TR-0848

想定外事態に対処する
制御エキスパートシステムの構築

河野　毅、鈴木　淳三、岩政　幹人、
末田　直道、神谷　昭基（東芝）

ICOT
Mita Kokusai Bldg. 21F
4-28 Mita 1-Chome
Minato-ku Tokyo 108 Japan
(03)3456-3191～5

Institute for New Generation Computer Technology

想定外事態に対処する制御エキスパートシステムの構築

河野　毅*，鈴木淳三*，岩政幹人*，末田直道*，神谷昭基**

＊　（株）東芝　研究開発センター

＊＊（株）東芝　府中工場

A Plant Control Expert System to Cope with Unforeseen Situations

Takeshi Kohno*,Junzo Suzuki*,Mikito Iwamasa*,
Naomichi Sueda* and Akimoto Kamiya**
(* Research & Development Center,Toshiba Corp.)
(** Fuchu Works,Toshiba Corp.)

In order to reduce labor and careless mistakes in plant control operations, supervisory control systems using expert system technologies have been developed. These control systems can handle foreseen situations, however, due to a lack of the appropriate control rules, they cannot handle unforeseen situations. Up until now, such situations have had to be handled by skilled operators. To overcome such unforeseen situations, the authors have developed model-based reasoning technologies, such as diagnosis with qualitative causal model, knowledge compiler generating control knowledge from plant models (structure, function and general rules) and fuzzy qualitative reasoning. This paper proposes an overall system concept and architecture which integrates these technologies. This system was developed by first observing how skilled operators handle unforeseen situations, and then emulating such actions. This paper highlights the importance of predicting and monitoring the results of applying generated control rules to the plant, and re-generating new control rules in the case that the unforeseen situation could not be restored to a normal situation. The proposed architecture has been successfully applied to an experimental thermal power plant control system.

Key Words: expert system, model-based reasoning, plant control, unforeseen situation, thermal power plant

1．はじめに

各種プラントの大規模化，複雑化にともない，ますます経済的で高信頼なプラント運転が求められつつある．それに応えるように，発展する計算機技術を取り込み，プラント制御の自動化は進展してきた．しかし，上位レベルのプラント制御は高度な判断を要するため，まだ自動化できずに熟練運転員の判断に頼る部分が残されている．

この問題を解決するため，最近，エキスパートシステム（ＥＳ）技術をプラント制御に適用する研究が行われている[1]．熟練運転員のノウハウを，予め計算機内に取り込み，計算機自身に熟練運転員並の判断力をもたせようとするものである．

しかし，従来のＥＳでは，想定された状況にしか対処できないという脆弱性が指摘されている．これは，ＥＳ内にプラント操作知識が存在する状況でのみ有効なことを意味している．ところが，熟練運転員ならば想定外の事態が発生しても，適切にプラント操作を行っている．彼らは，プラントの構造，機能，一般的に成り立つ物理法則等の知識を駆使し，経済性，安全性等の要請を勘案した操作知識を生成しているのである．

熟練運転員の確保は一層難しくなる昨今，このような熟練運転員並みの機能をもつ自動化システムの実現が待ち望まれている．

このような要請に応えるため，われわれはモデルベース推論技術を使い，想定外事態に対処できる制御ＥＳを開発している．これまでに，本システムのサブシステムである，定性因果ネットワークに基づく異常診断機構[2]，モデルベース推論を利用した異常状態回避用操作の生成機構[3][4]，ファジー化定性推論による操作知識の検査機構[5]について報告した．文献[4]では，操作の生成・検査機構の詳細と，実験によるその部分の評価を述べた．

本論文では，想定外事態の発生に対して，その発生の検出から，対策操作を生成し，正常状態へ回復するまでの一連の機能を達成する制御システム全体を対象に述べる．まず基本的考え方と構成方式を提案した後，これまでに開発したサブシステムを統合し，完結したシステム構成を提示する．それにより，制御システムとしての有用性，およびＡＩ技術の実用的価値を示す．なお，文献[4]と重複する，操作の生成機構とそこで用いられる深い知識，については必要な記述にとどめる．

２章では，プラント制御における想定外事態について考察する．３章では想定外事態が発生した場合の熟練運転員の認知行動を分析し，それに基づき４章で想定外事態に対処する制御ＥＳのシステム構成，備えるべき機能，知識を提案する．その後，火力発電プラントを対象にこれらの機能，知識を実装し，その有効性を確認する．最後に，本システムの特徴と限界につき考察する．

なお，上記の操作知識のようにタスクを直接実行する知識を浅い知識と定義し，また，上記のプラントの構造，機能や物理法則のように浅い知識を生成する能力をもつ知識を深い知識と定義する．浅い知識が欠如した場合，深い知識からモデルベース推論技術を使い浅い知識を生成する試みは，診断分野を対象に研究されている[6]が，制御分野で，かつ本格的にシステム化された例はない．

2．プラント制御における想定外事態

2．1　制御階層

通常，プラントの運転制御システムの構成は，監視制御，サブシステム制御，直接制御の３階層に分けられる．運転員は，この中の監視制御階層に含められているが，制御の流れを強調するために運転員を独立させると，Fig. 1に示す４つの流れがあることがわかる．

直接制御階層では，プラント機器から得られたセンサデータを基に，予め設定された制御ロジックでプラント機器を直接制御する．サブシステム制御階層では，プラント内のサブシステム単位に，与えられた制御アルゴリズムに従い制御を決定する．監視制御階層では，主にシステム全体が安全状態に，あるいは最適な運転状態に保たれているか監視し制御する．もし，監視制御階層の計算機自身で判断できない異常があれば運転員にアラームを出し，運転員の判断を受ける．運転員は，プラントの状況から次にとるべき操作を決定し，システムに伝える．本論文での議論は，この監視制御階層が中心となる．

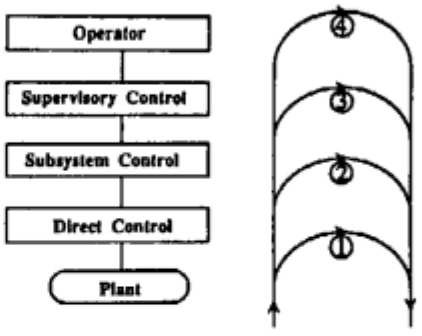


Fig.1 Plant control layers and control flow

2．2　異常状態の原因

一般に，プラントは許容された運転条件内で，与えられた目標性能の実現をめざし運転されている．これを正常状態と呼ぶ．異常状態とは，運転条件が許容範囲を逸

脱したり，目標性能が発揮できない状態をいう．以下に，異常状態の原因を種々の観点から分類し，本論文で取り上げる範囲を設定する．

1) なぜ異常状態が起きたのか，その理由[7]を挙げる．
   ① 機器の設計基準を越えた厳しい環境条件
   ② 地震，火災などの外部的事象
   ③ 設計ミス，製造ミス，保守・点検ミス，運転時の人的ミスなど人間の過誤
2) 異常原因の発生を場所別に分類する．
   ① プラント機器側
   ② 制御システム側（センサ故障，制御用計算機故障）
3) 異常の原因となった故障の多重性により分類する．
   ① 単一故障
   ② 多重故障
      ・複数の機器が同時に独立故障
      ・一つの機器の故障が，機能的接続関係，もしくは空間的接続関係にある他の機器に波及（従属故障／共通原因故障）．

以上の分類を基に，本論文で対象とする範囲を以下に示す．故障の多重性については，単一故障・多重故障ともに対象範囲とする．異常原因の場所は，プラント機器側と制御システム側に大別できるが，研究の第一段階として，より重要で実用上の要請の強いプラント機器側に限定し，制御システム側は正常であるとする．異常の理由については，すべてを対象範囲とする．

2．3 想定外の事態

通常，プラント制御システムには，想定される状況毎に実行すべき操作が知識として蓄えられている．これが制御分野における浅い知識である．想定内の事態とは，Fig. 1の③の流れで，浅い知識を基に計算機が自動的に対処できる事態をいう．一方，想定外の事態とは，制御システム内にこのような浅い知識が蓄えられておらず，Fig. 1の④の流れで運転員に対処を委ねる状況をいう．以下では，どのような場合，2.2 節で述べた異常原因に対処する浅い知識が欠落するか考える．

1) 設計時に欠落する場合
   ① 2.2 節で異常の理由として挙げた，環境条件変化，外部的事象，人間の過誤，において想定内に含めなかった．
   ② 原因と結果の関係が非常に遠く離れる等の理由で，結果が想定できなかった．
   ③ 個々の故障は想定内でも，それらが組み合わさったため複雑で考慮しきれなかった多重故障．
   ④ 多重故障のケース数は膨大なので，どうしても絞らざるを得ず，結果的に漏れが発生した．
2) プログラミング時に欠落する場合

プログラミング段階で入り込んだプログラムミスは，その後の検証・検査により取り除かれるが，ミスが残った時は，次の２種類のケースのいずれかになる．

   ① 対応プログラムが欠落するケースで，結果的に設計時の問題と同じになる．
   ② 対応プログラムが誤った操作を行うケース．2.2 節で述べた制御システム側の異常原因に含めることができる．

以上から，本論文では，（制御システムにとっての）想定外の事態とは，上記1)で述べた，設計時に対処する制御知識が欠落した異常状態と定義する．これは制御システムの計算機内に対処知識が存在しないことを意味しており，運転員にとって想定外か否かの問題ではない．

3．想定外事態に直面した熟練運転員の行動

２章では，制御システムにとっての想定外事態を定義したが，本章では立場を変え，運転員にとっての想定外事態が発生した場合，運転員はどのような行動をとるか観察する．それは，熟練運転員は想定外事態が発生しても対策を考え問題解決を行っており，したがって，熟練運転員の認知行動は，制御システムにとって想定外事態に対処する際の参考になるからである．

一般に，プラント内に異常が発生した場合の運転員の行動様式には，J. Rasmussen[8]によれば，次の３つの型がある．

1) スキル型行動：異常に対して予め定められた応答をする．
2) ルール型行動：過去の経験等から作成されたルールに従い，システムの現在状態から目標状態にいたる操作手順を決定し実行する．
3) 知識型行動：プラントの現在状況に直接適用できるルールがない場合，プラントの構造，機能等に関する知識（深い知識）から，現在状況の把握，目標状態の決定，手順のプラニングを行い実行する．

このうち1)，2)は想定された事態に対処する場合であり，定められた行動をとる．3)は，未経験な事態に直面した運転員の行動であり，運転員にとっての想定外事態の発生時に相当する．以下では，3)についてさらに詳細なステップに分解する．

（１）異常状態の把握：センサデータを観察し，プラント内の状況を把握する．

（２）異常原因の追求：対象プラントに関する深い知識を用い，異常状態をもっともよく説明する原因を探す．原因には，故障発生メカニズムを指す場合と，故障箇所を指す場合があるが，運転員の第一の狙いは，メカニズ

ムではなく，故障箇所の特定である．故障箇所も詳細に絞るのではなく，あるまとまり単位，たとえば，予備系との切り替え系統単位で利用可能か否かを判断する．

（３）異常状態回避操作の決定：目標性能をできる限り維持しつつ異常状態を回避できる新たな目標状態を考える．次に，現在状態から目標状態へ至る操作群を決定する．この時も深い知識を利用する．

（４）操作群の実行条件決定：操作群の実行プラン（順序，タイミング，確認条件等）を決定する．この時，対象プラントの動特性に関する知識を使い，プランの決定と並行的にプラントの状態変化を予測し，安全性と正当性の検証をする．

（５）異常状態回避操作の実行・監視：実行プランにそい，プラント機器を操作実行し，予測通りにプラント状態が推移するか監視する．

（６）回避操作の再導出：予測通りにプラントが推移しない場合は，再度（１）に戻り，異常原因の同定とそれに基づく回避操作の再導出を行う．

このような試行錯誤過程が繰り返される．

以上の過程の中で，運転員が使用している知識は，対象プラントの深い知識であり，問題解決手法は深い知識を基にしたモデルベース推論であることが分かる．

想定外事態に出会ったときの熟練運転員の行動の特質は，異常状態の回避操作を生成する能力が高いことはもちろんであるが，その他の特質の第１は，観察結果を多く使うことである．第２は，状況理解，および対策操作をとった場合，逆にとらなかった場合の状況予測，が的確にできることである．第３は，視点を種々切り替え試行錯誤的に新たな操作案を迅速に創出できることである．通常，運転員はある故障仮説を立て，それに対する回避操作をした時，予測通りには状態推移しなかった場合，最初の仮説に固執し易く，修正は難しい[7]．しかし，熟練運転員ならば，誤判断に気付き，多様な視点から新たな故障仮説を考え，迅速に回避操作をとることができる．

以上述べた熟練運転員の認知行動とその特質を計算機上に実現することが，想定外事態に対処する制御ＥＳ構築の基本的な方針である．

４．想定外事態に対処する制御ＥＳ

４．１　制御ＥＳの構成

本制御システムの目標は，プラントの正常運転の継続と，プラントに（制御システムにとっての）想定外事態が発生した時，運転員の助けを借りずに正常状態に回復することである．そのために，従来の，運転員を含めた監視制御階層を２階層にし，一つは想定内事態に対処する制御階層，他の一つはそこでは対処できない事態に対処する制御階層，からなるシステム構成にした．前者を正常時推論機構，後者を異常時推論機構と呼ぶ．Fig.２に制御システム全体の構成，および正常時推論機構と異常時推論機構の内部構成を示す．サブシステム制御階層と直接制御階層は，従来のプラント制御システムで実現されている構成通りである．

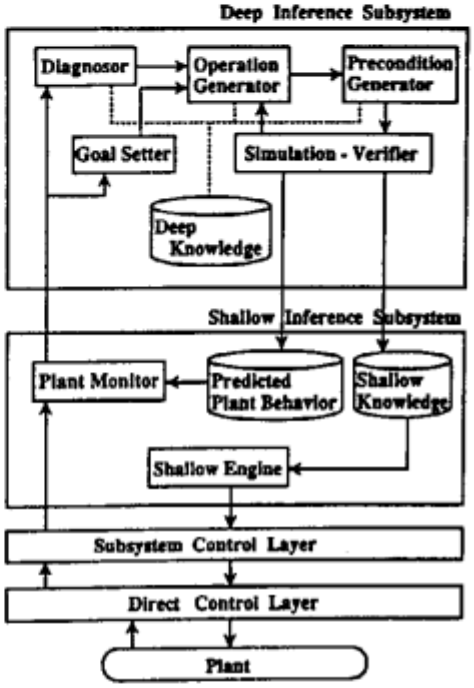


Fig.2 System configuration

４．２　正常時推論機構の知識と機能

想定内のプラント状況に対処する操作知識は，ルール形式で表現された浅い知識である．この浅い知識と，ルールベース型推論により，リアルタイム制御，および異常時推論機構との連携を実現した．

（１）　操作知識（浅い知識）の構造

操作知識は，条件部と操作部がIF-THEN 形式で表現される．その条件部は，一般的に次の３条件で記述できる．

①タイミング条件：運転効率および操作順序への考慮から決まる操作の実行タイミング条件．

②操作前条件：安全上の考慮から操作対象機器が操作可能状態であることを規定する条件．

③　完了条件：操作を実行した結果の完了状態を確認する条件．

（２）　状態監視機構

プラントからデータを取り込み，その状態を監視することにより，変化データ認識と異常検知を実現している．異常検知は，変化データから，想定内事態か，想定外事

態か判断する．想定内事態の場合は，次に説明するトリガアクション機構を起動し，想定外事態の場合は異常時推論機構を起動する．

想定外事態か否かの判断は，個々のプロセスデータの変化を予測し，予測値からの逸脱開始後，一定時間経過後も設定値以上のずれがある場合を想定外とした．予測値からのずれが発生しても，対処できる浅い知識があれば予測値に戻るはずであり，戻らないのは浅い知識が欠落していると推測できるからである．

また，プロセスデータに重要順に優先度を割付け，その順にスキャンすることにより，重要な事態の発生ほど迅速に検知ができるようにしている．

（３） トリガアクション機構

状態監視機構から変化データ（プロセス変数名とその値）を受け取ると，それを条件部に含む操作知識をアクション候補としてトリガする．トリガされた操作知識の中から実際に実行される知識が選択されるが，無駄なトリガを防ぎ処理効率を向上するため，操作知識とプロセス変数のグループ化を事前に行っており，実行すべき操作知識のフォーカシングを実現している．また，後述する異常時推論機構で生成された操作知識との競合を避けるためにも，操作知識のグループ化が必要となる．

４．３ 異常時推論機構の知識と機能

ここでは，異常状態を回避し，正常状態に回復するための操作知識を生成する．生成手順は，３章で述べた熟練運転員の手順にほぼ沿っており，大枠はGenerate-Test-Modifyの枠組みで表現できる．Generateには故障仮説の生成と操作知識の生成，Testには計算機内部での検査とプラント上での実行検査，Modifyには再診断と再操作知識生成の過程がある．

（１） 故障仮説の生成

プロセスデータから異常の徴候を見いだし，その原因を同定する．想定外事態であるから，異常事象の波及メカニズム，すなわち，故障モデルは予め用意されてはいない．したがって，正常機能に関するモデルから原因を推論する必要がある．原因といっても３章で見たように，熟練運転員は詳細なメカニズムを調べるのではなく，異常回避に必要な単位の異常発生箇所を知ろうとしている．本システムでも異常箇所が導出できればよいとした．一方，多重故障は，実用上重要であり，本システムの対象範囲である．

以上の要請に応えるため，われわれは定性因果モデルを用いたモデルベース診断方式を開発した[2]．定性因果モデルは，対象プラント内の変数間の因果関係（深い知識）を定性的にモデル化したものであり，全体で一つのネットワークを構成する．ある変数の正常値からの偏差（徴候）に対する原因候補の集合は，このネットワーク上の伝播で定性的に求めることができる．このようにして（徴候，原因候補の集合）の組み合わせをすべての徴候に対して求めた後，徴候が同時に観測されるための原因候補の最小な組み合わせをクラスタリングによって計算する．最後に，もっとも可能性のある原因候補の組み合わせを絞り込む．この組み合わせを故障仮説を呼ぶ．Fig.3 に以上の手順を示す．この際，熟練運転員の特質と同様，あらゆる観察結果を有効に利用し，原因候補を幅広く考えつくこと，及び探索の絞り込みに利用することが特徴である．

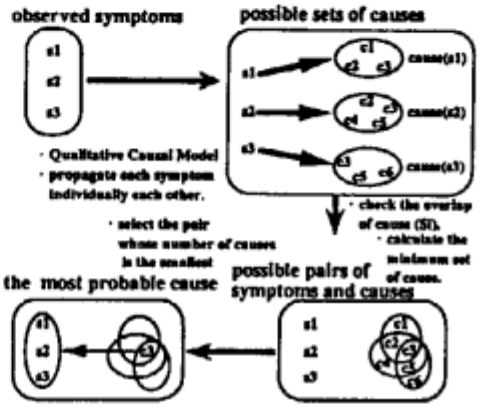


Fig.3 Diagnosis by qualitative causal model

（２） 異常状態回避操作群の生成

現在の異常状態から目標状態にプラントを導く操作知識を推論により導出する．目標状態とは，各機器に与えられた出力要求と制約を満足する状態である．生成する操作知識は，浅い知識と同じ表現とする．ここでは，操作部で示される各機器の操作を導出するが，その導出方法を説明する前に，利用する深い知識について述べる．

３章で見たように，熟練運転員は深い知識を利用し操作を導出しており，同様に，本システムにも以下に示す深い知識を用意する．

① プラント機器構成（機器モデル）

プラント構成機器毎に定義され，構造や機能上の制約条件を記述する．以下に一般的な機器モデル表現に含まれる項目を示す．「スロット：値」の組による記述と，階層的な継承関係の記述が可能である．

name:	機器名
demand:	パラメータ毎の要求値の組
goal:	demandの充足条件
states:	機器の取り得る状態とパラメータ間の関係式により表された機器の機能
operation:	機器に対し可能な操作

quality: operation によりプロセスへ与える可能な操作量
flow-in: 入力側接続機器
flow-out: 出力側接続機器
system: 上位階層関係

この機器モデルが，深い知識の要件，すなわち，浅い知識を生成できるだけの情報を備えているか見てみる．制御システムにおける各機器の役割は，要求(demand)を受け取り，それを達成するためにあるoperation を実行することであり，要求の達成はquality に記述される可能な操作量によりgoal条件が充足されたか否かにより判断できる．operation の実行により，ある状態(old state) から次の状態(new state) へ変化する．浅い知識の中の操作部は，この時選択されたoperation である．条件部の内，タイミング条件は，flow-in/flow-outに規定された操作の順序条件，および運転効率を考慮したquality の可能操作量から，操作前条件はold state から，完了条件はnew state から決定できる．すなわち，機器モデルは浅い知識を生成できる能力があることが分かる．

② 運転原則モデル

運転上守るべき条件であり，絶対条件と機器選択条件からなる．絶対条件は，安全上絶対に守るべき原則であり，たとえば，「故障機器の使用禁止」，「制限値範囲内での機器使用」等がある．機器選択条件は，効率上守るべき条件であり，たとえば，「機器は最少台数で運転」，「同種の機器は均等に使用」等がある．

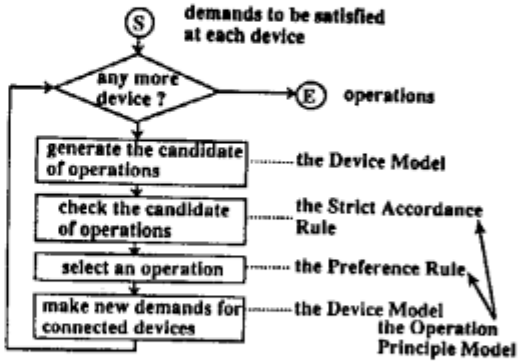
この運転原則は，推論時に要求値や状態変化パラメータが機器モデルで示されるプラント系統を伝播するとき，要求値の展開方法や状態の枝刈りをする際の判断知識である．生成される浅い知識の最適化の保証を左右し，プラント全体に共通する抽象度の高い知識である．

これらの深い知識を使った，異常状態回避操作の導出手順をFig. 4 (a) に，概念をFig. 4 (b) に示す．

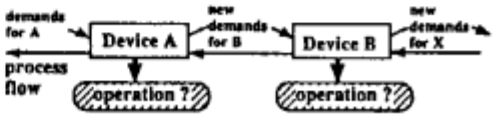
一般に，プラント内の異常発生により，ある機器の制約違反が引き起こされ目標状態からはずれる．そこで，機器モデルを用い，各機器ごとに要求を達成し制約を満たす状態に遷移させる操作を推論により求める[1]．上流の機器に対しては新たな要求を発行する．上位階層の機器モデルからは，下位階層の機器に対し要求の実現を依頼する．機器に要求を満足する能力がない場合はバックトラックし要求の変更を依頼する．以上の処理を，新しい要求が以前の値と同じになるか，あるいは要求の発行先がなくなるまで繰り返す．

（3） 操作条件の生成

生成された操作群に対し，実行順序や実行可能条件を求め，実行プランとする．実行順序は，プラントの設計方針に基づき決める．すなわち，機器の起動に関する操作は，プロセスの流れ，たとえば水の流れの上流から下流に向かって行う．機器の停止操作は，その逆に行う．実行可能条件は，4.2 節で示した浅い知識と同じ表現をとる．いずれも機器モデルから導出できる[1]．



(a)Flow chart of operation generator



(b)Demand propagation along with process flow

Fig.4 Generation process of operations

（4） 生成知識の検査

以上の過程で，目標状態へ遷移可能な操作知識が生成できた．しかし，過渡状態における動特性はまだ考慮していなかったので，各プロセス変数の値が過渡状態でも制限範囲内にあることを検査する．制限範囲を逸脱する場合は，異常状態の回避操作導出に戻る．

動特性も対象プラントの深い知識であるが，操作知識の生成時に動特性も考慮するのは計算量の問題が出てくるので，まず静的関係で操作知識を生成し，その後動特性を考慮した検査する方法をとっている．

過渡状態を知るには，対象の動特性を厳密に数式でモデル化しシミュレーションすることが考えられる．しかし，ここで扱っている想定外の事態に対して，予め厳密な数式モデルが用意されていることは期待できない．では熟練運転員は，どのようにして過渡状態の安全性を確認しているのであろうか．彼らは，厳密な数式モデルに基づき評価しているのではなく，自分が理解した対象プラントの挙動に関する定性モデル（メンタルモデル）を基に判断しており，それでほぼ目的を達成している．本システムでも，対象プラントの正常時，異常時における定性モデルを使い，生成知識を検査する．手法としては，

定性シミュレーションを採用する．ただし，一般的には，本手法は定性的なあいまい性により推論結果が一意に定まらない可能性がある．われわれは，ファジー推論機能を付加して一意の解を得られるようにし，熟練運転員と同様な検査過程を実現した[7]．

（５）　実行・監視

生成された知識は，正常時推論機構に送られ実行される．

本システムは，時間とともに状況が変化するプラントをリアルタイム制御しているので，厳密には計算処理中の状況変化を考慮すべきである．しかし，監視制御層に対して厳しいリアルタイム性は要求されないことと，プラントの状況変化に比較して計算処理は十分に速くできることから，生成された知識の実行タイミングの問題はないとして処理を行う．

生成知識の正当性が計算機内で確認されても，それを実際にプラントに適用した場合，プラントが予想通りの挙動を示すか監視する必要がある．もし，予想通りには異常回避が推移しない場合，上記（１）～（４）の機能を再実行できるシステム構成が必要になる．３章で見たように，想定外事態に出会った時の熟練運転員の認知行動の特質の一つは，最初の判断の誤りを認め，新たな視点から操作手順を生成し再実行することである．同様な機能を持つシステムを実現するために予測，実行監視，再診断，目標再設定の各機能が必要になる．

予測値は，生成知識の検査時にファジー化定性推論にて得られた過渡状態を利用すればよい．実行監視機能では，この予測値とセンサから得られた実測データと比較し，一致しない場合，前回の診断結果は誤りと判断し再診断に入る．

（６）　再診断

再診断では，前回と異なった異常原因を求めるが，前回とは時間が経過していること，および対策操作を加えたこと，によるプロセス状態変化を考慮する必要がある．この時見られる異常に関する徴候は，以下の３タイプに分類できる．

① 変化しない徴候：対策操作が全く効果がなかったプロセス変数．

② 新たに発現した徴候：対策操作により，偏差が発生したプロセス変数．

③ 消滅した徴候：対策操作により，異常の原因が消滅した，あるいは相殺されたプロセス変数．

再診断にあたっては，最初の診断で用いた定性因果ネットワークを再利用し，新たに発生した徴候，消滅した徴候に関する偏差のみを伝播することによって，（徴候，原因候補の集合）の組み合わせ情報を効率よく修正する．クラスタリングを再実行することによって，再び故障仮説が生成されるが，「第１回目の診断結果」に関する故障仮説は排除する．

（７）　目標値再設定

一般に，プラントの運転状態は次の３つに分類できる．

① 起動：現状から，目標負荷へ到達．

② 停止：目標負荷を零にし，プラントを停止．

③ 通常運転：目標負荷運転．

起動，通常運転中に異常が発生した場合は，目標を下げず，異常回避努力をするが，困難な場合は目標負荷下げをする．さらに，目標を下げても運転が困難な場合は停止状態に移る．

以上の，再診断で求めた新たな異常原因と，目標値再設定で求めた新たな目標値を基に，再度（２）の異常回避操作の生成を実行する．

５．　想定外事態に対処する制御ＥＳの実現

火力発電プラントを対象に，上記考えに基づく制御システムのプロトタイプを構築し，その有効性を確かめた．

５．１　システム構成

対象とした火力発電プラントの構成をFig.５に示す．本制御システムは，機能検証用なので実際の発電プラントと接続する代わりに，発電プラントシミュレータを利用した．また，制御システムは並列推論計算機マルチＰＳ１上にＫＬ１言語で実装した．

５．２　深い知識

火力発電プラントの主要系統である燃料系，給水系，復水系，循環水系の主要機器につき合計７８個の機器モデルを実装した．Fig.６に給水ポンプの機器モデルを示す．

Fig.７に定性因果モデルの例を示す．同図（ａ）に因果関係式を，同図（ｂ）に結合したモデルの一部を示す．

Fig.８にファジー化定性モデルの例を示す．同図（ａ）は脱気器のレベル制御系，同図（ｂ）はその定性モデル，同図（ｃ）は定性演算の例であり，通常の定性演算では不確定となる値（例えば，正値と負値の和）も同図（ｄ）に示すメンバーシップ関数によるファジー演算により一意の解を求めている．

５．３　動作例

想定外事態として，循環水ポンプ性能低下と主エア・エジェクション蒸気圧力低下が発生，という二重故障による復水器真空度低下をプラントシミュレータ内に設定する．想定外事態とするため，浅い知識ベースから対応する操作知識を取り除いた．実行監視結果から再診断機能を働かせるため，最初は循環水ポンプの性能低下のみの異常とし，その対策操作導出中に主エア・エジェクシ

ョン蒸気圧力低下が発生する状況を設定した．

Fig.9(a) は，真空度の予測値と観測値のトレンドである．①は，循環水ポンプの性能低下が発生したため，真空度が低下したことを示している．その故障原因は，Fig.9(b) の●で示すポンプであることが異常時推論機構により同定され，対策操作が導出・実行される．Fig.9(c) に対策操作の一部を示す．その結果，Fig.9(a) の②のように観測値は変化するが，この対策操作導出中に第二の故障である主エア・エジェクション蒸気圧力低下が発生したため，予測値通りにならなかった．そこで，再度，故障原因の同定が行われ，エア・エジェクション弁の一つに原因があることが分かったので，対策として弁の切り替え操作が再導出され実行された結果，Fig.9(a) ③に示すように予測値通りに整定した．

以上で，想定外事態の二重故障による影響が無事回避されたことが分かる．

6．考察

従来のシステムや，熟練運転員と比較しながら，本システムのシステム構成上の特徴と適用限界を考察する．

（1） 制御の階層性

従来のプラント制御系で実現されている各階層は，十分考慮され，実績もあるので，できる限り利用し，その上に想定外の事態に対処する階層を設けた．本システムの狙いは運転員の代行にあり，新たな階層は従来の運転員階層に相当する．想定外事態への対処をめざした他のシステム[10] が，運転員の支援を行うのに対し，本システムは運転員の代行を実現している．

（2） 正常時推論機構と異常時推論機構の連携

通常は正常時推論機構が働いているが，想定外の事態が発生すると，異常時推論機構が起動されるとともに，プラントの状況が知らされる．また，異常時推論機構で生成した操作知識とプラント挙動の予測値は，正常時推論機構に渡され，操作知識は実行され，予測値はプラント状況の推移監視に利用される．すなわち，状況に応じて，両推論機構は相互起動と知識の交換を行う．

（3） 実行フィードバックループを形成

制御システムとプラントの間で，フィードバックループが形成されている．すなわち，制御システムは，深い知識から浅い知識を生成するだけでなく，生成した浅い知識でプラント操作を行い，その状況を実行監視し，問題があれば再度知識生成部にフィードバックをかける．

これは，プラントは時々刻々変化すること，モデル化にあいまい性を含まざるを得ないことによる．また，予備機器への切り替えを試みた結果，その予備機器も故障であることが発見されるケース（潜在故障の顕在化）等，実行してはじめてわかることもあるためである．したがって，生成された知識を実際にプラントで確認することと，必要ならば再推論により修正できることが必須となる．機器レベルの制御系においてフィードバック機構が安定性に重要であるのと同様，最上位レベルにおいてもフィードバック機構は重要な役割を果す．

再推論の時，本システムでは診断過程で新たな仮説を求めているが，前回の仮説は変えず，生成過程で新たな操作を，前回の操作が失敗したことを考慮して探索することも考えられる．今後の検討課題である．

なお，故障診断分野で再診断を扱った関連研究[11] はあるが，故障モデルを準備する必要があり，想定外事態には使えない．

（4） 学習能力の可能性

異常時推論機構で生成された浅い知識は，正しく想定外異常を回避できるか確認される．確認後，浅い知識ベースに新たな知識として登録することにより，正常時推論機構の問題解決能力を向上することができる．ただし，現在は知識の汎化を行っていないので，全く同じ状況が発生した場合のみ再利用が可能である．汎化は，将来の課題である．

（5） 対処できる想定外事態の限界

現在，すべての想定外事態に対処できるのではなく，プラント内の異常に限定している．制御システム側の機器に関する異常は対象外であり，今後の課題である．

プラント内の異常であっても，常に正しく異常回避できる保証はない．また，深い知識のない部分の異常に対しては対処ができない．このような限界があるので，実用システムでは運転員は必要であり，その重要性は減るわけではないが，本システムにより運転員の労力の軽減とミスの減少が期待できる．

（6） 熟練運転員との比較

実験は，実際の発電プラントではなくソフトウェア・シミュレータを用いたので，運転員にとり真に想定外の事態を発生させ，比較することは困難であったが，運転員から見てほぼ妥当な操作を生成できた．

本システムに比較し，熟練運転員が優れている点は，取り扱う想定外の事態の範囲の広さ，経験からの学習機能，プラントの全般的状況を見た柔軟な判断力などである．また，熟練運転員は一つの対策だけでなく複数の対策を並行的に検討し，その中からベストの解を選んでいることや，試みた操作が失敗であったときその失敗経験を生かし別の原因の探索，操作の生成を行っているので，解への収束が早いと言える．

しかし，本システムの特徴は，想定外事態に出会っても冷静に対処でき，ヒューマンエラー（誤判断，誤操作，

見落とし）を防止できることである．

7．おわりに

想定外の事態，すなわち，対象プラントを直接操作する知識（浅い知識）がない事態が発生しても，プラント構造，機能といった深い知識があれば柔軟な対処が可能な制御ＥＳの構築方法を示した．また，その有効性を火力発電プラントへの適用実験で示した．

今後，より広範囲の想定外事象に対処できる制御システムの構築をめざしたい．

本研究はＩＣＯＴからの再委託研究として行われた．ご指導をいただいたＩＣＯＴ新田室長に感謝します．

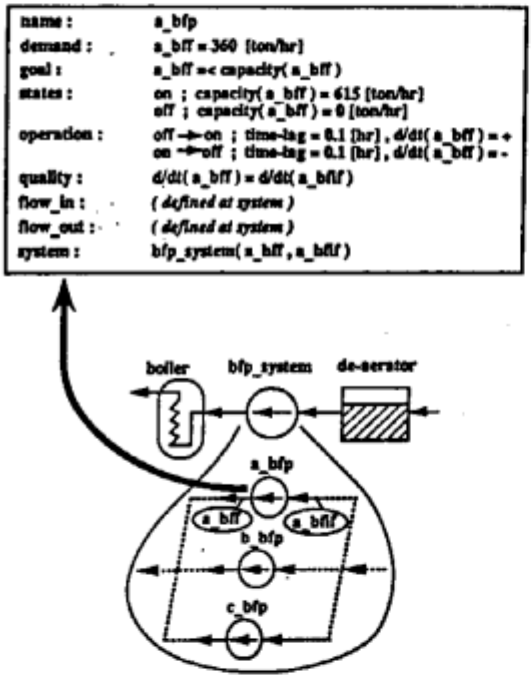


Fig.6 Device model of a pump

参考文献

1) 松本，坂口：制御型知識システム，計測と制御，27-10,887/892(1988)

2) M.Iwamasa,J.Suzuki,S.Hochiji and N.Sueda:Plant Diagnosis with Set Covering and Qualitative Causal Model,Proc. of CAIA92,60/66(1992)

3) J.Suzuki,C.Konuma,M.Iwamasa,N.Sueda,S.Hochiji and A.Kamiya:A Diagnostic and Control Expert System Based on a Plant Model,Proc.of FGCS'92, 1099/1106(1992)

4) 鈴木，田岡，小沼，岩政，神谷，末田，河野：モデルに基づく運転操作プランの生成機構を組み込んだプラント運転制御エキスパートシステム，人工知能学会誌（1993.7掲載予定）

5) J.Suzuki,N.Sueda,Y.Gotoh and A.Kamiya:Plant Control Expert System Coping with Unforeseen Events -Model-based Reasoning Using Fuzzy Qualitative Reasoning-,Proc.of IEA/AIE-90,431/439(1990)

6) 山口，清口，中村，小澤，鳥越，野村，角所：対象モデルと故障モデルに基づく知識コンパラⅡの構築と評価，人工知能学会誌，7-4，663/674(1992)

7) 松岡猛：確率論的安全評価における従属故障と外的事象，システム／情報／制御，36-3,158/170(1992)

8) J.Rasmussen:Skills,Rules,and Knowledge;Signals,Signs,and Symbols,and Other Distinctions in Human Performance Models,IEEE Trans. on Systems,Man,and Cybernetics, SMC-13-3,257/266 (1983)

9) G.Salvendy編，大島正光監訳：ヒューマンファクター－新人間工学ハンドブック，1446，同文書院 (1989)

10) K.Honta,J.Itoh and H.Hakino:An Advanced Man-Machine System for BWR Nuclear Power Plants, Proc. of IEEE Fifth Conference on Human Factors and Power Plants,1/10(1992)

11) D.Dvorak and B.Kuipers:Model-based Monitoring of Dynamics Systems,Proc. of IJCAI89,1238/1243 (1989)

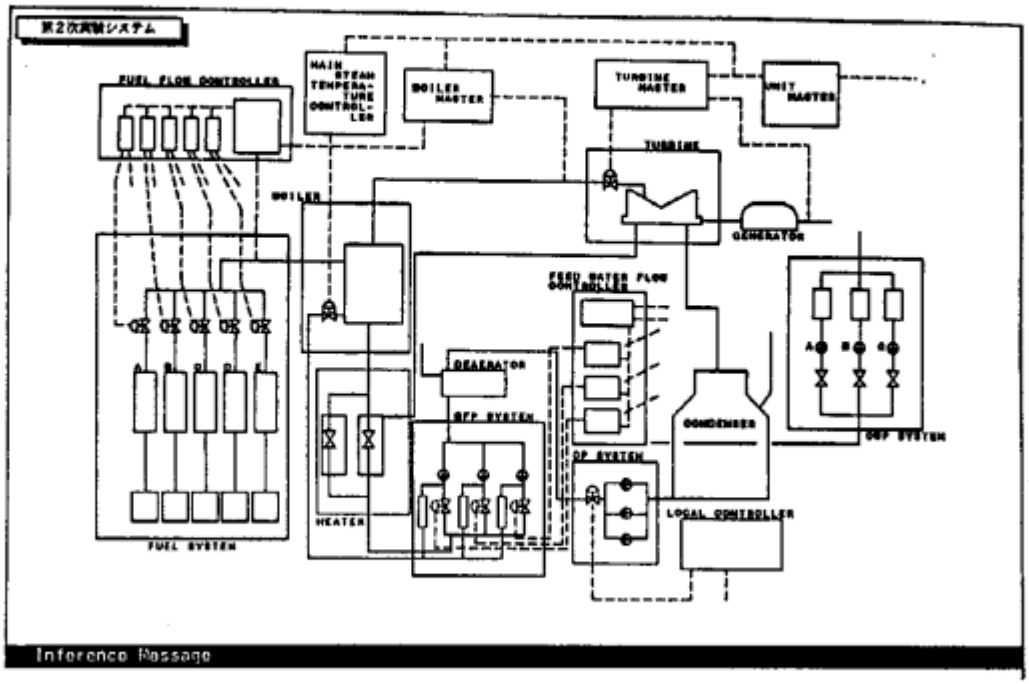
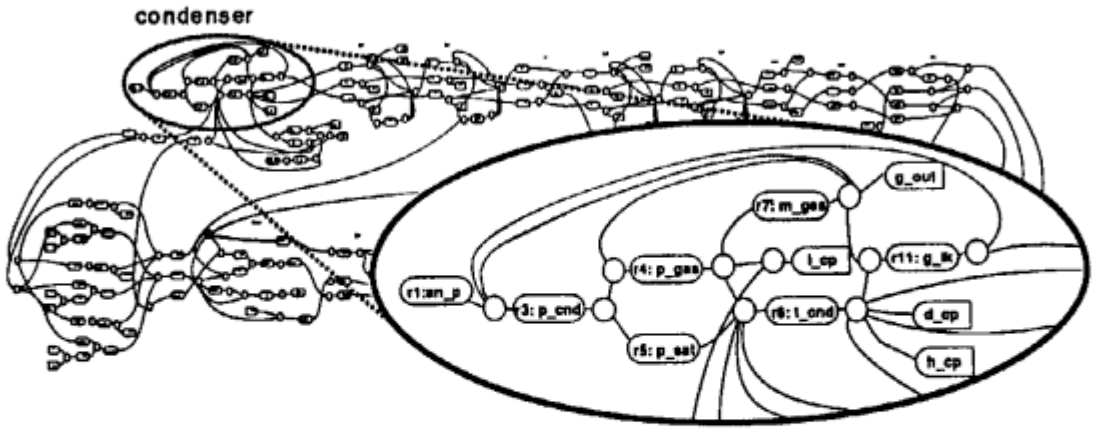


Fig.5 Thermal power plant configuration

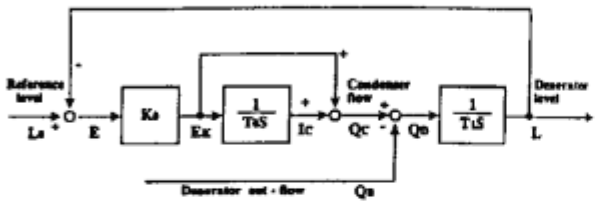
```
r1: an_p   <- {(+:p_cnd),(-:)}
r3: p_cnd  <- {(+:p_gas,p_sat),(-:)}
r4: p_gas  <- {(+:m_gas,l_cp,t_cnd),(-:)}
r5: p_sat  <- {(+:t_cnd),(-:)}
r7: m_gas  <- {(+:p_gas,g_lk),(-:g_out,.p_cnd)}
r6: t_cnd  <- {(+:g_cndi,h_cndi),(-:g_lk,d_cp,h_cp,h)}
r11: g_lk  <- {(+:g_cndi),(-:p_cnd)}
```

(a)Constraints



(b)Qualitative causal network

Fig.7 Qualitative causal model



(a) Block diagram of deaerator level control

minus (ml, l)
add (e, l0, ml)
coef (ek, k0, e)
coef (et, t0_inv, ek)
integ (ic, ic0, et)

add (qc, ek, ic)
minus (mqb, qb)
add (qd, qc, mqb)
coef (qt, tl_inv,qd)
integ (l, l0, qt)

(b) Qualitative Model

add (W, X, Y) W = X + Y

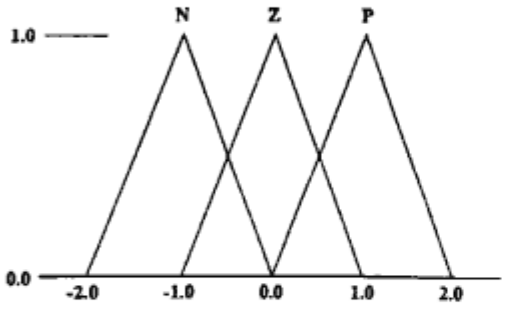
Y \ X	P	Z	N
P	P	P	Z
Z	P	Z	N
N	Z	N	N

P : Positive
Z : Zero
N : Negative

Rules

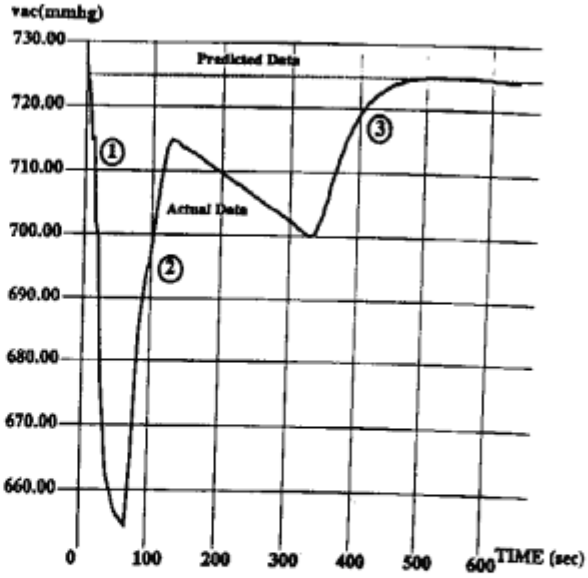
add 1 IF X is P and Y is P THEN W is P
add 2 IF X is P and Y is Z THEN W is P

(c) Constraints Rules

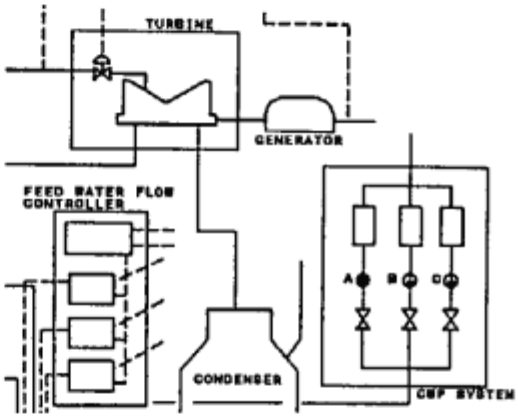


(d) Membership Function

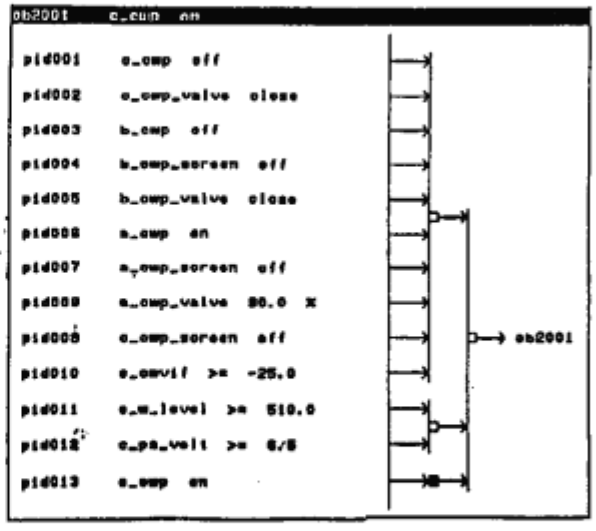
Fig.8 Fuzzy Qualitative model



(a)Predicted and actual plant behavior



(b)Fault diagnosis



(c)A generation operation rule

Fig.9 Operation sequences recovering an unforeseen situation