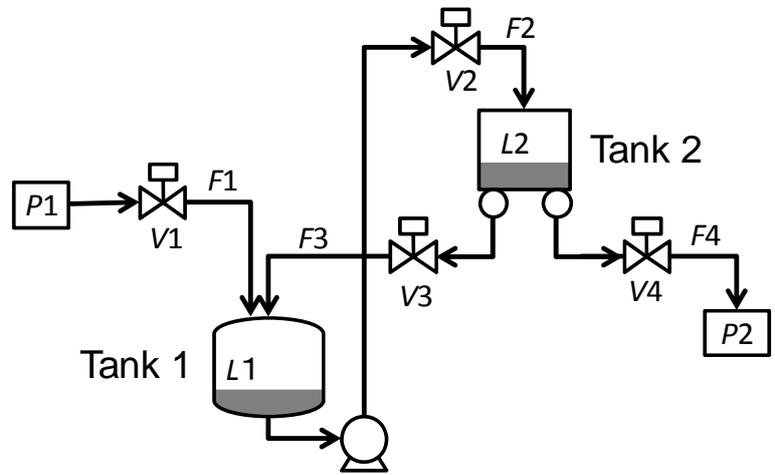


**Fig. 3** Propagation of abnormal situation

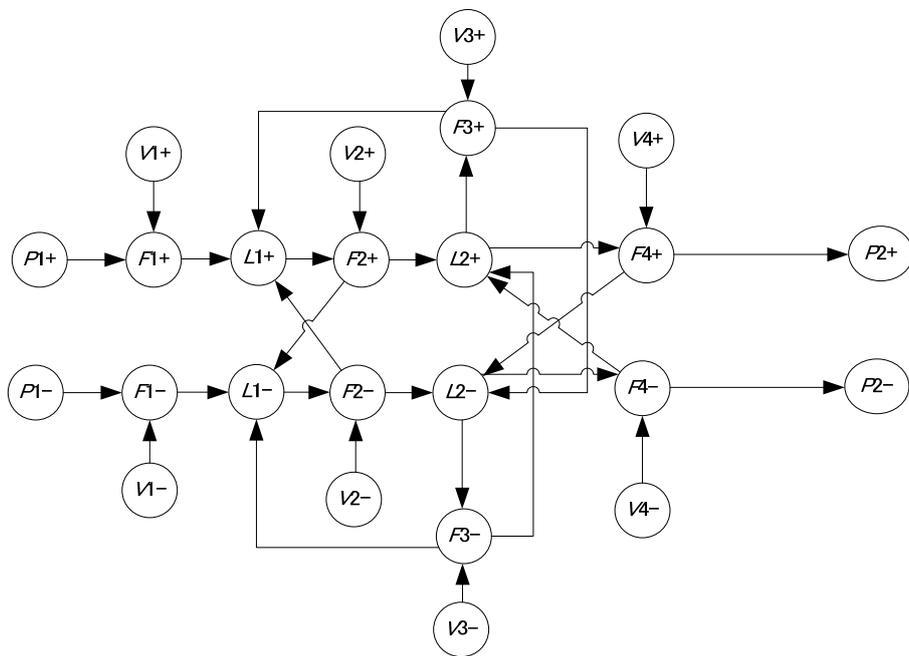


Distinguished pairs of origin variables and signs:  $[F1+, F1-, L+, L-]$   
 Pairs of measured variables and signs:  $\{F1+, F1-, F3+, F3-, L+, L-\}$

**Fig. 4** Search of fault origin using two-layer CE model



**Fig. 5** Reaction process



**Fig. 6** Two-layer CE model for reaction process

**Table 1** Sets of candidates for all pairs of alarm variables and signs

<i>F1</i>	<i>F3</i>	<i>L</i>	Sets of candidates
+	+	+	<i>F1</i> [+]
+	+	-	×
+	+	0	×
+	-	+	×
+	-	-	×
+	-	0	×
+	0	+	<i>F1</i> [+]
+	0	-	×
+	0	0	<i>F1</i> [+]
-	+	+	×
-	+	-	×
-	+	0	×
-	-	+	×
-	-	-	<i>F1</i> [-]
-	-	0	×
-	0	+	×
-	0	-	<i>F1</i> [-]
-	0	0	<i>F1</i> [-]
0	+	+	<i>L</i> [+]
0	+	-	×
0	+	0	×
0	-	+	×
0	-	-	<i>L</i> [-]
0	-	0	×
0	0	+	<i>L</i> [+]
0	0	-	<i>L</i> [-]
0	0	0	

**Table 2** Sets of pairs of alarm variables and signs for each pair of origin variable and signs

Sets of alarm variables	Distinguished pairs of origin variables and signs	Sets of pairs of alarm variables and signs
$F1, F3, L$	$F1[+]$	$\{F1+, F3+, L+\}$
	$F1[-]$	$\{F1-, F3-, L-\}$
	$L[+]$	$\{F3+, L+\}$
	$L[-]$	$\{F3-, L-\}$
$F1, L$	$F1[+]$	$\{F1+, L+\}$
	$F1[-]$	$\{F1-, L-\}$
	$L[+]$	$\{L+\}$
	$L[-]$	$\{L-\}$
$F1, F3$	$F1[+]$	$\{F1+, F3+\}$
	$F1[-]$	$\{F1-, F3-\}$
	$L[+]$	$\{F3+\}$
	$L[-]$	$\{F3-\}$

**Table 3** Results of alarm variables selection

Number of alarm variables	Number of sets of alarm variables
3	7
4	36
5	80
6	100
7	76
8	35
9	9
10	1
Total	344

**Table 4** Pairs of alarm variables and signs for distinguished pairs of origin variables and signs

Distinguished pairs of origin variables and signs	Pairs of alarm variables and signs
$F2[-]$	$F2-$
$P1[-]$	$F1-, F2-$
$P1[+]$	$F1+, F2+$
$V4[-]$	$F2+, V4-$
$V4[+]$	$F2-, V4+$