実践講座 原子力発電所におけるヒューマン・マシン・インタフェースの現状と展望－新提示技術と課題－

原子力安全システム研究所　丹羽 雄二／岡山大学　五福 明夫
筑波大学　古川 宏／宮城学院女子大学　大橋 智樹／東北大学　高橋 信

「原子力発電所におけるヒューマン・マシン・インタフェースの現状・新提示技術と課題」に寄せて

この技術レポートは、平成14年9月20日に大阪科学技術センターにおいて開催したシンビオ社会研究会第2回技術交流会での、「HMIと中央制御室の現状と将来展望:HMIは何故変わらないか、変える方策は何か」と題するパネルディスカッションをもとにしています。そもそもシンビオ社会研究会の技術交流会とは何か？とのご質問があろうかと思いますのでこれを先に説明させていただきますと、これは「エネルギー技術と社会との関わりを共考するフォーラム」と位置付けて行っている筆者主宰の「シンビオ社会研究会」での諸活動の一環として、中央制御室設計、自動化技術、検査技術、試験技術、プラント機器改造など、プラント構造技術、計測制御技術全般の、技術の現状と今後の技術開発課題について、電力、メーカ、大学研究者の間で定期的に技術交流会を行っています。

この第2回技術交流会では、「グローバルで競争力のあるヒューマン・マシン・インタフェース設計」を目指し、前記のようなパネル討論をコーディネータ丹羽雄二氏に企画していただきました。この技術レポートはコーディネーターの丹羽雄二氏を司会者にして、4名のパネラー（五福明夫氏、高橋信氏、古川宏および大橋智樹氏）のパネル当日の話題提供に、その後技術交流会に参加した電力、メーカの方々のコメントを加味して、当日のパネル討論をさらに発展させて上記の方々を筆者にして技術レポートとしてまとめられたものです。

このレポートを一読しますと、その底流には、本来は社会の安定な電気供給を支えるインフラ技術である原子力発電が、「原子力」という現代の世界平和に関わる重要キーワードが定冠詞にあるが故に、社会的に一種独特でナーバスな取り扱い方をされるようになっている現状を背景にしつつ、そのヒューマン・マシン・インタフェース設計のあり方を論じています。そしてその改善が一向に進まない理由として「研究者と現場のギャップ」を論じつつ、結局は現場をインタフェース設計のライフサイクルの上流から積極的にインボルブさせていくアプローチをギャップ解消への有効な道と提起しています。（30年、40年を超えて60年間も使おうとしている）原子力プラントのヒューマン・マシン・インタフェースは、日常的な携帯電話等のインタフェースと比較しますと、使う人の専門性以外に、市場への投入までの時間、実際に製品が使われなくなるまでの使用時間スパンが根本的に異なります。原子力プラントは、むしろ家やマンションなど耐久消費財とよく似たところがあって、プラントの基本構成は同じでもいろいろな部分で改造工事が始終行われます。

そのような原子力プラントの中でも中央制御室は家やマンションになぞらえれば、さしずめ一家団欒の部屋のようでもあり、また一家のすべてを取りしきる奥方様のお部屋のような大事なところですから、そこをもっと快適にするために日常的なリノベーションへの努力を現場のイニシアティブで行っていけるように、大学やメーカの研究者、技術者が現場の方々と協力していくべきでしょう。ただし肝心の原子力の原理を知らないで使い勝手や見栄えだけで工夫しても過日のJCO事故のように現場の人が不幸な事態になるので、「基本は忘れない」ように如何に「安全について技術伝承するか」が大事、という安全確保への熱き思いと深い配慮が筆者の方々の記事全体に込められていることを当方には痛く感じられました。

読者の方々には以上を背景知識に、「インタフェース設計の文化論」として本技術レポートに盛られている筆者諸氏の新たなアイディア提起を参考にしていただければ幸いです。

最後になりましたが、このような技術レポートを快く本会誌に掲載の便をはかってくださいました、会誌委員会幹事の杉原敏昭氏に厚く御礼申し上げます。

吉川 榮和（京都大学）

1．緒言

この数年の間に電力の自由化が社会的な話題となり、原子力についても内部告発による「不具合隠し」の問題も含めて今後の成り行きが注目されている。今まで原子力の将来については余り議論されることがなかった。新設の発電所立地はなくとも、原子力は1つの電源の要素として、必ず生きながらえると原子力産業に従事するものは信じ続けてきた。しかしながら、新たな電源に関する技術は我々が想像する以上に技術革新が進んでいる。このような流れを受け、原子力産業では、さらに省力化、原子力運転の信頼性向上が求められるであろう。

とりわけ原子力発電所の新設プラントがないことから、中央制御室設計やヒューマン・マシン・インターフェース（以下HMIと書く）設計の開発関連については、撤退の動きがあるところも出てきた。一方、学会等に目を転じて見ると従来と変わらず新たな設計が提案されており、それらは斬新で確かに運転の信頼性向上に寄与しそうである。これらの研究成果が今まで通り商用炉に実装されるかを考えた場合、電力等で原子力発電に十分な資金投資が見込めないので、研究に従事するものは、折角新しい概念で設計したHMIが適用されず、研究のための研究に終わるのではないかと疑問を持っている。これは研究や関連業務に従事するものにとって不幸なことである。

このような問題を内含する昨今、研究の進め方に対して研究者自身が「戦略」を持って臨むべき時に来ているのではないか。一言で言えば、大学、メーカーあるいはユーザーが共同しないまま研究を遂行することは、この時代にあっては、時間と資金の無駄である。海外の制御盤やHMIの設計を基本とし、日本の運転員にあった設計原理までを議論しないまま、日本のユーザーが使用するに当たって、一見支障のないように比較的軽微な変更を行うことも、生き残りを考えた場合、得策とは思えない。各々の国情が異なるので、参考にはなっても、そのまま導入するのに無理がある。

従って、本レポートでは、先ず最近の流れである「ユーザー中心の」新しいインタフェース設計の例を課題とともに提案する。これら先進的なHMIの設計研究は日本では専

ら技術系の人間により行われているが、人文系からの設計提案も今後一層重要性が増すであろう。HMI設計研究を社会系－技術系の融合研究と捉え、産業心理の側からHMI設計はどうあるべきなのかの提案について述べる。最後にこれまで先進的なHMI研究が行われてきたにも拘わらず、現場への適用が寡少である事実を鑑み、エンドユーザーにHMI研究の成果が受け入れられるには、どのようなHMI研究の進め方が望ましいかについて議論を進める。

2. 直接的な情報支援と間接的な情報支援

簡単な例を示す。通常エレベータには、扉の自動動作に人間のオーバライド操作を許すものが多く、「開」、「閉」のボタンが付いている。最近のエレベータはデザイン重視のものも多く、開閉の意味がシンボルで示されている場合が多い。ところが、著者の一人はしばしば意味の取り違えをし、逆のボタンを押してしまう。エレベータが閉じかけている場合は、シンボルの意味を理解している時間もないので、適当にボタンを押してしまい、急いで入って来ようとする人は挟んでしまうこともしばしばである。こんな時、逆に昔（今も無論、装備されているが）の実際に字で「開」、「閉」で表示されていたら、多分問題は無かったと著者の一人は思う。このことをもう少し掘り下げて考えてみよう。一般に人間の物事の認知過程はよく知られているように「観測・同定」、「解釈」、「意志決定」、「スケジューリング」の情報処理の流れとしてとらえられる[1]。

上記のシンボルを理解しようという場合、まさにこの過程に従って処理が行われる。ところが、「開」、「閉」を見た場合、人間は日常使う文字に余りに親しんでいるので、この「解釈」というプロセスを一見バイパスするような情報処理が行われる。「解釈」はしているが、軽度すぎて、人間自身解釈しているとは思わないであろう。特に「開け」「走れ」等の命令は、考える間もなく行動を起こすことができる。このように上記のような「構文系」を表示することにより、人間の行動を支援するHMIも考えられる。これを仮に「直接的な情報による支援」（以下、簡単のため直接法と書く）と呼ぼう。直接というのは、観測・同定が、一見処理されずに行動に結びつくという意味で使用している。これに対して、グラフィック表示は、「間接的な情報による支援」（以下、簡単のため間接法と書く）と呼べるであろう。技術的な問題意識を分かりやすく図1に示す。次章では、これらの最新の研究結果について俯瞰する。

3. 直接法

原子力発電所で事故時に参照される事故時手順書EOP (emergency operating procedure) 内の典型的な構文は以下のとおりである：

[操作]::=[条件][行動]　　(1)

また、補足情報はコメントとして書かれている。[条件] が真の場合、指定された [行動] がとられる。この事故時手順書の構文を表示するCPP (computerized procedure presentation system) の基本的な設計方法は、EOPの中のテキストをすべてこれらの3つの要素へ分解し、固定されたパンの中に割り当て、表示することである。これはTiled formatと呼ばれている。運転員が参照すべき箇所は、反転表示により強調される。また、チェックボックスはブリンクしている。条件を満足していることが確認されたり、操作が実施された場合は、当該の箇所にチェックマークを挿入する。チェックマークは、当該のチェックボックスをクリックするか、リターンキーを押すことにより容易に画面上に表示され、CPPは次に参照すべき箇所を自動的に反転表示させ表示する。

事故時の操作の途中で、一連の事故回復操作完了までで自分がどのあたりの操作を把握することは、Human error防止の観点から重要である。これをオリエンテーションの把握と呼ぶ。CPPの画面では、この目的のために、Operations mapというパンを設けている。これは確率論的安全評価で用いられるEvent treeのノードと同じ概念であり、大きな操作の流れがノードで示されている。当該のノードをハイライトを強めて表示することで、運転員の実施している操作が全体の流れのどのあたりに該当するのかの把握を容易にしている。CPPの典型的な画面イメージを図2に示す。

なお、直接法で肝要なことは、このHMIの使用だけでは、人間は操作を行うだけのマニピュレータに陥る危険性がある。また、EOPに状態の確認はあるものの、情報フィードバックが運転員に行われにくいという欠点がある。要は直接法、間接法ともお互いに長所と欠点があるのであり、両者を併用するのが運転操作の信頼性につながるものである。

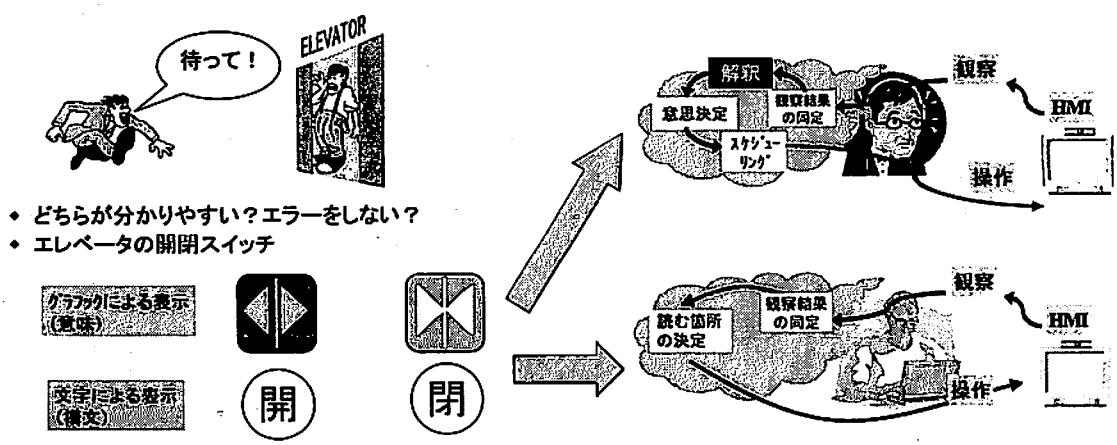

図1　問題提起－構文表示と意味表示

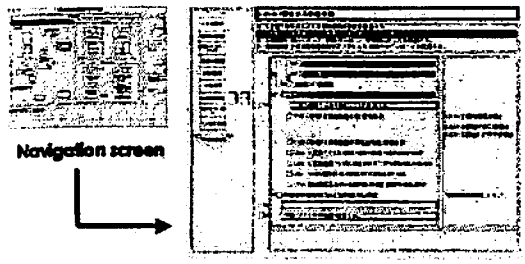

図2 CPPのスクリーンイメージ

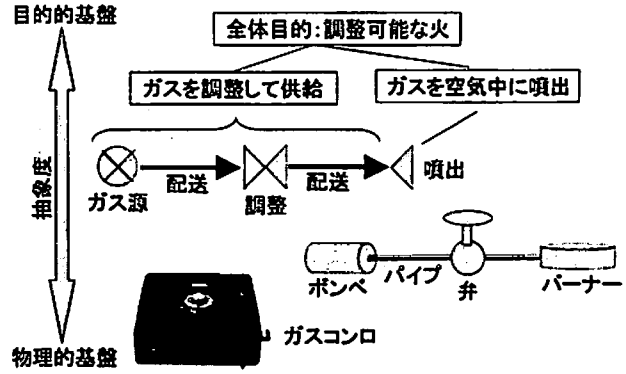

図3 深い知識の表現：機能による目的手段モデル

4. 間接法

間接法、即ちグラフィックに意味を付加することにより、事故時の操作支援にあてようとする研究が世界各国で行われている。我が国でもHMI研究の主流をなしている。それらの内から、特に興味深く、先鋭的な研究を概説する。

4.1 生態学的インタフェースと自動化システム協調支援インタフェース

本節では、大規模複雑システムにおいて今後重要となる想定外事象での支援と自動化システムとの協調支援に注目し、生態学的インタフェース設計論と、自動化システムの意図を明示する協調支援インタフェース設計論の主張とその重要性について概説する。

4.1.1 想定外事象と生態学的インタフェース設計論

生態学的インタフェース設計論（Ecological Interface Design: EID)[2]は誤解の歴史をもっている。「あのEIDは複雑で難しくて運転員には使えない」という声である。このようなとき「あのEID」とは、Vicenteらによる、あるいはBeltracchiが提唱した具体的なHMIのデザインを指している[2,3]。しかしEIDとはHMIの一つの設計原理であり、具体的なデザインを指すものではない。生態学的インタフェース設計論が提唱するのは、大規模複雑システムの制御における

(1) 抽象階層のメンタルモデルとしての適切さ、
(2) 直感的理解が可能なHMIによる抽象階層の外在化の必要性、
(3) スキル、ルール、知識ベース行動（skill-、rule-、and knowledge-based behaviors）の支援に適するデザイン設計の必要性

である[4]。

ここで特に重要となるのは、知識ベース行動を支援するために抽象階層がHMI上に外在化されていることであろう。EIDが想定外や未経験事象における対応支援に有効とされるのは、この抽象階層をメンタルモデルとして用いることにより、運転員はシステムに関する深い知識を利用した知識ベース行動をとり得ると期待されている点にある。スキルおよびルール、すなわち自動的な意思決定を行いうる知識（条件と対応策の対）に対して、深い知識とはシステムの目的、機能、構造、制約に関する知識を言う。事前に対応策が決定されていない事象において、運転員には、まさにこの深い知識に活用することで有効な対応を決定し実施することが期待されている。抽象階層（abstraction hierarchy）とは、対象システムにおける目的と手段の関係を機能により表現した目的－手段モデル（means-end model）である[11]。図3に、カセットガスコンロを例とした抽象階層の概観を示す。

4.1.2 人間と自動化システムの協調のための意図表示インタフェース

安全性や効率を高めるために、原子力プラントや自動車などの多くの人間機械系で、今後自動化が積極的に進められることが考えられる。一方、人と自動系からなるシステムに生じる様々な問題が重要視されてきている[6,7]。そのような課題のひとつに、Automation Visualizingの問題がある[8]。自動化システムの多くは、制御ルール／ロジックが複雑であるのみではなく、多数の制御モード、さらに自動的にこのモードが変更される機構（indirect mode transition）を有していること[18]から、利用者にとって状態を把握することが非常に困難な対象である。これに対し、手順書遵守の十分な訓練を実施している、自動化システムのモードの表示がHMIにある、あるいは、簡単にプロセスパラメータから安全機能が維持されているかどうかが評価できるとして、これまでは状態把握の失敗を利用者の責任としてきた。しかし昨今におけるその結果の重大さから、より積極的に自動化システムの状態について利用者の理解支援を行うことの重要性が認識されてきている。すなわち、自動化システムの導入による認知的タスクの増大は軽視されてきたが、この改善を目指してHMI側からのアプローチを図る考え方である。

これに対し古川等は、生態学的インタフェース設計論に基づいた自動化システムの意図表示インタフェース設計論を提唱している[9,10]。この中心的な考え方は、自動化システムを運転員の1人と仮に置き換えた上で、その目的と手段を抽象階層上に記述し、これをHMI上に明示的に表現することである。例えば架空の温水供給システムは目的－手段展開すると図4のようになる。

制御すべきパラメータが4つあり、1960－70年代では多変数制御理論の典型的な適用例であったが、IT（情報技術）の発展した現在では、プログラム制御の適用が主流であろう。この制御系の場合、温度と設定値の偏差と水位で制御のモードが、温度重視制御、タンク水位制御、水位維持制御モードの3種類に切り替えが自動的に行われるものとする。このような場合、自動系は何をしたいのかという意図

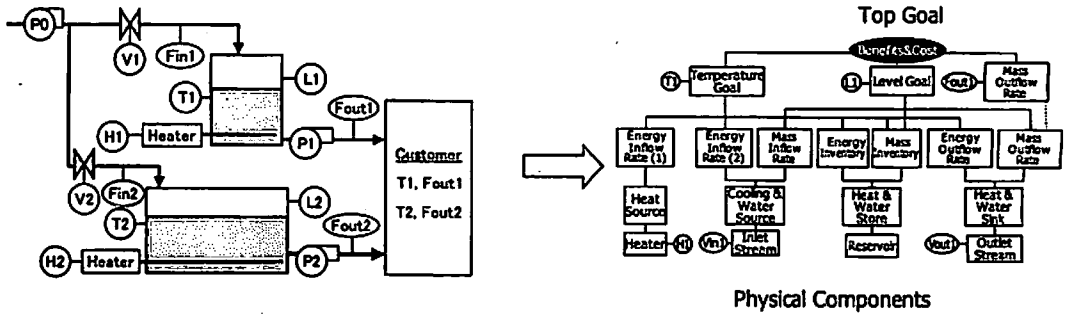

図4 目的・手段の抽象階層の記述例

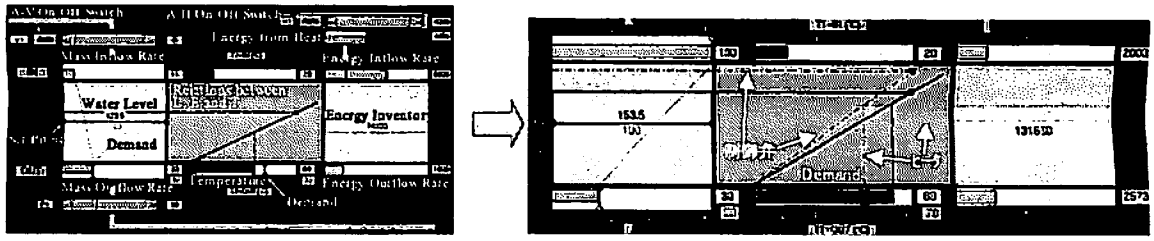

図5 目的・手段の抽象階層に基づいたHMI例

が人間に分からなくなる場合が発生する。このような場合には、現在どのような制御モードにあるかのみの表示では支援として十分ではない。制御すべき変数が複数の場合、人間の目からは互いのパラメータの制御が干渉しているように一見見えるからである。従って、上記のような人間の疑問にHMIは適切な情報提示を行わなければならない。

このような場合には、タンクの水位（質量保存則）と温水エンタルピー（エネルギー保存則）、体積、エネルギー、温度の関係といった制御システムの内含関係を表示することにより、制御系は何故、そのような補償動作をとっているのかを容易に認知することが可能となる。この考えに基づいたHMI画面設計と上記温水供給システムへの適用を図5に示す。

利用者は、自動化システムの目的を把握（goal awareness）し、その手段を把握（means awareness）することで、何をすべき／すべきでないか、何ができるか／できないかを理解することが可能となる。これによって、人間と自動化システムがそれぞれ異なるタスクを実施している状況において（mixed-initiative situation）[6]、相互の干渉を防ぐことができると考えている。このとき、状態把握時の時間制約を考慮し、自動化システムの制御ルール・ロジックを示すのではなく、その目的と手段、およびその関係のみをHMI上に表現する考え方が、これまでのHMI設計概念と大きく異なる点である。

これからの人間・機械システムでは、より複雑な自動化システムの導入がますます進み、これによってよりシステムが複雑となることが予想される。今後、ここで述べたような自動化システムとの協調支援インタフェースの必要性がより一層高まり、新たな設計の基本概念と具体的デザインに関する研究が盛んに行われるようになると考える。

4.2 意味表示インタフェース

この節で紹介するHMIの基本的な発想も機能的な表現を基礎としている。それは運転員がプラントやコンポーネントの目的、役割や設計における制約事項等を把握していれば、単なる操作者ではなく柔軟な発想を持つ知的なエージェントとしてコンピュータの支援を受けながらプラントの運転ができると考えられるからである。意味表示インタフェースのユニークな点は、HMI設計の過程で機能モデルの導入を図り、従来のDigital Control System：DCSと同様に構造や挙動の面からの情報に加えて機能的な情報を積極的に運転員に表示するとともに、プラントの機能モデルを用いて異常時に有効と考えられる対応操作を導出している点にある。以下では、その動作を中心に直接法と間接法との関連について述べる。

意味表示インタフェースは、他と協調動作する1つの分散協調エージェントとして開発された[11,12]。ここでの「意味表示」は、プラント状況に対応するための本質的な情報を表示するという意味である。他の分散協調エージェントとの関係を図6に示す。運転員支援のための情報生成の点では、異常原因推定、対応操作候補の導出、および、各対応操作候補の操作量や効果の推定を行う。これらの生成された運転員支援情報は、従来のHMIと同様のP&ID図とマルチレベルフローモデリング（MFM[13]）による対象プラントの機能モデル図を用いて表示するとともに、内容を自然言語表現で表示する。支援情報の自然言語表現への変換は、分散協調エージェントのオントロジーサーバ[11]で行われる。

運転員支援情報の表示例を図7に示す。

まず、異常状態の検知が分散協調エージェントのインタフェースエージェント[11]により通知されると、異常状態が検知されたコンポーネントに対応するP&ID図上のシンボルと、その対応する機能の機能モデル図上でのシンボルの色を黄色に変化させて、異常状態検知場所やプラントのどの機能が異常状態となったかを通知する。機能モデル図での表示に関しては、各MFM機能流れ構造は詳細表示モードと簡略表示モードの2つの表示モードを有し、正常状態

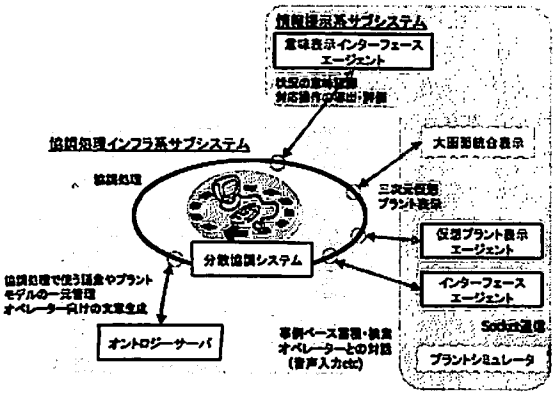

図6 次世代プラント用ヒューマンインタフェースのプロトタイプの構成

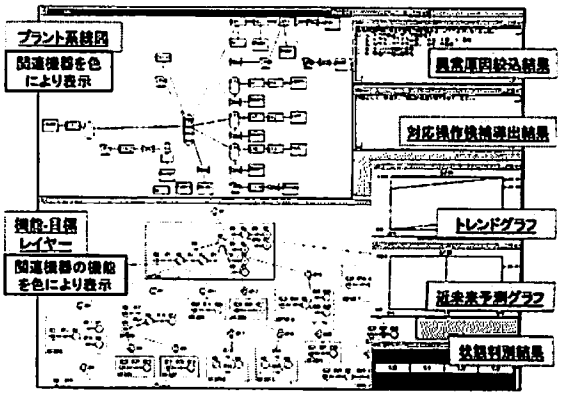

図7 意味表示インタフェースの画面例

においては、正常状態時のプラント監視や運転において重要なプラント機能の流れ構造は詳細表示モードにて表示され、重要でないものは簡略表示モードで表示される。異常検知通知時や異常原因が推定できた場合には、関連するMFM機能流れ構造は自動的に詳細表示モードで表示される[14]。これにより、プラント状態に応じて、運転員が注目すべき範囲をナビゲーションしている。熟練運転員は事故時のプラント状態認識をアラームの点灯パターンによっても行っていることから、運転員が慣れ親しんだP&ID図上で図的に異常検知場所等を表示することは、迅速な状況認識を支援する上で有効であると考えられる。また、機能モデル図も適切な教育により、パターン認識的な扱いが可能となると思われる。P&ID図や機能モデル図をパターン認識的に運転員が捉える場合には、これらの表示は直接的な支援と考えられるが、どのようなコンポーネントが異常の影響を受けるかや、どんなプラント機能が劣化しているかと解釈する場合には、間接的な支援を提供していると言える。

異常の原因が推定されると、異常原因に関連するコンポーネントとその機能は、それぞれ、P&ID上と機能モデル図上において、対応するシンボルの色を橙色に変化させることで表示される。必要がある場合には、MFM機能流れ構造は自動的に詳細表示モードとなる。また、推定された異常原因情報は、オントロジーサーバにて自然言語表現に変換され、右上のウィンドウに表示される。この自然言語表現は、図的に表示された異常原因推定結果の説明となって運転員の状況認識を補完するとともに、インタフェースエージェントから音声ガイダンスとして運転員への支援情報伝達に用いられる。

異常原因推定後、異常の影響を緩和するための対応操作候補が機能モデルを基礎として導出され、数値シミュレーションの併用により操作量や操作の効果が推定される。これらの結果は自然言語表現に変換され、右側上方の2つのウィンドウにそれぞれ表示される。なお、対応操作候補はインタフェースエージェントを介して音声ガイダンスされる。また、対応操作候補の表示では、EOP内の構文の[行動]的な表現となっており、直接法的な表示となっている。ただし、その内容は、EOPでは操作目標にあたるレベルであり、個々の操作機器に対する操作方法を表示するまでには至っていない。しかしながら、操作目標に対する具体的操作を対応させることは比較的容易であり、短期的な操作手順を表示するように拡張することは十分可能であると考えられる。

4.3 状態パターン化とオーバレイによるインタフェース

この節では、上記の2つの節とは異なり、機能のいう抽象的な概念を使わず、より具体的なプラントのパラメーターから「意味」をグラフィック化してHMI上に情報提示しようという試みである。

従来のHMIと同様に、P&ID図を基礎的な表示要素とする。これは前節4.1に述べた運転員の表示情報への親和性によるものである。典型的な原子力発電所の主要機器、例えば、蒸気発生器、一次冷却材ポンプ、タービン、再過熱器とそれらをつなぐ配管が常時表示画面となる。この上にプロセスパラメータの通常値からの偏差から生成されるパターンを重畳表示する。系統図にプロセスパターンを同時に表示する設計方法は既に提案されている[15]が、偏差に着目する方が得策である。原子力発電所では、通常、100%負荷で運転されているので、通常値からの偏差を得ることは容易である。本稿で提案する間接支援HMIの例では、圧力、温度、流量のパターンを切り替え表示できて、通常安定状態（即ち偏差の生じていない場合）では、それぞれ正方形を描くような変換を計算機内で行う。又、実際にプロセスが時間と主に変化することを運転員に認識させるために輝度変調をかけている[16]。

この状態パターンを重畳することで、故障した機器や系統図で不具合の発生している大まかな位置を把握することも可能である[17]。これら、P&IDと状態パターンは常時表示されており、通常運転中の異常診断も可能となっている。

さて、一旦事故が起こると、このパターンは大きく歪み、複雑な多角形を形成すると思われる。これだけで運転員はどのようなことが起こったのかを、低負荷の解釈で行うことは困難である。これを低負荷で行うためには、予め想定された事故をコード等でシミュレートして得られる予想状態パターン図を事故時に重畳させて、よく似たパターンを探すことにより、事故の原因同定を支援すればよい。このアイデアは医療分野において、患者の脳波や心電図中の異常をチェックするためにテンプレートを当てて診断を行うことにヒントを得ている。この一種のテンプレートによる「診断層（Diagnosis layer）」とも呼んで差し支えないこの