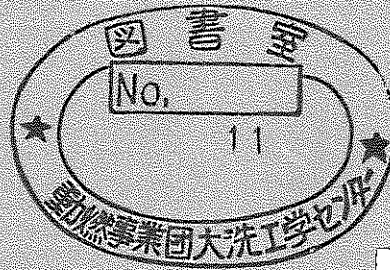


区分変更	
変更前番号	二
変更年月日	平成13年7月31日

# 原子炉設計基準と運転員の行動基準

— より安全な運転を目指して —



1978年4月

<b>技術資料コード</b>	
開示区分	レポートNo.
	N951 78-04
<p>この資料は 図書室保存資料です                  閲覧には技術資料閲覧票が必要です</p> <p>動力炉・核燃料開発事業団大洗工学センター技術管理室</p>	

動力炉・核燃料開発事業団  
 高速実験炉部

本資料の全部または一部を複写・複製・転載する場合は、下記にお問い合わせください。

〒319-1184 茨城県那珂郡東海村大字村松4番地49  
核燃料サイクル開発機構  
技術展開部 技術協力課

Inquiries about copyright and reproduction should be addressed to:  
Technical Cooperation Section,  
Technology Management Division,  
Japan Nuclear Cycle Development Institute  
4-49 Muramatsu, Tokai-mura, Naka-gun, Ibaraki, 319-1184  
Japan

© 核燃料サイクル開発機構 (Japan Nuclear Cycle Development Institute)

## まえがき

本資料は、米国規格協会 (ANSI) および米国原子力学会 (ANS) が作成中の “Criteria for Safety-related Operator Actions” を翻訳したものである。

従来から原子炉施設の安全解析においては、運転員による手動操作には期待しないのが建前になっているが、本基準は原子炉施設内に常駐し、施設に最も精通している運転員の操作について改めて注目し、各プラントについて安全上の操作を時間試験を通じて分類し、それぞれの区分に応じて運転員の操作に期待しようとするものである。逆の見方からすれば、設計者は本基準を満足する場合は、運転員の操作を設計上期待してもよいとしている。

今後は本基準の思想を十分に理解し、「常陽」プラントの事故のケースについて検討を加えていく必要がある。

翻訳にあたって design base event を「設計基準イベント」としたのは、「設計基準事故」と訳すと design base accident (DBA) と間違ふこと、また required operator action を「必要とされる運転員の操作」としたのは、required が各プラントによって異なると考えられ、プラント安全上から必要とされるという意味を持つものと判断したことによる。

訳 者

## 目 次

序 文	1
1. はじめに	7
2. 定 義	10
3. 運転員操作に関する一般的要求事項	13
4. 運転員の操作および運転員の環境保護の為の操作場所	14
5. “必要とされる運転員操作”に対する時間制限	15
6. 適用指針	19
7. 情報の有効性	21
8. 計装および制御の信頼性	22
9. 安全解析および緊急処置	23
10. 適用除外と施行	24
付録A 管理職者用の概要	25
# B 実例および説明資料	29
# C 運転員の選択的または計画外の操作指針	34

## 序 文

目的及び適用の背景

添付の基準は、原子炉施設の設計基準イベント (Design Basis events) の結果を緩和する安全系について、それらが

(a) 運転員の操作を利用したもの、あるいは

(b) 自動保護システム

によって開始されるのか、または調節されるのかを決定するための機能上の要求事項を確立するためのものである。計測系、制御系、指示計等に対する運転員の操作に必須な機能の指針についても確立されている。Executive summary (管理職の為の概要) は、付録 A に示されている。

現在、原子炉安全に係わる運転員の行動規範については、一般的に認められたものがない。現在使用されている「指針」なるものは、基準のベースにするには、不明確すぎる。N660の基準が、この空間を満たすべく意図され、将来の設計の基礎となるべく用意されている。ANS-51委員会は、明細な、かつ合理的に保守的な基準が必要であると信じている。その基準は設計に対する同等の基盤を備える優先度の高い基準を有し、設計上の仮定についてのケースバイケースの解決を減らすことによって、もって許認可のプロセスの安定化に役立てんとするものである。

大型原子力発電プラントの通常運転において、運転員はプラントの安全に係わる多くの決定および操作を行っている。設計基準事故の経過においても、プラントの安全と環境の保全を確実にするために、設計基準イベントに対する自動安全保護システムの応答性を増す上に運転員の細心な、そして時として記憶に基づく合理的な方針決定の能力は価値のあるものである。加うるに、人間という運転員は、人間が作った装置では対応できないような予期せざる場合においても、対応することができるのである。

運転員の操作は、3つの基本的なタイプからなると考えられる。(1) “必要とされる操作”，(2) “選択的な操作”そして、(3) “計画外の操作”で“運転員の必要とされる操作”は、プラントの設計の基盤の一部であり、安全システムの作動または調整に用いられる。“選択的な運転員の操作”は、事故に引きつゞく結果の改善に有用である。しかしながら、この場合の結果は、そのような操作がなくても、許容できるものでなければならない。“計画外の運転員の操作”は、事故後の状態の修正や予想せざる事故の対応におい

て有益であろう。これらの基準は、プラント設計上の主要点として必須であると認識され、これらの選択的及び計画外の運転員の操作を促進させているのである。しかしながら現状では付録Cに示す如く、未だ指針が示されているのみである。

添付の基準の中の規則には、システムおよびプラント設計および安全評価を行うための適切な安全余裕を与える安全側の時間余裕、時間遅れ及びその他の制限条件が含まれている。それらは、実際の運転員の操作時間、手順もしくは訓練の基本として役立つよう意図されたものではない。実際に行うにあたっては、運転員は設計基準イベントに正しく対応し、短時間のうちに必要な操作を採ることが可能であるべきである。

これらの基準の適用については、ある種の保護手段で現在運転員によって実施されているものを自動化する結果に導くかもしれない。これらの基準に対する例外は、その適用が保護手段の自動化を必要とする場合にのみ勧告される。それら保護手段としては、(a)人間の行える範囲を逸脱しているか、(b)非常に複雑で、(1)計画外の事故が起った場合のプラントの安全性または、(2)プラントの信頼性を危くする場合のいずれかである。

#### ANS-51委員会による発展

これらの基準の初期のドラフトは、産業界でしばしば受け入れられている「1.0分間の原則」という非常に簡単なものを進展させてベースとしていた。NRC（原子炉規制委員会）の代表を含むANS-51委員会の委員には、このアプローチの仕方には、個々のケースに対する時間余裕が不適切であると強く感じていた者がいた。NRCとIEEEのSC-6（Steering Committee）の会合の後、運転員の行動の為のワーキンググループは、もっと包括的な、またある場合には、より保守的安全側の要求事項を基準に盛り込むことを決定した。

これらの基準においては、よく知られた運転員誤操作率の経験や、現在の運転員の訓練の慣習と時間上の要求に関して何ら直接の関係を示していない。ワーキンググループは、原子力発電プラントという環境に今日適用しうる運転員の信頼性に基づくデータは十分整っていないことを認識している。EPRI（Electric Power Research Institute）（米国電中研）および他の機関によって緒につき、または計画されている研究計画が長期に渡って時間上の要求に関する科学的ベースを提供するであろう。当分の間は、ワーキンググループは、これらの基準の時間上の要求に対して、以下に掲げる事項の判断と合理的考察に基づいて対応していくのが妥当と考える。それらは、(1)事故の見込み、(2)たまの事故に伴なり高い応力レベル、(3)より起りそうもない事故については分析に多

くの時間を要すること，(4)必要な操作の複雑さ，および，(5)必要な操作をとらなかつた場合の結果である。原子炉の安全性研究における限定されたデータであるがWASH-1400<sup>注)</sup>は，上記の考えとより長い時間上の要求をこの基準に求めていることを支持している。(注) WASH-1400：ラスムッセン報告)

ANS-51委員会のメンバーの大多数は，これらの基準における時間上の要求について展開があることに同意している。数人の評価委員は，これらの基準を流体システム設計，電気，計装および制御設計，シュミレータ訓練，安全解析，許認可およびプラント運転管理に携わる人々による評価を得るべくアレンジした。時間上の要求は数例の事故についてシュミレータにより評価され，格納容器外での配管破断の解析に適用された。

これらの基準のドラフト№10は，1975年5月付ANS-51委員会で投票の結果13対2で承認された。ドラフト№12は，投票の際のコメントに基づき変更を示唆されたものを大部分反映したものである。1975年10月の会合で，ANS-51委員会は9対2で，この基準のドラフト№12を試用ならびにコメントのベースとするべく発行するよう勧告した。

投票で反対もしくはコメント付反対をするについて，ANS-51委員会の2人のメンバーが提案された基準に対して大きな疑念を表明した。特に彼等は，時間上の要求は任意であり，非観的であり，かつ非現実的であり，基準に合致させることは考えているよりずっと困難でコストがかかり，現在予想されるよりもっと多くの分野に適用されるべきで，手動操作の為の訓練や，人間の技術およびその必要な確率は，失敗の重大さと同等と考えるべきであり，そしてついに，運転員の操作に対する新しい要求の基準の設定は，原子炉設計手段として運転員の信頼性に関する確率評価の発展に先ずるのではなく，従属すべきであると信じていた。

3人目のANS-51のメンバーは，時間上の要求の時間試験1および2から状態Ⅱの事故は除くべきであると勧告した。彼はコメント付の肯定的投票を行い，状態Ⅱの事故の緩和は，基準の与える衝撃を考慮して決定すべきであるという条件を付した。

ANS-51委員会のコンセンサスは，これらの反論点については，基準の発展の過程で考えられており，現在用いられているケースバイケースのアプローチに代るものとして明確で，コンシステントな，かつ合理的に安全側の設計上の指針を持つとする必要性に比べれば，反対は価値がないか，あっても重みが低いという点に到達した。

### ANS-50委員会による検討

これらの基準は、次いでANS-50委員会によって全てのタイプの原子炉に適用すべきか検討された。この検討は論議を巻き起こし、そのうちのあるものは、ANS-51によるN660の発展において出たコメントと同類である。ANS-50は、1976年10月の会合でN660を試用しコメント用に発行するよう決定した。これらの基準の主体は、ANS-51によって了承された基準と実質的に同等であった。ANS-50によるコメントは序文で考慮されている。

### 基準の試用並びにコメント期間の間およびその後の実施項目

次に示す資格、検討計画、およびR&D計画が、ANS-50およびANS-51による検討において高揚された関心事に取りかゝるべく用意された。

#### 1. 資 格

時間試験1, 2および3におけるタイミングの要求は、試用およびコメントの期間において暫定と考えるべきであること。それらはまた運転員の信頼性についてのデータの基礎が利用できるようになるに従って長い期間に渡って改訂されるべき問題であると考えべきである。

#### 2. 検討計画

2.1 検討を行う者および利用者は次の事項を実施しなければならない。

- (a) 将来のプラントの設計にこの基準を適用すること。
- (b) 安全解析書(SAR)の第15章の設計基準イベントについて、この基準に合致するために必要な設計上の動作および追加の自動化があればそれについて、シュミレータで解析すること。
- (c) 事故を緩和する事を意図して追加した自動化装置について、その装置による妨害の可能性について評価すること。
- (d) 追加した自動化装置について、誤動作の可能性と、その影響について評価すること。

2.2 検討者および利用者はワーキンググループに対して、次の事項について回答を用意しておくよう要請されている。

- (a) 特定の基準が受け入れ難いか実行不可能な要求を負わせ、それらが不可能、非実際のまたは高度に望ましからざる設備の設計を必要とすると認められた場合(コメントを提出のこと)。この場合、コメントには基準に対する特定の改訂案を



付して提出のこと。

(b) 特定の基準に対して同等に受け入れ可能な代案を認めた場合

(c) 上記の 2.2(a)および(b)の項目については，提案された改訂案に対する価値／影響に関する理由書を付すこと\*。

### 3. R & D 計画

#### 3.1 EPRI の計画，即ち「トレーニングシュミレータを用いた行動測定システム」

(RP769-1)は，方法開発に集中しており設計基準イベントの結果を緩和するために，自動保護システムによるよりも，運転員の操作に期待する方が妥当であると判断する基盤の一部（例，機能配当）として使用しうる運転員の信頼性についての十分なるデータを収集する計画に発展させんとするものである。この計画は更に発展させて次の項目を含むべきである。(1)数台の異なる訓練用シュミレータ，(2)十分なるデータのベースを開発するに十分なデータ，および(3)SARの第15章で審査された設計基準イベントの全てについてである。

勧告された作業団体はEPRIである。

3.2 運転中の原子力プラントからの運転員の信頼性に関するデータを収集したり，他の産業や軍事関係で現存するデータを採用する計画を発展させること。このことは同時に上記 3.1 で述べた機能配当のための訓練シュミレータのデータとしても使用することができる。この作業は，EEIの原子力プラント信頼性データシステム(ANSIの小委員会N18-20による)計画と同様のもので，コンポーネントの故障率を収集し，IEEEの故障率基準マニュアル(IEEE-FARADAM)計画が行っている原子力以外の産業界からコンポーネントの故障データの採用と同様のものである。

勧告された作業団体はANSIの小委員会N18-20:EPRIである。

3.3 これら基準における安全システム設計および安全評価の目的で運転員の信頼性に

---

\* これらの基準における要求事項について，完全なる価値／影響に関する評価をすることは実行不可能である。ANS-50は価値／影響の評価の必要性はANSの政策決定として，個々の提案された基準に要求するよりも，提案された基準全体に対して要求すべきであると決定した。

関するデータ（上記 3.1 項及び 3.2 項）と時間上の要求の間に適切なる安全余裕を決定する方法を開発すること。

勧告された作業団体は，ANS-5 1.4 のワーキンググループ；NRCである。

3.4 運転員の訓練と規制を改善する方法の開発

勧告された作業団体は，その利用者；NRCである。

3.5 運転員の有効性を増大させる制御室の設計の改善に関する継続した開発

勧告された作業団体は，利用者，A-E's，およびメーカである。

本委員会のメンバー氏名一覧 略

## 1. はじめに

### 1.1 目的

原子力プラントの通常運転において、運転員はプラントの安全に関する多くの決定を行い、多くの操作を行う。異常なイベントの過程で、プラントと周辺環境の安全を確保するために運転員の操作が遂行されるのは、有益、賢明かつしばしば必要なことでもある。ここで述べるクライテリアは設計基準イベントの結果を軽減するのにいかなる場合に運転員の操作に信頼を置くことが許されるかということについてガイダンスを提供しようとするものである。

### 1.2 適用範囲

設計基準イベントに続く運転員の操作は、“必要とされる”(required)“選択的”(optional), または“計画外”(unplanned)のいずれかである。

“必要とされる運転員の操作”(required operator action)とはプラント設計基準の一部であって安全系\*機器に最低許容限度の運転を行わせるためにそれらを起動または調整するような操作を含むものである。

“選択的な運転員の操作”(optional operator action)とは、プラント設計基準上要求されはしないが、安全系の能力を高めるのに有益かもしれない。しかし、(事故の)結果はその様な操作がとられなくとも許容可能でなければならない。

“計画外の運転員の操作”(unplanned operator action)とは予想されない事態の結果を軽減するのに有益であるかもしれない様な操作である。

ここで述べるクライテリアは、設計条件\*\*が侵されるのを回避するために手動操作が行なわれるプラントのためのSARの15章で検討した設計基準イベント(すなわち、特定事故)において遂行される“必要とされる運転員の操作”に限定される。さらに、これらにおいては次の事項が設定される。

- (1) 安全系を起動または調整するための特定の保護動作が運転員の操作によって完了されてもよいかあるいは自動保護システムによって完了されねばならないかを決定するための条件。

---

\* ANSI NI 8.2 の 2.2 章で定義する。

\*\* ANSI NI 8.2 の 2.1 章で定義する。

(2) “必要とされる運転員の操作”を補助するために必要な計装，制御機器，指示計，表示器，等々のための機能上のガイドライン

上記の，“必要とされる運転員の操作”の使用の許容可能性の決定を目的として，全ての安全系機器は原因イベントの結果を軽減するために正しく機能するものと仮定する。安全系機器の単一故障あるいは運転員の単一エラー（単一操作）の影響の解析は別のクライテリア\*において扱う。単一故障クライテリアは単一操作における運転員のエラーについて述べたものであり，これに対してここに記すクライテリアは“必要とされる運転員の操作”を首尾よく成し遂げるための設計および解析において採るべきクレジットを与えるための判断について述べるものである。

ここで述べるクライテリアは安全系機器の単一故障のあと必要とされるかもしれないどんな運転員の操作にも適用されない。

ここで述べるクライテリア（3.5章および6.8章(d)を除く）は“選択的な運転員の操作”および“計画外の運転員の操作”を対象としない。しかし，ガイドラインは付録Cに示した。

管理職者のためのサマリを付録Aに，そしてクライテリアの背後の論理的根拠および特定の章をわかりやすくするための例を付録Bに示す。

### 1.3 基礎および仮定

ここで述べるクライテリアは，安全系の保護動作を開始させ，及び／あるいは制御するための運転員の操作に対して設計および安全解析においてクレジットを探る際の最少条件を規定するものである。これらのクライテリアは，操作がここで規定するクライテリアを満足しなくても自動“保護系”\*\*が運転員の設計基準イベントにおいて安全システムの保護動作を開始するように設計されているという概念に基礎を置いている。

引き続き述べるクライテリアにおいて設定するルールは，安全システム設計および設計基準イベントの安全解析の目的に対して十分な安全余裕を与えるために保守的な所要時間およびその他の限定条件を用いている。それらは実際の運転員の操作時間，操作手順，またはトレーニングのための基礎として役に立つことを意図したものでは

---

\* 単一故障クライテリア：ANSI N658およびIEEE-379

\*\* IEEE-279-1971で定義する。

ない。つまりクライテリアにおいて与えられた時間の長さは最低限必要なものと考えられるべきであり、もっと長い時間を与えてもかまわない。

このスタンダードのクライテリアは次の仮定に基礎を置いている。

- (1) 運転員に警報を発し、ガイドするために安全系の一部として十分な計測表示装置が中央制御室に据え付けられている。
- (2) 運転員はよく訓練されており、プラント設計とプラントの動きを理解している。
- (3) 非常時操作手順が文書化されており、定期的な教育訓練で使用されている。
- (4) プラントの運転員資格から、運転がどのような“必要とされる運転員の操作”でも遂行しうる事が保証される（これによってもしある運転員が“必要とされる運転員の操作”を遂行できない場合には実力のあるバックアップ運転員が代行することが要求される。）

## 2. 定 義

### 2.1 設計基準イベント

設計条件が侵されるのを回避するために保護機能が必要であると決定されたそれぞれのイベントは設計基準イベントとして定義される。設計基準イベントは安全系の備えるべき条件を決定するのに用いられる。

### 2.2 安全解析\*

それぞれの設計基準イベントに対してプラントの全ての応答をシミュレートし、設計変数の値がそれらの個々の設計条件の制限を越えないことを確認する解析を安全解析という。安全解析はそれぞれの設計基準イベントの過程の各段階ごとの場面における個々の行動あるいはイベントの発生時刻を明きらかにする。

### 2.3 保護機能

設計基準イベントの安全上重要な結果を制限するのに必要な機能（たとえば、炉出力をすみやかに下げること、炉心からの熱除去、予備ポンプへの切換）をいう。保護機能には自動保護システムまたは“必要とされる運転員の操作”を含めてもよい。

### 2.4 保護操作

安全系にその保護機能を遂行させるために要求される始動操作、保護操作はそれを完遂するためのいくつかの独立した一連の操作を含めてもよい。

### 2.5 “必要とされる運転員の操作”

特定のイベントカテゴリーに対して設計条件が侵されることを回避する最低許容動作を安全系が遂行できるように設計基準イベントの過程において機器の手動操作を必要とする操作。

### 2.5 “選択的な運転員の操作”

設計基準イベントに引き続いて要求されるものではないが、安全系の動作が許容出来る最低のレベルに達しないようにするために運転員によって遂行される可能性のある操作。

### 2.6 “計画外の運転員の操作”

安全系の最低許容限度の機能が遂行されず、その結果イベントが設計条件を越える

---

\* ANSI 1.8.2 の 4 章を参照せよ。

かもしれないと云う予測されないイベントに対して、正常化するための手段として必要あるいは有益かもしれない運転員の操作。

## 2.8 経過時間上の主要点

設計基準イベントにおいて用いられるところの経過時間の主要点のいくつかはFig.1で定義する。その他については以下で定義する。

### 2.8.1 “運転員操作アラーム点” ( $t_a$ )

“必要とされる運転員の操作”の必要性が、たとえばインジケータの様を読み取り情報あるいは音響警報によって確認される時点

### 2.8.2 “運転員操作開始点” ( $t_i$ )

ここで述べるクライテリアの時間試験を満足させるために“必要とされる運転員の操作”を開始しなければならない時点

### 2.8.3 “保護操作完了時点” ( $t_c$ )

設計条件が侵されるのを回避するために、ある特定の保護操作が完遂されなければならない限界時点

### 2.8.4 “時間余裕” ( $t_i - t_e$ )

設計基準イベントを知らせる警報からの経過時間であって、運転員の初期の緊張がやわらぎ、行動計画をたてるためにここで述べるクライテリアにおいて与えられる時間

2.8.5 “運転員操作時間遅れ” ( $t_c - t_i$ )

運転員が保護動作を遂行するためにここで述べるクライテリアにおいて与えられる時間

2.8.6 “設備及び装置の時間遅れ” ( $t_j - t_c$ )

(運転員の)保護操作が完了した時から(安全系の)保護機能動作が完了した時までの時間

2.8.7 “異常警報発生点” ( $t_e$ )

イベントが1以上のビット数のたとえばインジケータの様な読み取り情報や音響警報によって確認される時点

2.8.8 “保護機能動作完了時点” ( $t_j$ )

設計条件が侵されるのを回避するためにある特定の保護機能動作が完了しなければならない時点。この時点においては設計条件に近づくことはあっても越えてはならない。

2.9 設計条件\*

それぞれのイベント・カテゴリーについて、あらゆるイベントの結果が次の(1)、(2)に示す状態になることがないことを十分に保証する様な設計パラメータの制限値。

- (1) 公衆の健康および安全に対する過度の放射線リスク
- (2) ブラント機器の許容できない機能低下

結果はイベント・カテゴリーと関連して発生回数によって異なる。

---

\* イベント・カテゴリーおよび設計条件は、PWRについてはANSI N182の2.1章で、BWRについてはN212/ANS-52.1で、そしてGORについてはN213/ANS-5.3.1で定義する。これらはANS-50のCWG-2の作業に基づいて改訂される可能性がある。



### 3. 運転員操作に関する一般的要求事項

- 3.1 設計基準イベントに対応する安全系は、もし、5章に示す時間試験1の時間内で許容されるよりも早く保護動作がとられなければならないのであれば、自動保護系によって開始されなければならない。
- 3.2 設計基準イベントに対応する安全系は、もし、この資料の要求事項の全てが満足され、特に5章の時間試験の要求事項に合致する場合“必要とされる運転員の操作”によって開始されてもよいであろう。
- 3.3 もし、この資料の要求事項の全てが満足されるならば、オートマティックな、もしくは運転員による安全系の動作開始後において、設計基準イベントのシーケンス上必要とされる連続する保護操作の開始を“必要とされる運転員の操作”によって行ってもよいであろう。
- 3.4 “必要とされる運転員の操作”もしくは操作のシーケンスは、運転員がエラーを確認するのに有益な時間と情報があり、かつ設備および装置の設計上、修正動作が許容される場合にのみ用いられるであろう。
- 3.5 “必要とされる運転員の操作”もしくは操作シーケンスの数は、運転員がプラント状態を把握するのに十分な時間を有し、かつ“選択的な運転員の操作”を行うのに十分な時間を有する程度に少くすべきである。
- 3.6 実施できる場合は、頻繁の、もしくは連続の監視や調整を要する保護操作は自動化すべきである。
- 3.7 “必要とされる運転員の操作”の内、いかなるポイントにおいてもタイミングよくと規定される操作の数は、使用しうる運転員の人数で行いうる数に制限されるべきである。

#### 4. 運転員の操作および運転員の環境保護の為の操作場所

- 4.1 設計基準イベントに引きつづく30分以内に必要とされる全ての運転員の操作は、制御室から行いうるようすべきである。
- 4.2 設計基準イベントに続く30分経過の後に必要とされる運転員の操作は、4.3および4.4の制限を守ることを条件に制御室もしくは制御室外の場所のいずれから行ってもよいであろう。
- 4.3 制御室外の操作場所（およびそこへの接近ルート）において“必要とされる運転員の操作”を行う場合は、設計基準イベントによって生じた環境条件の下で接近するのに必要な時間、運転員を保護するようになっていること。
- 4.4 中央制御室の内外で設計基準イベント時に作業に従事する運転員の集積線量は、NRO GDC-19の制限値を超えてはならない。
- 4.5 設計目標としては
  - (1) 制御室外の場所から行う運転員の操作の数を少なくすること、および
  - (2) 必要とされる運転員の操作を行う制御室外の場所を少なくすること、である。

## 5. “必要とされる運転員操作”に対する時間制限

- 5.1 “必要とされる運転員の操作”が考慮されている安全系の開始もしくは調整に要する保護動作は、以下に規定する3つの時間試験に基づいて評価すべきである。もしこれら3つの時間試験の全てと、この基準の他の要求が満足されるならば、設計者は原子炉の保護動作を行うところのよく訓練された運転員の活用を考慮に入れてもよいであろう。記号や時間々隔についてはFig. 1に定義されている。保護動作の例と時間試験の適用については、6章に説明され、Fig.2に図示されている。
- 5.2 事故の挙動は、まず第1に事故のカテゴリに対する様々な設計上の要求を越えてしまふのを避けるために、保護機能が完了するまでの時間上の最初のポイント( $t_i$ )を決定する際考慮されている運転員の操作開始という保護的操作および機能を期待しないで確認すべきである。

### 5.3 時間試験1

第1のテストは、その間に全ての保護動作が自動保護系によって開始される安全側の時間々隔を規定するものである。最小時間余裕、即ち( $t_i - t_e$ )は、その事故が下記の表に示される状態Ⅱ、ⅢあるいはⅣのいずれに類するかによって規定される。ある事故に対する時間余裕は、(1)その事故のシビアさが増す程、(2)その頻度が少ないもの程、および、(3)運転員のその事故に対する慣れが少ないもの程長くとられる。この事は、運転員が、(1)運転員の初期のショックから回復するのに、(2)起った事象の分析を行うのに、および(3)自らの行動を考えるのに、より長い時間を許容することとなる。この時間余裕はまた運転員に対して、(1)適切なる自動保護動作が起っているかを確認、(2)自動保護動作をバックアップする手動操作を開始する、および(3)自動保護機能の正規の達成をモニタする、ことを許容するものとなる。

#### 時間試験1

最小時間余裕( $t_i - t_e$ )は、設計基準イベントの警報発生から、保護機能の開始のための運転員の操作が考えられるまでの経過時間

#### 事故の区分

状態	Ⅱ	イベント	10分
〃	Ⅲ	〃	20分
〃	Ⅳ	〃	30分

これら時間余裕には、10%の許容範囲を適用する。

Fig.1 タイムポイント(時点)および時間間隔の定義  
 DEFINITION OF TIME POINTS AND INTERVALS

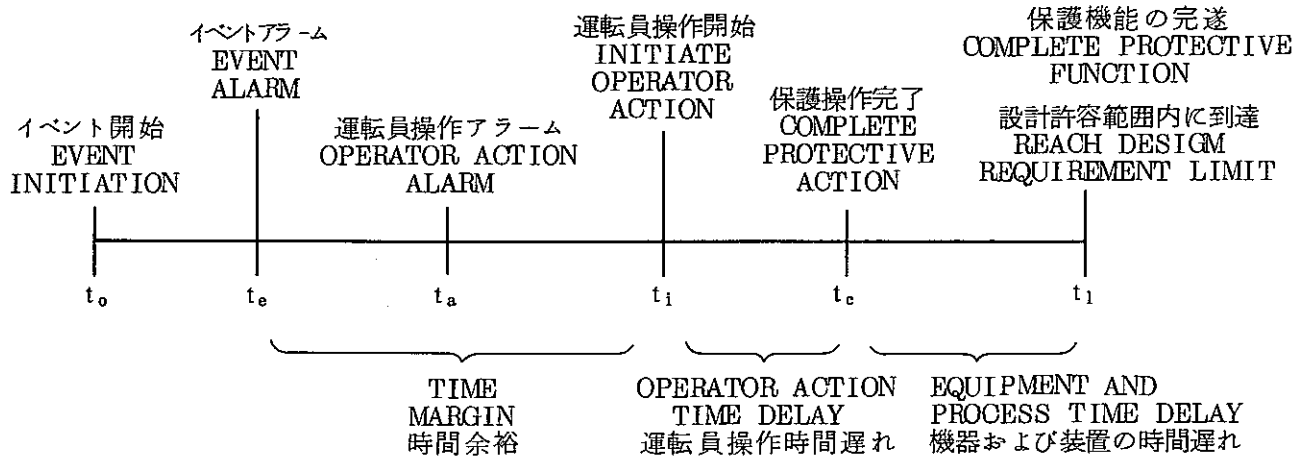
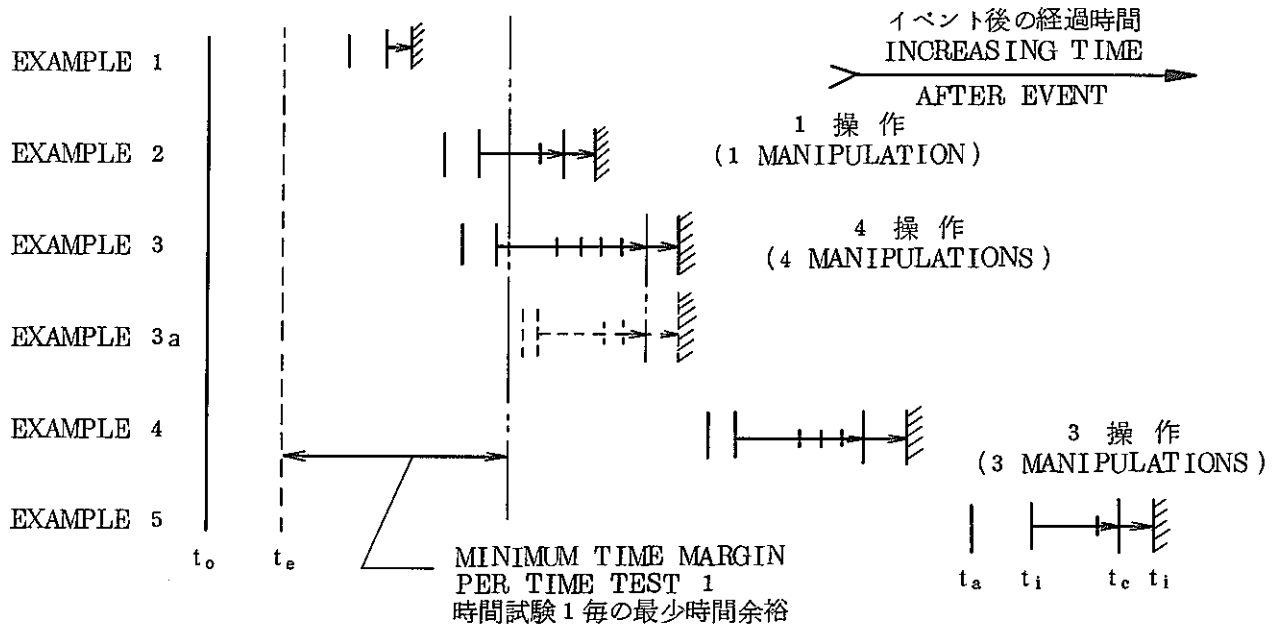


Fig.2 イベント解析における時間々隔のとり方(例)  
 EXAMPLE TIME INTERVALS INVOLVED IN AN EVENT ANALYSIS



結 論

1. EXAMPLE 1 および 2 の保護動作はオートメ化すること。
2. EXAMPLE 4 および 5 の保護動作は、もし運転員の操作の必要性を評価する情報が利用でき ( $t_a < t_i$ )、かつそれらが時間試験 3 の要求に合致するなら運転員操作によってなされてもよい。
3. EXAMPLE 3 の保護動作は、部分的または全体的にオートメ化すべきである。(EXAMPLE 3 a の 2 操作の場合の変更された時間遅れを参照のこと。)

## 5.4 時間試験 2

第2のテストは、運転員による操作開始を考慮した状態での保護動作の各々に対して適用される。時間試験2は、運転員各人の操作に対して許容される、より安全側の時間遅れを表わす。運転員の操作の最小時間遅れ ( $t_c - t_i$ ) は、次の表に示す通りである。

時間試験 2

保護動作を完了させる運転員操作最小時間遅れ ( $t_c - t_i$ )			
事故の区分			
状態	II	イベント	$1 + n$ *分
	III	“ ”	$2 + n$ *分
	IV	“ ”	$3 + n$ *分

\* “n”は独立した操作時間を意味する（例、ポンプの起動、弁の開放）

これら時間余裕には、10%の許容範囲を適用する。

時間遅れの固定部分として、次の2つを含めることを許容する。即ち、(1)非常に単純な読み取り情報の受信（指示、可聴アラーム等）で、操作の必要性を最初に示すもの、及び、(2)操作の必要性を分析し、操作の方法を考える付加的な時間。時間遅れの固定部分は、時間試験1の時間余裕の後直ちに時間試験2が開始されるという特殊なケースに対しては取り除くことができるであろう。

もし、“必要とされる運転員の操作”が中央制御室の外で行われる場合は、固定された時間遅れには、運転員が必要な準備をして現場に到着するのに十分な時間を適度に延長することが許容される。

運転員の操作の時間遅れにおける可変の部分には、保護動作を完了するのに必要なそれぞれの独立した操作に対して最少限1分間の余裕を含めることを許容する。各々の操作には、運転員の操作の実施及び操作によって制御された動作が開始されたことを確認する（状態表示灯またはメーターの読みによる）行為を含むと考えられる。

操作時間は必要に応じて3.4および5.6に掲げる要求事項に合致すべく調整すべきである。

前記テーブルにおける“n”の使用については、連続した独立の操作におけるある中間点での意志決定のプロセスの発生のケースに対しては許容しない。もし、そのような意志決定が、数個（5～6）の操作の間に必要な場合は（評価のタイプとして）、中

間の意志決定のポイントは、2つの独立した保護操作の分岐点として処理し、新たに時間試験2を適用しなければならない。

運転員の操作を喚起するアラーム ( $t_a$ ) は、“必要とされる運転員の操作”が開始される時点 ( $t_i$ ) より前に出されなければならない。

### 5.5 時間試験3

時間試験1および2の基準に合致した保護動作の各々に対して、ある特殊な運転員の操作を開始した時の運転員の誤操作を仮定して、運転員操作アラーム ( $t_a$ ) に続く少く共1時間以内に最終的なチェックを行うことをイベントの過程に含めるべきである。これに先立つ操作及びこれに引き続く、“必要とされる運転員の操作”は正しく行われたと仮定する。実際の解析仮定が、安全側の安全解析の仮定に代って使用されるべきである。

時間試験3の要求は、保護動作を開始した際の1時間に及ぶ運転員の誤操作が下記の結果を、もたらしてはならないということである。

- (1) 環境へのF.P.の大放出をもたらす有効な1次バリア（燃料被覆管，原子炉冷却材圧力バウンダリ，および原子炉格納構造\*）の全ての大破損，又は
- (2) 安全系の冗長性をもったセットの全てに回復不可能な損傷を与えて，その結果，以下に示す機能が引続いで実施できない場合，即ち
  - (a) 省略されていた保護動作を行うこと，又は
  - (b) 引続く必要とされる保護動作を実施すること。

5.6 設計基準イベントの過程における適切な時点より以前に，“必要とされる運転員の操作”の実施がなされ，受け入れがたい安全上の問題を惹起する可能性がある場合は，早すぎる運転員の操作を回避するIEEE-279-1971の要求に合致したインターロックを備えるべきである。

5.7 保護動作の実施に自動保護系が使用される場合は，運転員による状態リセットは適切な監督管理の下に，自動開始後の制御な運転員が取り戻せる場合のみ行うべきであろう。

5.8 独立した“必要とされる運転員の操作”の間には，設計基準イベントの各々の全過程における全ての操作の複合した結果が，本資料の要求事項に合致するように，十分な時間々隔を確立すべきである。

---

\* ANS I N18.2の第3章を参照のこと。

## 6. 適用指針

6.1 設計段階の解析は 3.0～5.0 の基準を適用して処理すべきである。

6.2 “必要とされる運転員の操作”が利用されるよう計画されているプラントでは、SAR (Safety Analysis Report) の 15 章中で吟味された設計基準イベントの各々について解析されるべきである。第一に、発端となる出来事(事故)は固有の設計基準イベントの範疇(状態Ⅱ,Ⅲ又はⅣの事故)に入れ、次に設計要求事項の相当するレベルが決められる。

6.3 5章の時間試験1は指定された運転員のために事故発生から安定したプラント状態に達するまでに必要とされる定められた保護操作をなすべきである(例えば、ホットシャットダウン、コールドシャットダウン)。この時点でプラントは他の設計基準イベントが適応する点で安定する。

6.4 時間試験1の適用

時間試験1の時間余裕間隔の間に設計上の要求を越えるのを防止するために最初に実施しなければならないあらゆる保護動作は自動保護システムによってなされなければならない。(参照 Fig.2 の例1)

6.5 時間試験2の適用

運転員操作時間遅れ( $t_c - t_i$ )に設備及び装置の時間遅れ( $t_i - t_c$ )を加えた時間は、設計基準イベントの挙動調査から決まるように保護動作が完全に作動することが可能な最短時間( $t_s$ )から控除される。これは“必要とされる運転員の操作”がなされなければならない時間( $t_i$ )を確立する。

もし、運転員の操作、設備及び装置の時間遅れの合計が“必要とされる運転員の操作”がなされなければならない時間( $t_i$ )に時間試験1の時間余裕内であるようにさせるならば、運転員が最初に実施する保護動作は受容できない(参照 Fig.2 の例2および3)。分離された操作のいくつか又はすべては運転員操作時間遅れを減少させるために結合させ、又は自動操作化しなければならない(参照 Fig.2 の例3a)、あるいは安全システム機器は設備及び装置の時間遅れを減少させるよう修正させるべきである。

もし、運転員操作、設備及び装置の時間遅れの合計が“必要とされる運転員の操作”がなされなければならない時間( $t_i$ )に時間試験1の時間余裕を越えて起こさせるな

らば(参照 Fig.1の例4), 時間試験2の必要条件は, 運転員動作警報( $t_a$ )が“必要とされる運転員の操作”がなされなければならない時間( $t_i$ )の前に準備することができる場合に満たされることになる(参照 Fig.1の例4及び5)。

#### 6.6 時間試験3の適用

もし, 時間試験3の必要条件を満足することができないならば, そのときは次のいずれかである。

- (1) 全保護動作は自動操作化されるべきである。あるいは,
- (2) 全保護動作は十二分に時間試験3の失敗を避けるため自動操作化されるべきである。あるいは,
- (3) 時間試験3が満足されるようなより早い運転員操作警報が準備されるべきである。

もし, 時間試験1~3の必要条件が満たされるなら, 3つの時間試験は満足されるものである。

6.7 解析はまた全体としてすべての保護機能を考慮すべきである。このことは, 3.7及び5.8の要求に違反しないこととなるだろう。

6.8 このとき, 解析は次のことを十分に評価すべきである。

- (1) 5.4, 7.8を満足するための動作をなしている間, 運転員の指針となる有用な情報。
- (2) 4及び5.4を満足するための動作をなしている間, 操作すべき装置の位置。
- (3) 事故時3.4を満足させるために行った間違った操作を正しい操作にやりなおすために運転員に必要な時間。
- (4) 3.5を満足するよう任意のあるいは計画されていない運転員の操作をするために運転員にとって有効な時間。

6.9 もし, 解析が上述必要条件と, 3~5の他の必要条件が申し分なく満たされることを証明するなら, このときは訓練された運転員はこれらの保護動作をたやすく行うだろう。



## 7. 情報の有効性

- 7.1 運転員に対しては必要な時に何らの重要な判断を行わなくても特殊な保護操作の必要性を評価できるように、明瞭に表示された読み取り情報が準備されるべきである。
- 7.2 設計基準イベントの ( $t_e$ での) 発生を示す情報伝達手段はアナンシェイタのような表示器と可聴の警報とを含むべきである。設計基準イベントの発生を確認するためには、1つ以上の異った手段が必要であろう。
- 7.3 運転員操作警報後30分以内に開始しなければならない(即ち、 $(t_i - t_a) < 30$ 分)  
“必要とされる運転員の操作”について、それが必要な事を示す時点  $t_a$  における情報伝達手段はアナンシェイタのような表示器と可聴の警報を含むべきである。
- 7.4 運転員操作警報後30分かそれ以上まで開始する必要のない(即ち、 $(t_i - t_a) > 30$ 分)  
“必要とされる運転員の操作”にとっての必要事項を示す読み取り情報は表示器と可聴の警報かあるいは緊急処置によって補足された表示器のいずれかを含むべきである。  
この処置は必要な運転員操作が開始しなければならない時間の評価を含むべきである。
- 7.5 運転員の手動操作によって制御された各動作が正確に実施されていることを示す読み取り情報が準備されるべきである。

## 8. 計装および制御の信頼性

- 8.1 計装，制御器，指示計，アナンシエーター，等の“必要とされる運転員の操作”の指針となるべき基本的なものは，クラス1Eであるべきであり，また安全系の一部（即ち，安全に関連した表示や制御計装）として設計されるべきである。設計者は適用しうるIEEE-279-1971の部分を確認し，そして充足すべきである。
- 8.2 最低限3系統の読み取り情報が，1系列以上の安全システム装置に対して影響を及ぼすために，“必要とされる運転員の操作”が必要であることを示すために準備されるべきである\*\*。この要求はもし運転員が表示された情報の不一致に対面した時，常に安全操作をとることができるならば，あるいはもし異なった関連状態量が適切に厳選された指示として同様の情報を与えるのに有効であるならば，2系統に減らすことができる。
- 8.3 少なくとも2系列の安全システム装置が用意されている場合には，1系列当り最低限1系統の読み取り情報が，1系列の安全システム装置のみに影響を与えるところの“必要とされる運転員の操作”が必要なことを指示するために用意されるべきである。
- 8.4 上記機能を有する計装及び制御系は設計基準イベントの間にあるいは後に生じる環境（周囲の事情）の中で運転するためにIEEE-323, 1974の要求に合致した的確なものでなければならない。

---

\* 次章は，IEEE原子力エンジニアリング委員会（NPEC）の小委員会6によって開発されたIEEE P497やIEEE P603のような適当なIEEE基準が開発されるまでの暫定指針として準備されている。

\*\* 3チャンネルは，2チャンネルが矛盾した指示を与え，そして明らかに運転員に有益となる安全方向動作がなく，あるいは動作が不足しているときに判断するための基準を提供するために必要とされる。

## 9. 安全解析および緊急処置

- 9.1 時間遅れ，時間余裕，“必要とされる運転員の操作”およびそれらに関連した計装，制御系，そして位置（もし中央制御室の外ならば）は各設計基準イベントの安全解析で実証されるべきである。
- 9.2 “選択的”あるいは“計画外”の運転員操作については設計基準イベントの安全解析上はクレジットはとれない。
- 9.3 “必要とされる運転員の操作”は，正式なプラント緊急処置に含むべきである\*。  
分離された手動操作（時間試験2から）は処置と同一のものとみなすべきである。
- 9.4 運転員は緊急処置を使用した訓練の一部として適当な時に“必要とされる運転員の操作”を行うような訓練されるべきである。

---

\* ANS I N18.7-1972の第5.3.8を参照のこと。

## 10. 適用除外と施行

現在、安全に関係した運転員操作の一般的に受け入れられる基準はない。このように、これらの基準は現在のプラント設計には適用されていないし、また経済的な可能性も証明されていない。しかしながら、この領域における指針の必要性は存在する。これらの基準は将来のプラントの設計目標として役立てるように意図したもので、現在進行中のものや、設計中建設中のもの、あるいは稼働中のプラントに遡って適用させるものではない。従ってこれらの基準は“試用並びにコメント用”の基準として出すつもりである。

もし、基準の適用が、(1)技術の状態 (the state of the art) を超えあるいは、(2)過度の複雑さを含む自動化へとつながって行くなら、ケースバイケースの考え方をベースに基準の例外を設けてもよい。

## 付 録 A

## 管理職者用の概要

大型の原子力発電所の通常運転において、運転員は多くの決定を行いプラントの安全に関連する多くの操作を行っている。設計基準イベントの際にも、運転員の記憶や思考および意志決定の能力を利用してオートマチックな安全系の設計基準イベントに対する応答性をよくし、その結果としてプラントの安全性並びに環境の保全を確かなものとすることは賢明であるばかりか、しばしば必要なことである。加えるに人間である運転員は、人工の装置では対処できないような予測不可能な事態にも対応できる。

今日安全性に関連する運転員の操作について一般に承認されている基準は存在しない。今日用いられている指針の類は、基準のベースにするには不明確である。N660の基準は、この不明確さをなくし、将来の設計の基礎となるべく企画された。この基準は、設計基準イベントの結果を緩和するのにいかなる時に運転員による操作に依存してもよいかという指針を与えるために意図された。

これらの基準においては、よく知られた運転員の誤操作率の例や現在の運転員の訓練とこゝで云う時間上の要求とは何ら直接の関連はない。そのような基準を作成する上で使用に耐える原子力発電プラント環境における運転員の信頼性に関するデータは不十分である。EPRI（米国電中研）や他の機関により計画され、実施されつゝある研究計画により、より实际的な時間上の要求に対する科学的根拠が提供されるであろう。当分の間は、これらの基準の時間上の要求は、種々の設計基準イベントや、これより頻度の少ない事故に伴う高い応力レベルや、運転員操作の手ぬかりの結果や、並びに運転員操作の複雑さ等の確かさについて合理的に考えることを示唆する。原子炉安全研究WASH-1400（ラスムッセン報告）における限られたデータに基づいても、上記の考え方や安全サイドの時間上の要求をこれらの基準で用いる事が妥当であることを示している。

設計基準イベントに引き続く運転員の操作は“必要とされる”，または“選択的の”あるいは“計画外の”のいずれかである。“必要とされる運転員の操作”には、プラント設計基準の部分であり、かつ許容しうる最少限の動作を行う安全系設備を始動させたり調整する操作を含める。“選択的な運転員の操作”これはプラント設計基準からは要求されないが、安全系の動作を改善するのに有効であろう。しかし何ら事故の結果はこのような操作がなくても許容しうるものでなければならない。“計画外の運転員の操作”

は予見できない事態の結果を緩和するのに有益となる操作を云う。

“必要とされる運転員の操作”の利用を受入決定する為には、安全系の設備は全て開始したイベントの結果を緩和するように正しく機能することが前提となる。安全系における単一故障の影響または運転員による単一誤操作の影響に関する解析は、他の基準でカバーされる。単一故障基準は一操作における運転員の誤操作を強調するのに対して、ここで述べる基準は、“必要とされる運転員の操作”に関してその操作の数に関係なしにそれらがうまく完遂された場合に対して設計及び安全解析においてクレジットをとることに決定することを強調したものである。これらの基準は安全系設備の単一故障を考慮した場合に必要なであろう運転員操作のいずれに対しても適用するものではない。

N660の基準は公衆の安全に必須である“必要とされる”運転員操作に対してのみ適用されるものである。従ってこれにはシステム及びプラント設計と安全解析に対して適正な安全余裕を与える為の安全側のルールと制限が含まれる。実際の場合には、運転員はもっと短時間に正しく対応できるであろう。

この基準は運転員の操作開始を考えた場合、それぞれの保護操作に対して3つの時間試験の採用を要求するものである。もしこれらのテスト（及び他の適度の条件）が満たされるならば、設計者は保護動作を行うについてオートマティックな保護系よりむしろ運転員に期待することができるであろう。

まず第1にRegulatory Guide 1.90に基づくSAR（安全解析書）の15章で解析を要求されている設計基準イベントの各々を適当なイベント分類に分ける。即ちANSI N18.2等に基づく状態Ⅱ、Ⅲ又はⅣのいずれかに分ける。そしてそれに対応した設計のレベルの要求を決定する。然る後に手動操作の候補として考慮している保護操作がないとした場合の事故の挙動を調べてみる。最初の時間試験1が適用される。するとこれによってすべての保護操作が自動保護システムによって開始されるべき安全側の時間余裕が明確になる。最少時間余裕は、その事故が状態Ⅱ、Ⅲ又はⅣのイベントのいずれによるかによって決定される。あるイベントに対する時間余裕は、(1)その事故の重大性が増す程、(2)その頻度が少ない程、そして(3)その事故に対する運転員のなじみが少ない程、長くとられる。このことは運転員に対してより長い時間を許容し、その結果(1)運転員が最初の衝撃から回復し、(2)起ったイベントを診断し、(3)操作を考えることを許容する。この時間余裕はまた運転員に、(1)適切な自動保護動作がとられたかを確認し、(2)自動保護動作に対するバックアップの手動操作を開始し、(3)自動保護機能が正しく行

われたことを監視するのを可能にする。

もし保護操作が時間試験1をパスするか、時間試験1の時間々隔以後まで必要でなかった場合は、時間試験2および時間試験3が適用される。

時間試験2は運転員によって開始される保護操作に対して許容される安全側の時間遅れを規定する。

時間遅れの固定部分には、(1)操作の必要性を最初に告げる非常に簡素な読み取り情報の受信、及び、(2)手動操作の必要性及び操作そのものを計画する診断の付加的時間を含めてよいであろう。

時間遅れの可変部分には、保護操作の完遂に必要な一連の独立した手動操作の各々に対して最少1分間をとってよいであろう。それぞれの手動操作には運転員の操作の遂行と、手動操作によって行われた動作が開始したことを確認する動作を含むと考えられる。

運転員操作時間遅れと設備及び装置の時間遅れを加えた時間は、設計基準イベントの挙動に関する試験で決定されるように保護機能が完了するまでの時間から差し引かれる。この時点が“必要とされる運転員の操作”が開始されなければならない点を確立する。もし運転員操作時間と設備及び装置の時間遅れを加えた時間が、時間試験1の時間余裕内に“必要とされる運転員操作”が開始されなければならないとの結果になったら、この場合は保護動作を開始するのに運転員の操作によることは許容されない。一連の独立した手動操作のいくつか、または全ては、運転員の操作遅れ時間を減らすために結合するか自動化すべきであろう。また安全系の設備は設備及び装置の時間遅れを最少にすべく手直しすべきである。

もしも運転員操作と設備及び装置の時間遅れとの和が、“必要とされる運転員の操作”が時間試験1の時間余裕をはるかに越えて開始されるべしという結果になったら、この場合は時間試験2の必要条件として、運転員操作喚起のアラームが“必要とされる運転員の操作”が開始されねばならない時点より早く警報されるべきことが加えられる。

時間試験1および2の基準に合致するそれぞれの保護操作に対して、イベントの経過において、運転員が行った特殊操作に誤操作があったことを仮定して少く共、運転員操作のアラームの後1時間の間はイベントをチェックしなければならない。この場合、これに先立つ、およびその後の“必要とされる運転員の操作”は正しく遂行されたものとする。

時間試験3の必要条件は、保護操作を開始するにあたって1時間におよぶ運転員の誤

操作が、次のいずれの結果を招いてはならない。すなわち

- (1) 全ての1次障壁（燃料被覆管，原子炉冷却材圧力バウンダリおよび原子炉格納施設）の大破損で，これによって核分裂物質が環境へ放出される結果を招く，または
- (2) 安全系設備の冗長設備の全てに対して回復不可能のダメージを与え，その結果次の機能を引き続いて発揮しえない場合，すなわち
  - (a) 省略していた保護操作を実施する。または
  - (b) 引き続いた必要保護操作を実施すること。

もしも時間試験3の必要条件が満足されない場合は，次の3つのいずれがでなければならぬ。

- (1) 保護操作の全てを自動化すること。または
- (2) 保護操作の全ての内十分なものについて，時間試験3の誤操作を回避すべく自動化するか，
- (3) 運転員操作開始のアラームをもっと早く出す。

もしも3つの時間試験の全てをパスしたら，厳選された保護動作を運転員が開始してもよいであろう。

この基準は，現行の慣習を越えており，現在は運転員によって行なわれている多くの保護操作を自動化する結果を招くかもしれない。従って，これは完全実施に移す前に，試用並びにコメントの期間としてこの基準の設計基準事故における可能性をテストする十分な期間をとるべく刊行された。



## 付 録 B

## 実例および説明資料

次の内容は、実例もしくは補足説明資料を述べたものである。これらは、基準本文のうちで関係する特定のセクションに対応して番号がつけられている。

- 1.2 この基準の範囲は、Regulatory Guide 1.70 をふまえた安全解析レポートの15章によって解析が規定されている事故に厳密に限られている。この制限の意向というものは、必要となる解析および可能な自動化を結びつけることにある。その意向は、又“必要とされる運転員の操作”を明確にすることにもある。Regulatory Guide 1.70 によって現在カバーされていない事故は“計画外の運転員の操作”および作動するであろう自動防護機構の1部に関係した予想外の事故と認めらるであろう。SAR 15章の範囲が拡張される場合には、N660は他の設計基準イベントに対しても厳密に適用されるであろう。

これに加えて、この基準は単一故障基準を超越している。単一故障基準においては、実行すべき運転操作における失敗又は、与えられた防護動作を完了するために必要な、一連の過程における特定な一ステップにおける動作不良について検討がなされている。この基準は完全な防護動作を実施するための運転操作における失敗について（多くの過程と無関係に）検討を行っている。

- 2.1 （安全系の操作を必要としている）可能性のある設計基準イベントは、ANSI N18.2のSection 2.1等に定義されている。特定の自然現象を組合わせた、状態Ⅱ、ⅢおよびⅣの事故を含んでいる。Section 1.2はN660に対して、SARの15章において検討されている設計基準事故の1部分だけに制限が設けられていることに注意を要する。
- 2.3 防護機能を完了させるための所要時間は、操作員の操作時間遅れと装置およびプロセス系における時間遅れの累積である。それらは、操作員が必要な手動操作の全てを実際に完了するに要する時間および、機械的、電氣的機器が設計基準事故の経過に必要とされる影響があらわれる時点まで動作するに要する時間を含んでいる。それには冷却水が熱交換を始めるまでの時間と、熱交換器がその設計熱除去能力でもって、機能するまでの時間と、そのプロセスが応答するまでの時間の一定時間がかかる。
- 2.4 防護動作の例には、制御棒の挿入開始、もしくは冷却水の流動開始が含まれる。隔

離された熱交換器に対する冷却水の流動開始もしくは、緊急用ディーゼル発電機の起動は、1つ以上の独立した段階を必要とする防護動作の例であり、その段階は防護動作が良好に完了させるために特定の順序に従って、実施されなければならない。

2.7 このカテゴリーは、プラント設計基準の1部分ではなく、又その事故の経過を前もって予想し得ないそれらの事故をカバーするために取り入れられている。運転員は、プラントパラメータの変化により安全系が応答することよりもむしろ参加して、初期のうち安全系を作動しておくことの方が必要とされるかもしれない。運転員は又、許容できない結果には至らないよう確保するためである。安全系の全て又は1部分の挙動を終結させるよう求められるかもしれない。最終的には、運転員は許容しがたい結果に至った事故の経過を阻止するために、ある安全系の操作を破棄することが求められるかもしれない。

2.8.6 機器およびプロセス系における時間遅れの1例として、弁が開き、ポンプが起動し、スピードが上昇し、緩和動作を必要としている系統に対し必要量まで流量が増加するまでの、累積時間があげられる。

3.2 1例として、化学制御系における不注意な希釈事故の結果があげられる。

3.4 通常、長期の復旧期間にわたり完了する保護動作の1例として、短時間だけポンプ入力が喪失した場合、炉心冷却の回復を可能とするLOCAに引継ぐまでの長期の炉心冷却期間は、動力源を手動操作により確保することがあげられる。

3.7 この要求の意向は、“必要とされる運転員の操作”が設計基準イベントに先立つ一時期に集中することをふせぐことにある。このようなことがおこると、数名の運転員が必要な防護動作を全て適切に完了することが不可能となるかもしれない。

4.3 運転員が、その現場において防護動作を確実にこなす場合には設計基準イベントの以前に、制御室から離れている現場に運転員が行くことも可能にちがいない。さらに又、誤操作を修正するための時間を含む防護動作を完了するために十分な間、その現場に残ることも可能にちがいない。

運転員が制御室から離れて防護動作を行なうことを認めている防護規定は、遮蔽、空調、filtering、防壁、抑制、物理的分離、耐電設計等を含んでいるかもしれないが、これらだけに制限されることはない。

5.0 このセクションは、設計者により使用されるものである。SAR 15章に対し Regulatory Guide 1.70等における状態Ⅱ、ⅢおよびⅣのいずれかの特定な

事故カテゴリーに位置しており、設計要求の相当レベルが定められている。それから、マニュアル動作の候補として考慮されている保護動作無しで事故挙動が調査されている。

設計者は、設計から要求される制限を超えないように、保護動作の完了と関連させて、機器／プロセス系の時間遅れを考慮しなければならない。次いで、設計者は特定の保護動作が完遂されねばならない時点を検討すべきである。然る後に設計者は運転員の操作開始時点を検討して各々の保護動作について3つの時間試験を適用する。これには時間試験1および2に対してFig.2と同等の解析が含まれる。もしこれらの試験と(他の適切な条件)が満足されるならば、設計者は、保護動作を行わせるのに、自動保護系よりも運転員を用いることができる。

- 5.3 時間試験1における時間々隔は、運転員がイベントによる初期のストレスから回復し、イベントのタイプを分析し、そして操作を計画することを許容する時間余裕を示している。この時間々隔は、また運転員に対して、(1)自動保護動作が行われているか、(2)自動保護動作のバックアップの手動操作を開始し、(3)保護機能が正しく行われていることをモニターすることを許容する。この時間余裕は、(1)イベントの重大さが増す程、(2)その頻度が低い程、(3)運転員のそのイベントに対する慣れが少い程長くとられる。

時間試験1は、そのイベントの結果および頻度または可能性に基づいている。もしあるイベントが危険な結果に帰する場合は、すべての保護動作が自動的に開始する迄の事故に引き続く時間々隔は長くなる。これは、シュミレータによる場合を除いて、この種の事故は、運転員によってめったに発見されなく、そして運転員の反応時間は遅く、かつ思考のプロセスも明解を欠くからである。この時間々隔の間、運転員は、大きなストレスの状態下におかれ、より誤操作を起しやすくする。

- 5.4 時間試験2の関係は、各々独立した保護動作(これらを完遂するにはいくつかの操作を含めることができる)に対して新らしい固定部分を伴う時間遅れを課する。この固定した時間遅れは、運転員が特別の保護操作に対する、必要性についての簡単な確認およびそれを計画する時間を許容する。ここでも、時間遅れの固定部分は、事故の起りうる程度が増す程、および頻度や運転員の慣れが少ない程、長くとられる。

時間試験2における固定した時間遅れは、運転員が、単一のアラームまたは単一の「メータ読み」のプロセスのような読み取り情報を基に、保護動作の必要性を判断す

る時間を許容する。時間試験 2 の可変部分は、操作の代替過程について、更に事故挙動の解析または診断を行ういかなる時間を許容するものではない。このように、これらの基準は、安全に関する表示装置が次に述べるような形態で利用できることを前提としている。すなわち

- (1) 運転員に対して、いかなる診断を行わずに保護操作の必要性を知らせ、かつ
- (2) 手動操作が正しく行われて、保護操作の対応する部分が開始したことを知らせる簡潔な情報を提供すること。

もしも読み取り情報が、運転員に対して（保護操作のどれを探るべきかの）診断を要求する場合、これは上で述べた簡単な確認よりも複雑であるので、この場合は、

- (1) 時間試験 2 における固定された時間遅れを長くするか、または(2) 各々の診断のステップ毎に時間余裕を追加しなければならない。防護動作が経過中の場合、運転員は独立した次の操作を完了する以前に読出された情報を参考にしなければならない。それから、新たな「防護動作の流れ」が新たな時間試験 2 とともに開始されなければならない。1 つの防護動作は、その動作を完成させるために多数の独立した操作又は段階を含んでいる場合もある。時間試験 2 は防護動作に対し全体的に適用され、そして時間試験 2 において可変部分の“n”には、そこに含まれている多くの独立した操作を表現するために用いられている。

時間試験 2 の関係で変化する部分は、運転員がチェックリストを使用して、それから運転員の操作によって制御される動作が開始したことを簡単な機械的読取り、たとえばリミットスイッチの点灯の如きものにより確認するための時間を許容している。それは又多くの独立した操作を含む操作に関して制限されたペナルティを位置づけている。

- 5.5 時間試験 1 および 2 の目的はひかえめな時間間隔を採用することにより運転員が必要とされている安全動作を正確に遂行する確率又は、誤動作の際特定の設計基準イベントに対する設計上必要な制限を超えないうちに復旧させるために、十分な時間を有する確率を高めることにある。時間試験 1 および 2 の比較のために、保守的な安全解析法が事故経過の解析に使用される。しかしながら、良く訓練された運転員さえも防護動作を開始させるための必要な操作を怠る可能性は少ないながら無いとは言えない。

時間試験 3 の背後にある理論的根拠は提案されている Annex D of 10 CFR 50 (36 FR 22851) において議論されていることに類似した概念に基づいている。こ

の根拠は設計基準イベントの発生の確率が低く加えて良く訓練された運転員の失敗と、一連の警報、および指示を確認し、そして1時間以内に必要とされる操作を行なうといった通常有効なバックアップの失敗を前提にしている。時間試験3は“最期の”テストでありそれは1時間以内に必要とされる運転員の操作を怠った結果がプラント状態および（又は）安全性に関係した機器をひどい破壊に至らしめないことを保証するためのもので通常の安全解析の域を超えているものである。

時間試験3において仮定された状態になる可能性は非常に少いとみなされるため、保守的な安全解析上の仮定を試験3において採用するには不適當である。それゆえ、現実的な解析上の仮定が運転員の誤操作の結果を評価するために採用されるべきである。加えて、事故によって影響を受けず又、運転員の操作怠慢の結果により故障しないような通常有効な機器が解析に採用されるべきである。同様に操作怠慢によるある程度までのプラント状態の破壊は、時間試験3における2つの要求が満足されれば許容できるものである。それは

- (1) 核分裂生成物の放出に至る3つの障壁全てにおける大規模な破壊は生じない。  
そして
- (2) 設計基準イベントに対処するのに必要な全ての冗長な安全系装置に対しては、  
とりかえしのつかないダメージは生じない。

- 5.6 この要求は、もし操作員が特定の保護動作の必要性を予期しこれを実施する場合には、運転員はその特定の保護動作の目的を破棄し、その設計を無効にすることが可能となるケースをカバーしていることを意味している。

例えば、LOCAに続いて循環の開始が早過ぎると、コンテナ内の水は不足し、ECOSポンプのNPSHが不適當となる場合があり得る。

- 5.7 この特徴は安全系を制御するための運転員の初期の能力が、(1) 3.3項に要求されている機能を果たすために長時間にわたって安全系を実現することおよび、(2)安全系の動作および、(a)不注意な起動又は、(b)予期せぬ事故の発生のどちらかによる重大な逆効果を終了させぬことを許容するよう求められている。

## 付 録 C

## 運転員の選択的または計画外の操作指針

1. 多くの原子炉安全システムは、単一の具体的な装置の故障または運転員の誤操作、(この場合引き続いて運転員による調整がない)を考慮して設計され、また設計基準イベントに対する設計上の要求(設計条件)を侵害するのを防止する最小限の作動を用意している。しかしながら、運転員の選択的操作が正しく行われるならば、安全システムの動作を改良し、許容しうる最少限にできるかもしれない。
2. その他の事故、装置の故障、システムの動作、または運転員の操作 etc で設計基準イベントとして考慮しなかった事が、事故として、あるいは事故に続いて起るかもしれない。これらの場合、計画外の運転員の操作は、修正の手段として有効であろう。
3. 事故後の修復を容易にする運転員による選択的操作が可能ないように設計上考慮されるべきである。例として遮へいや隔離弁等、安全系装置や Cross Connect の電気盤 etc の設備を含むこと。
4. 設計基準イベントのなりゆきをやわらげる安全系の効果をモニタするための計装設備が用意されなければならない。この計装設備には、クリティカルとなるプロセス量や構造材の設計限界の全範囲をカバーしなければならない。(例、格納容器の設計圧力とコンシステントな格納容器圧力および安全解析で用いられている最大の放射能レベル等)  
これは、設計基準イベント解析において、事故の過程で期待しなかった事故の結果を軽減する運転員の計画外の操作ベースとなるある種の情報を提供するものであること。IEEE の SC-6 では IEEE P497 を作成し、この種の計装に対する基準を提供している。
5. 極端な非常事態においては、選択的または計画外の運転員の操作が人命の損失やプラントの損害拡大を防止するかもしれないが、運転員の集積線量の制限を NRC の GDC-19 で前もって制定された緊急時被曝値以上に増やすのには慎重にすべきであろう。
6. 必要とする運転員の操作を行う運転員は、選択的または計画外の操作を、緊急被曝線量を越えるおそれのある高い放射能レベルのエリアで行うことは禁じなければならない。

REQUEST FOR EVALUATION  
DURING  
TRIAL USE AND COMMENT PERIOD

Users of N660 are requested to carefully evaluate N660 during its Trial Use and Comment period. Guidelines for this review and evaluation are given in section 2.1 on page F3 of the Foreword.

These criteria have proven to be of a highly controversial nature, and may have a significant impact. Thus, the Working Group needs broad industry trial use, evaluation, and feedback before the criteria can be finalized. Feedback is requested on all of the following questions. It is important that the basis for any significant deviations that are recommended be per the guidelines in section 2.2 on pages F3 and F4 of the Foreword.

- (1) Do you agree with the basic concepts and timing requirements?
  
- (2) Have you identified any unacceptable or infeasible requirements?
  
- (3) If you disagree with the basic concepts and timing requirements, or if you have identified any unacceptable or infeasible requirements, can you provide either any positive recommendations for future work, or equally acceptable alternatives to specific criteria?

Note : Please tear out and return the attached copy of this request to the chairman of the working group for Operator Actions, ANS-51.4: H.G.O' Brien, Tennessee Valley Authority, W9D182, 400 Commerce Avenue, Knoxville, Tennessee 37902

## あ と が き

本基準は、米国原子力学会（ANS）から発行された

ANSI N660

ANS-5 1.4 Published January, 1977

PROPOSED AMERICAN NATIONAL STANDARD CRITERIA FOR  
SAFETY-RELATED OPERATOR ACTIONS (Trial Use and Comment)

を翻訳したものである。

邦訳にあたっては高速実験炉部原子炉第一課の下記のメンバーが担当した。

森	将	臣
原		広
田	村	政 昭
仲	村	喬
谷	山	洋