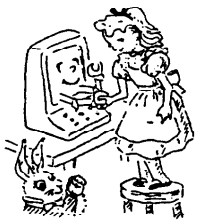
解　説

各種システムにおける人間的側面



原子力発電所における人間工学上の課題†

近　藤　駿　介††

1. 序

原子力発電所は，構成部品数が1千万点以上で，設計に数百万人時間，建設に5年以上，その定期検査，保守作業に数千人の人が必要とされる典型的大規模システムであり，一方その運転管理には100～150人程度の人があたるが特に中央制御室には5～6人が常駐しているのみの自動化の進んだシステムである．このシステムの設計・建設・運転・保守の各作業には，安全確保の観点からさまざまな人間工学上の配慮が加えられその問題解決のために計算機が利用されてきている．たとえば，設計作業では，設計ミスを減少させる観点から設計図書の作製と管理にプラモデルと電子計算機が大規模に採用され，最近ではその総合化も行われつつある．また建設時の品質保証活動の一環として，各個の部品の来歴の管理システムが採用されつつある．さらに，保守作業における個人の被曝管理が全国的な組織で行われており，一方，被曝量をできるだけ小さくするという観点から，作業の事前訓練の徹底とロボットの採用が積極的に推進されている．しかし本解説では，紙数も限られているので，これらには触れず，中央制御室における人間工学上の課題と計算機の役割に絞って現状を述べる．

2. 原子力発電所の安全確保と人間工学

原子力発電所は大量の放射性物質を内蔵しているので，いかなる事態でもこれが環境へ放出されないようにすることが安全確保の目標であり，これを高いレベルで達成するために多重防護の思想を採用している．具体的には，まず発電に必要な機器を使用中に故障しないよう，また外乱に対して安定であるよう，保守的な技術でゆとりを大きく設計すること，第2に，そのような配慮にもかかわらず故障・異常は発生すると考え，そのときでも原子炉を安全に維持できるよう必要な設備を設けること，第3にそのような安全設備についてわれわれの知識が不十分で期待する役割を果し得ないことがあると考え，そのときでも公衆の安全を確保できるよう安全設備を付加・強化するという三層の防護構造を採用している．このような設計面の配慮が有効であることは，過去の主要な原子炉事故において，一般工業の事故とは異なり，1人の公衆の被害も発生していないことから明らかである．

しかしながら，「事故が起きても安全」というのは，公衆の信頼確保の必要条件であっても十分条件ではなく，制御室において積極的に初期異常のうちに措置する考え方や方法論の研究も求められていた．1979年3月に発生した米国のスリーマイル島(TMI)発電所事故は，公衆の直接的被害はなくても発電所所有者の財産損害は莫大となること，さらに規制当局を含めた関係者の原子炉状態についての判断の乱れが大きな社会的インパクトを引起すこと，そして何より運転員がするべきことをしない (omission error) のみならず，するべきでないことをする (commission error) ことにより上の多重防護が破られる可能性のあることを示した．この事故についての調査報告[1]が，特に制御室における人間工学的配慮が不十分であることがこれらの問題の主な発生原因であることを指摘した結果，電子計算機の多様な利用による運転員と原子炉のインタフェースの改良努力を含む制御室の人間工学研究が急速に要求され，その成果の一部はすでに採用されている．これらの狙いは運転員の行動を予測可能なものにすることによって多重防護設計の有効性を強化するものであるが，同時に上に述べた公衆の信頼を確保する十分条件を確立しようとする努力の1つでもある．

3. 中央制御室における人間工学

原子力発電所においては，プラントの多岐にわたる

† Human Engineering in Nuclear Power Plant Control System Design by Shunsuke KONDO (Department of Nuclear Engineering, University of Tokyo).

†† 東京大学工学部

情報を一括管理する中央集中管理方式が採用されており，中央制御室には中央制御盤がおかれ，5～6人の運転直員により，運転監視の業務が行われている．したがってこの中央制御盤は，原子炉プラントと人間のインタフェースの中心的存在である．

ところで，人間-機械（プロセスプラント）系のインタフェースの設計には，プラントにおける人間の役割を定めることが必要である．原子炉と運転員の場合，Kisner[2]の説を引用すれば，「プラントに必要な情報，人間の能力と限界，機械の能力と限界，プラントシステムの安全上の要求，ならびにその他の制御的制約から決定される人間のもつユニークな能力によるプラントとの関係」であり，具体的には，**図-1** に示されるように，

（1） 運転員の頭の中にあるプラントモデルに基づくプラント応答の解読ととるべき行動の決定

（2） 計器盤とか作業環境とか運転員が五感で感知できるものによる判断と行動

（3） 制度的なもの，たとえば手順書，管理者の方針，および規制当局の方針などに基づく行動

（4） 他の運転員や保守その他の担当者との交渉や働きかけ

という広がりをもち，

（Ⅰ） 文書・建物・人員などを管理する業務

（Ⅱ） システムの監視，最適化，異常の予測の業務

（Ⅲ） 自動系の限界を超えたプラント状態において手動で介入する業務

（Ⅳ） 連絡調整の業務

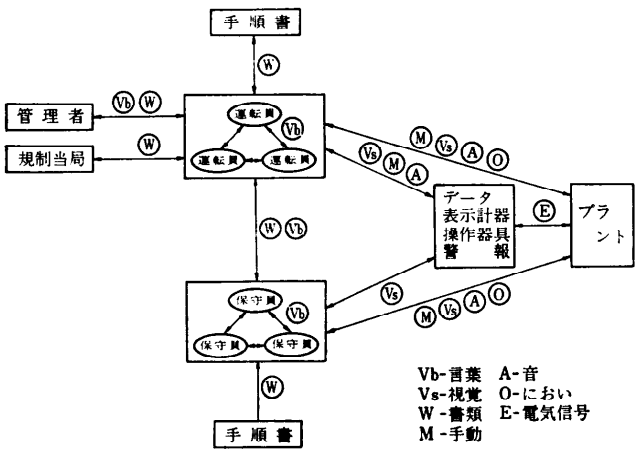


図-1 原子力発電所における運転員の付置付けとインタフェース
(Kisner の論文（2）により引用)

の4つのレベルの異なる機能を有する．

一方，Goodstein と Rasmussen は，運転員の行動を，

（1） 訓練による熟練に基づくもの

（2） 手順書などルールに基づくもの

（3） 訓練も手順書も有効でないとき発現する知識に基づくもの

に分類し，そのうち Kisner の(Ⅲ)の機能に対応する(3)の知識に基づく行動においては，単に制御室の情報のみならず過去に蓄積した多くの情報を柔軟に動員し，創造的かつ適確な判断を行うことが期待されているとしている[3]．

ところが，運転員の心理的ストレスが急に高くなったり，退屈の極みにあるときには，そうした柔軟性が失われ，判断が硬直化し，かつ注意の範囲が狭くなることが知られており[3]，**これに対応することが中央制御室の設計における人間工学上最大の課題といってよい．**

この困難を回避する第1の対策は，より多くの行動を熟練やルールに基づくものとすること，さらには訓練によって知識ベースの行動における柔軟性もある程度体得できるとする考え方に基づき，運転員の訓練内容を向上することとされ，訓練内容に広範な事故事例を取り入れる努力が進められており，さらに世界各国の故障・異常の事例を各発電所で常時検討することも求められている．特に最近は原子力発電所の運転が安定化しつつあり，2～3年間に一度も故障・トラブルを経験しない運転員もでてきているので高ストレス下の行動の経験は減少しており，運転員のシミュレータによる再教育の機会にこのような訓練をより体系的に行うことが特に重要である．この場合の訓練内容，訓練方法についての研究開発は，その成果が目に見える形の利益をもたらさないこともあって担い手が少ないが，ますます充実させる必要がある．

第2の対策は，この知識ベースの行動が創造的に行われる条件の整備・充実である．その内容は，いわゆる中央制御盤の設計の人間工学的観点からの再検討と，**4** で述べる電子計算機の積極的利用による運転員支援システムの開発から構成される．

中央制御盤は，プラントの情報がほとんどすべて表示されており，これを監視する

ことによりプラントの運転状況が把握される．またこれを操作するための各種スイッチもそれぞれの監視装置に対応して配置されている．最近では，プラントの単機容量の増大，安全機能の確保のためのシステムの拡充により制御システムの規模が大きく，複雑になってきており，これに対応して，人間工学的観点も含めて改良が行われ，あるいは計画されている．その要点は以下のとおりである[5]．

（1） 室の照明，雑音，広さなどを含めて作業環境を改善する．

（2） プラント運転の監視性・操作性の向上をはかるために，中央制御盤の表示，操作内容をその重要性，緊急性，および頻度の観点から検討し，常時監視すべき範囲を主盤に，その他を副あるいは補助盤へと分割する．通常は，プラントの通常起動・停止，出力運転の監視操作および緊急時の監視を行う部分を主盤に，工学的安全施設，原子炉補助系，およびタービン補助系の細部の監視を行う部分を補助盤においている．

（3） プラント運転の信頼性，安全性の向上の観点から制御盤に取付ける計器，操作スイッチ，警報表示器をその機能別にまとめ，系統の流れに沿って配置し（簡易グラフィック表示），重要なものは大型とするなど，全体に機能・重要性に応じて識別が容易なようにラベル付け，形，色を変え，それらを手順書の記載と一致させる．

現在の課題は，警報の表示法である．上に述べたように，色・形・配置などのコーディングを徹底して行うことにより，識別の容易さは向上しつつあるが，その数は世界のどこかで問題が発生するたびに増加する方向にあり，その結果，現在では冷却材配管の大破断という安全評価のために想定されている事故が発生すると最初の2分間に約240の警報がなるという．これではせっかくの警報がかえって運転員を混乱に導くおそれがないとはいえない．そこでこれを減らす方法論の開発が進められており，これは4で述べる運転員支援システムの主要開発テーマでもあるが，この点に目的を絞った研究開発としては，ハードワイヤの警報信号群を電算機に入力して，「1つのプロセス（安全動作）に1つの警報」を原則に処理した結果を表示するHALO システム（Handling of alarms with logic）がある[4]．これは OECD ハルデンプロジェクトの中で開発が進められているものであるが，これによれば上記の240が約30に減少するとされている．

4. 電子計算機利用の強化方向

中央制御室における電子計算機利用の基本的考え方には，従来の中央制御盤の担っているプラント運転の監視のためのインタフェースという機能を代替する方向と，さらに進んで計算機のもつ動特性シミュレーション能力と情報処理能力を利用して，人間の行う知識ベースの行動のもとになる判断作業を代替していく方向とがある．さらに自動化により制御室そのものを代替していくという考え方もあり得るが，原子力発電所については，当面のというよりは，長期的課題とされている．

4.1 プラント監視性能の向上

これは，従来の制御盤が，いわばすべての情報を同時に提出して，その選択を運転員にまかせていたのに対して，電算機-CRT 表示というインタフェースを用いて CRT 画面の限られた情報伝達能力を逆に生かしつつ，プラント情報を集約的にかつ包括的に，しかも運転員の要求に対して柔軟に提供して運転員の監視労働を支援しようとするものである．これを実現するためには，運転員に有益な情報とその階層構造を知る必要があるが，現在のところ，たとえば主要系統の状態の総括表示など全体プロセスの包括的把握を助ける情報を最上位に，例えば各系統の機器の制御に必要な状態量，パラメータの値などプロセス制御に必要な情報の表示を次位に，そして，それぞれの機器についてのすべてのデータを最下位に配置しているのが普通である．

この考え方はプラントが緊急停止（トリップ）したときの監視系の設計にも適用されていて，プラント全体系統の運転状態表示を最上位に，主要パラメータの値およびそのトリップ前後の経過のトレンド表示，各機器の運転パラメータなどが得られるようになっている．これらの表示画面の構成にあたっては，人間工学的観点からシンボル，色，大きさ，表示方式，更新周期などを設計するのは当然である．

最近発表された新型中央制御盤では，この考え方に立った CRT 表示を大幅に取り入れつつあり，主盤だけでも7～8台の CRT を有するものが多い．これらは，故障時を考慮して隣接の2台で相互にバックアップ可能な形にするなど信頼性の確保にも配慮が加えられている[6]．

この監視機能のうち，特に事故時の監視機能の向上については，TMI 事故後規制当局も注目するところ

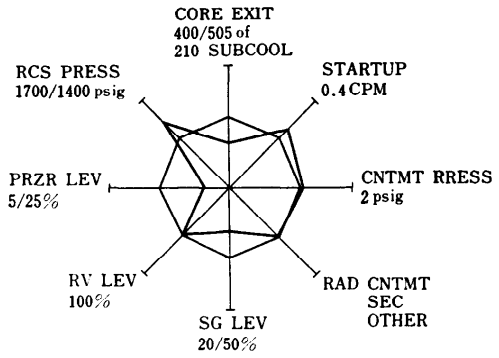


図-2 Westinghouse 社で開発した Safety Sarameter Display System の CRT 表示の1例[9]

となり，特に事故時安全上重要なパラメータについてはこれを集中的に監視できるシステムの設置を計算機利用の推進とともに求めている．このシステムは米国では SPDS (Safety parameter display system) と呼ばれており，運転員がプラントの安全状態を迅速かつ正確に判断できる最小限のパラメータとして**図-2** のように，ⅰ）炉心反応度，ⅱ）一次系冷却材量と圧力，ⅲ）炉心熱除去の状況，ⅳ）二次系熱除去の状況，ⅴ）格納系の温度圧力ならびに隔離状況が選ばれ，それらの全体状況と，関係状態量の時間変化あるいは関連機器の状態の表示などが得られるようになっているのが普通である．これらの機能は，前述した新型制御盤には当然含まれている．

4.2 知的作業の支援

原子力発電所では，異常・故障により原子炉変量が通常運転許容限界を超えるおそれのあるときは緊急停止装置が作動するので，運転員は少なくとも最初の10分間くらいは所定の安全機器が作動していることを確認するだけでよく，その後復旧動作に入るとされている．この観点からは上の SPDS が設置されることにより，重要な対策は終ったといえる．しかしながら，現実には運転員は，原子炉緊急停止時の多数の警報から停止原因を察知して安全動作が適切であると判断し，あるいは，手動介入が必要であると判断する．さらにその後に引続く復旧動作についていくつかの選択肢の1つを選びその準備を開始したり，緊急停止に至る以前に異常・故障を発見し，適切な措置を講じることもその主要任務の1つである．とすれば，このような，いわばプラント中で進行中の事態についての「診断」と，ある措置のもたらす影響の評価という「運転員の頭の中でのプラントモデルとの対話」を支援することは有意義であると判断される．

そこで現在開発が進められているのは，前述の SPDS の発展形態として事故時に運転員を積極的に支援するのみならず，通常運転時の異常診断も行い，プラントの安全性と稼動率を向上させるシステムである．これは，米国では DASS (Disturbance Analysis and Surveillance System)，日本では，運転員支援システムと呼ばれている．このシステムの概念は極端なケースは自動運転システムにも至り得るので，多様であり，定まったものがあるわけではないが，「プラントーエンジニアリングー運転員ー訓練・手順の4要素を結ぶ触媒」というのが一般的な見解であり，原子炉ならびに運転員操作の異常・故障・事故の発生を未然に防止し，発生した場合には早期に検出し，拡大しないうちに終息させることが目標とされて，**図-3** のような構成がそのあるべき姿の1つとして考えられている[7]．その機能としては，プラント全体の状況についての総括業務，プラント状態について置かれている状況，ルールに照しての妥当性の監視業務，異常・故障の検出と診断業務，故障・異常等の終息のガイド業

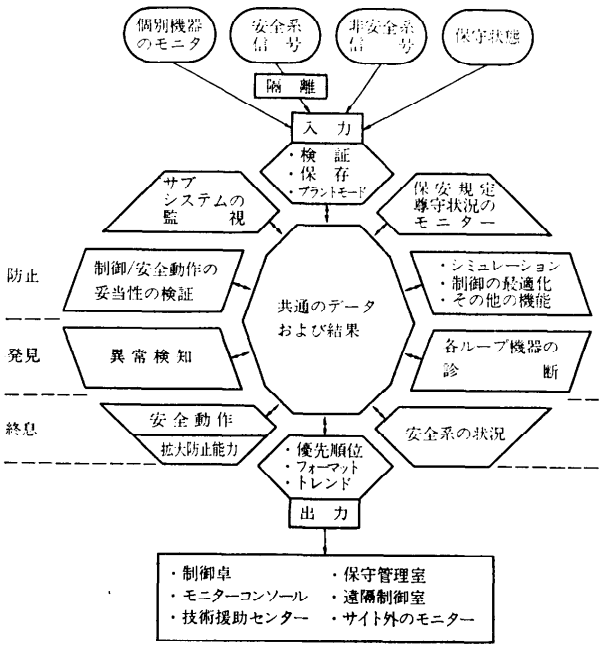


図-3 DASS の構成の一例[7]

務，事態の今後の展開，操作の効果等の予測業務，などが含まれる．これらの業務能力の設計には，いわゆる知識工学の応用など新しい工学の展開が求められる面も少なくない．わが国では，原子力発電支援システム開発組合が発足し，その開発が進められている．

5. あとがき

以上，原子力発電所の人間-機械系のインタフェースをめぐる最近の動きを述べた．これらの目指す方向は，いわば点状から面状のインタフェースへの発展であるが，一方，安全確保のためには，これまでのようにたとえ点状のインタフェースでも運転できるよう訓練を重ねることが多重防護の観点から求められていること，人のエラーという観点に絞っては近年文献8)，9)の解説があることを付記して終りとしたい．

参考文献

1) Kemmeny, Chairman, J. G.: Report of the President's Commission on the Accident at Three Mile Island.
2) Kisner, R. S. and Flanagan, G. F.: A Systems Approach to Defining Operator Roles, IEEE Trans. **NS-28**, 1, p. 972 (1981).
3) Goodstein, L. P. and Rasmussen, J.: Man-Machine System Design criteria in Computerized Control Rooms, ASSOPO 80, IFIP/IFAC Symposium, Trondheim, Norway (1980).
4) Sargent, T. O.: A Study of Human Behavior in Adverse Stress, Trans. Am. Nucl. Soc. Vol. 38, p. 244 (1981).
5) Hanes, L. F. et al.: Control Room Design: Lessons from TMI, IEE Spectrum, June, p. 46 (1982).
6) 富沢他：原子力プラントの運転状態監視システム，電気学会雑誌，Vol. 102, No. 9, p. 726 (1982).
7) Long, A.: Private Communication (1980).
8) 橋本邦衛：マン・マシン系における人間の特性と過誤，計測と制御，Vol. 19, No. 9, p. 836 (1980).
9) 武田充司：人間-機械系としてみた原子力発電とヒューマン・エラー，人間工学，Vol. 17, No. 4, p. 157 (1981).

(昭和58年1月12日受付)