

# 沸騰水型原子力発電所における安全設備の信頼性

## Reliability of the Safeguard System for BWR Type Nuclear Power Station

The authors introduce in this article the results of evaluation, both qualitative and quantitative, of the reliability of the ECCS (emergency core cooling system) for use with BWR (boiling water reactor), and a scheme for maintaining the reliability of the system. Also introduced are the results of probabilistic analysis on the amount of radiation hazard to the surrounding areas of the site in a hypothetical case of LOCA (loss of coolant accident).

堀内哲男\* *Tetsuo Horiuchi*  
 杉崎利彦\* *Toshihiko Sugisaki*  
 太組健児\*\* *Kenji Takumi*

### 1 緒言

沸騰水型原子炉（以下、BWRと略す）では設計、製作、建設および運転に至るあらゆる段階で事故防止のための対策を講じており、放射性物質が系外へ放出されるような事故はまず起こり得ないと考えられるが、万一の事故を仮定してそれに対処し得るための多重の工学的安全設備を設けている。

仮定される事故のうち、冷却材喪失事故（以下、LOCAと略す）では、放射性物質が炉心外へ放出される可能性があり、これを最小に抑えるために工学的安全設備として非常用炉心冷却系（以下、ECCSと略す）を設けている。

技術的に考え得る最悪条件下で原子炉の安全性を評価する場合は、事故の発生確率を1とし、それに対処するための工学的安全設備に最悪の単一故障を仮定したうえでその結果が、安全上の基準を十分下回ることを確認している。

しかるに、LOCAなど、仮定する事故の発生確率はきわめて低く、また、それらの事故に対処する工学的安全設備の作動確率は著しく高いので、技術的に考え得る最悪の条件に至る可能性は無視し得る程度に小さい。

以上のことから、原子炉で仮定される事故を確率論的に評価するための第一段階として、まずECCSの信頼度評価を行なった。さらにこの信頼度を高水準に維持するための適切な保全計画について検討を行なった。

また、事故の災害期待値を確率論的に求め、自然のバックグラウンドの期待値と比較して、事故による災害規模を検討した。

### 2 原子力発電所の安全性

原子力発電所では、厳しい安全性が要求されている。このことは、動力炉安全審査指針などでも明確に規定されている。

LOCA時、原子炉内に冷却材を注入して、積極的に炉心を冷却するECCSに対しては、設計段階ですでに十分な冗長性、信頼性を確保するよう次の事項が要求されている。

- (1) 単一動的機器の故障を仮定した場合でも、その機能が果たし得るよう多重性を有する設計であること。
- (2) 1系統で所要の性能を十分発揮できるものを少なくとも2系統有する設計であること。
- (3) 動的機器は、その共用によって他方の機能と安全性がそこなわれていないことが示されないかぎり、共用されない設計であること。

(4) 重要部分は、物理的検査が可能なよう、また系統の性能試験が定期的に行なえるような設計であること。

さらに、次の事項にも考慮が払われている。

- (1) 過酷な設計条件と、適切な基準、規格の下で系統の機器、部品を選定し、十分な品質保証を行なう。
- (2) 運転開始前の系統別機能試験で機器の作動性を確認し、初期故障、不良などを十分摘出する。
- (3) 原子炉運転中も系統別に作動確認試験を定期的を実施し、機器、部品の摩耗、故障などを適切に摘出する。

現在のBWRのECCSは、これらの要求事項を完全に満足しており、その系統構成（ネットワーク）は図1に示すようになっている。

高压炉心スプレイ系（以下、HPCSと略す）、低压炉心スプレイ系（以下、LPCSと略す）は、スプレイ冷却により炉心冷却を、低压注水系（以下、LPCIと略す）は、炉心再冠水（リフラッド）により炉心冷却を施す。自動減圧系（以下、ADSと略す）は、原子炉を強制的に減圧し、LPCSやLPCIの作動を促進する機能を有している。

ECCSは、最終的には下記のどちらかの機能が達成できればよい。

- (a) 炉心スプレイ冷却：冷却水を炉心頂上からスプレイ散布することにより炉心冷却を達成する。
- (b) 炉心リフラッド冷却：炉心内に冷却水を注入し、炉心をリフラッドすることにより冷却を達成する。

仮定する破断領域に応じ最小限、図2に示すようなECCSが作動すればこれら(a)、(b)の機能を達成でき、いかなる単一故障によっても(a)または(b)の機能がそこなわれることのない構成となっている。

図2は、LOCA発生後、ECCSの作動により炉心冷却達成されるまでの成功パスで、たとえば、設計基準事故ではHPCS、LPCS、LPCI 3ループのいずれか一つが正常に作動すればよいことを示している。

### 3 ECCSの信頼度

#### 3.1 ECCS構成機器の故障モードとその影響の定性的評価(FMEA)

まず、システムの冗長性、構成機器の信頼度要求を総括的に把握するために、ECCS各系統の構成機器の故障モード

\*日立製作所日立工場 \*\*日立製作所電力事業本部 工学博士

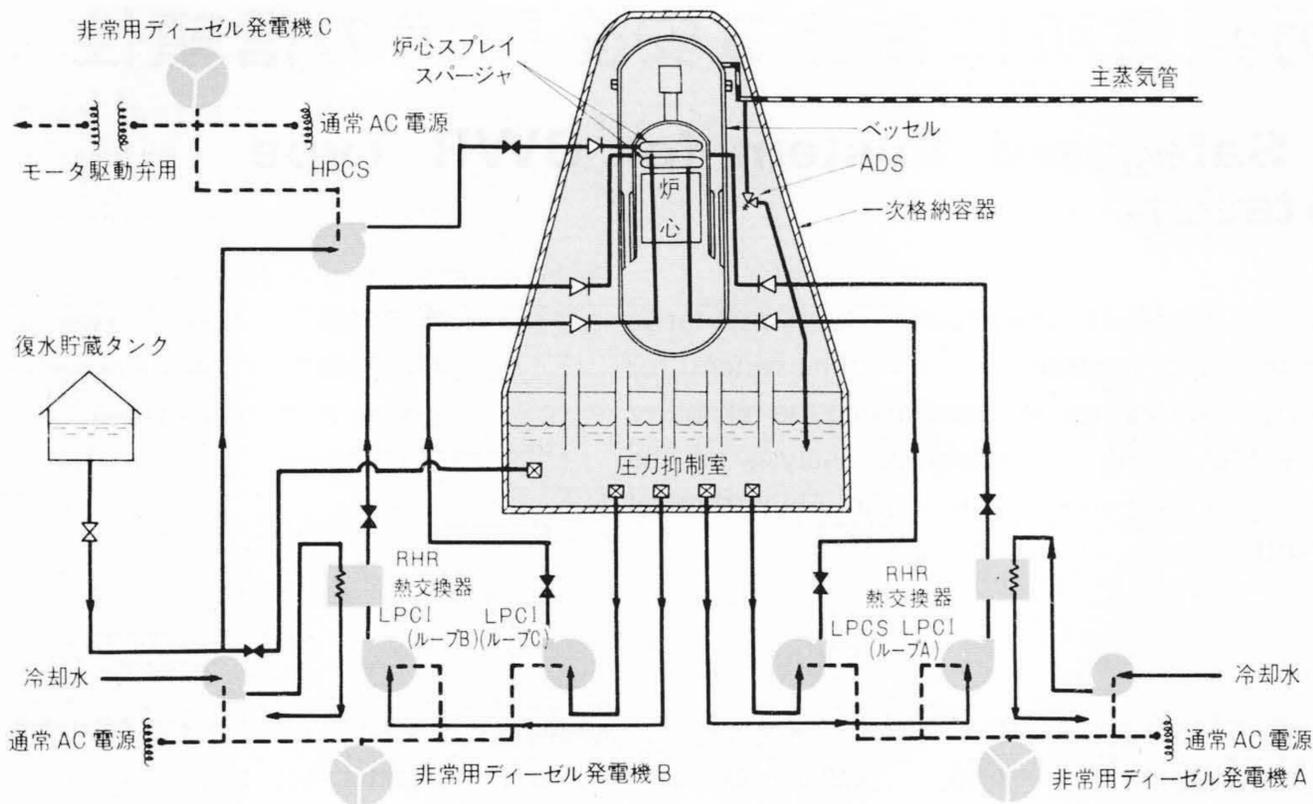


図1 BWR ECCS ネットワーク 炉心冷却機能に対して各種の系統が設けられており、十分な冗長性、独立性を有している。  
Fig. 1 BWR Emergency Core Cooling System

と、それによる ECCS の機能および原子力発電所が受ける影響を定性的に評価した。

評価の結果は、表1に示すとおりである。これにより図1に示す ECCS ネットワークでは、ECCS およびその電源系に十分な冗長性が付与されており、表中(A)~(F)の故障モードに対しても十分な冗長系が残存するので、ECCS の機能がそこなわれることはなく、原子力発電所に対する影響も微小であることが分かる。また、表中(G)の故障モードは、もともと、いかなる最悪の単一故障を仮定しても発生するものではないが、その結果が重大な影響を与えるので、DC電源にはきわめて高信頼度のものを使用するよう要求される。実際 DC電源 (バッテリー) は、信頼度が高く、現実に故障モード(G)が起きる可能性は、他の故障モードに比べてもきわめて低いものと考えられる。

各故障モードは、機器の故障と運転員誤操作に大別されるが、前者は機器の冗長性で、後者はフェイルセーフ設計と厳

重な運転手順管理により、故障モードの発生自体を極小に抑えている。

### 3.2 ECCS アベイラビリティの評価

ECCS は通常時は待機状態にあり、LOCA 時にのみ作動する。このような待機系の信頼度解析には、アベイラビリティの概念を適用するのが妥当である。

アベイラビリティとは、「ある任意の時点で、系統が正常に動作する確率」のことである。ECCS のアベイラビリティ解析は図3の手順に従って行なう。

待機系は、そのアベイラビリティ目標値を維持するために、定期的に作動性確認試験を実施している。

ECCS ネットワークのアベイラビリティ目標値は、LOCA の発生確率と LOCA 時に ECCS が作動しなかった場合に仮定される事故の結果を確率的に評価して決定すべきであるが、現在のところ、まだ広く一般に採用されている評価方法がないので、工学的判断から十分保守的な値を設定している。ECCS の各系統の作動性確認試験周期は、このアベイラビリティ目標値を満足するように決められる。

大破断事故の場合、最小限必要な ECCS は図2に示すとおりであり、ECCS のネットワークのアベイラビリティ  $P_d(S)$  はブール代数で次のように表わすことができる。

$$P_d(S) = P(A + B + C) \dots\dots\dots(1)$$

また、小破断事故の場合も、同様にして次の式が成り立つ。

$$P_s(S) = P(A + E(B + C')) \dots\dots\dots(2)$$

- ここに、
- $P$  : 成功確率
- $A$  : HPCS 成功
- $B$  : LPCS 成功
- $C$  : LPCI (3ループ) 成功
- $C'$  : LPCI (2ループ) 成功
- $E$  : ADS 成功

一方、各系統の成功、不成功の確率は、試験期間  $\theta$  と、コンポーネント故障率に基づいた各系統全体の等価的故障率  $\lambda_T$  から、

$$P_s = 1 - \frac{\lambda_T \theta}{2} \text{ (成功)} \dots\dots\dots(3)$$

$$P_F = \frac{\lambda_T \theta}{2} \text{ (不成功)} \dots\dots\dots(4)$$

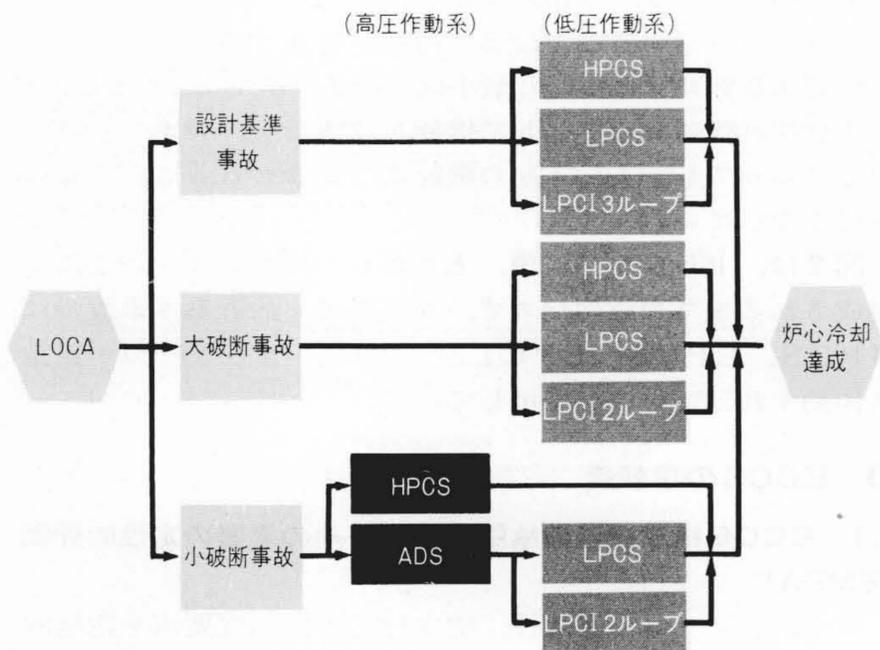


図2 最小限必要な ECCS の組合せ 各種の冷却材喪失事故に対して、十分な冗長性を有している。

Fig. 2 The Combination of Component Systems Initiated for Every Size Break of the LOCA

表 I ECCS 構成機器の故障モードとその影響の解析 (FMEA) ECCS 各系統の故障が ECCS の機能および原子力発電所に与える影響は微小であることが示された。

Table I ECCS Failure Modes and Effects Analysis

ECCS 構成系統	故障モード	残存冗長系統	ECCSへの影響	原子力発電所への影響		結 果
				短 期 間	長 期 間	
(A) LPCS (低圧炉心スプレイ系)	LPCS故障 (原因): 部品の故障	LPCI HPCS	無視できる。	無視できる。	無視できる。	スプレイ冷却有効 リフラッド冷却有効
(B) LPCI (低圧注水系)	LPCI故障 (原因): 部品の故障	LPCS HPCS	炉心リフラッド 時間の遅れ(無 視できる)。	無視できる。	残留熱除去モード 喪失可能性あり。	残留熱除去モードに十分な冗長性を 設けており, 残留熱除去モード喪失 の可能性は無視できる。 スプレイ冷却有効 リフラッド冷却有効
(C) HPCS (高圧炉心スプレイ系)	HPCS故障 (原因): 部品の故障	ADS+LPCS ADS+LPCI	無視できる。	なし	なし	減圧能力有効 スプレイ冷却有効 リフラッド冷却有効
(D) ADS (自動減圧系)	ADS故障 (原因): 弁の多重故障	HPCS	無視できる。	なし	なし	減圧能力有効
(E) 通常AC電源	外部電源および主発電機 の故障 (原因): 送受電線事故	非常用ディーゼル 発電機	無視できる。	なし	なし	非常用AC電源有効
(F) 非常用ディーゼル 発電機	ディーゼル発電機の起 動失敗 (原因): 多重故障	通常AC電源	なし	なし	なし	通常AC電源有効
(G) DC電源系	DC電源の喪失 (原因): 母線の故障 (多重故障)	なし	自動制御喪失 自動起動不可	燃料破損の可能 性あり。	短期間での影響 より小。	運転員はECCSを手動で起動し, 格 納容器を冠水させることができる。 高信頼度のDC電源を設けており, この故障モードの発生確率は無視で きる。

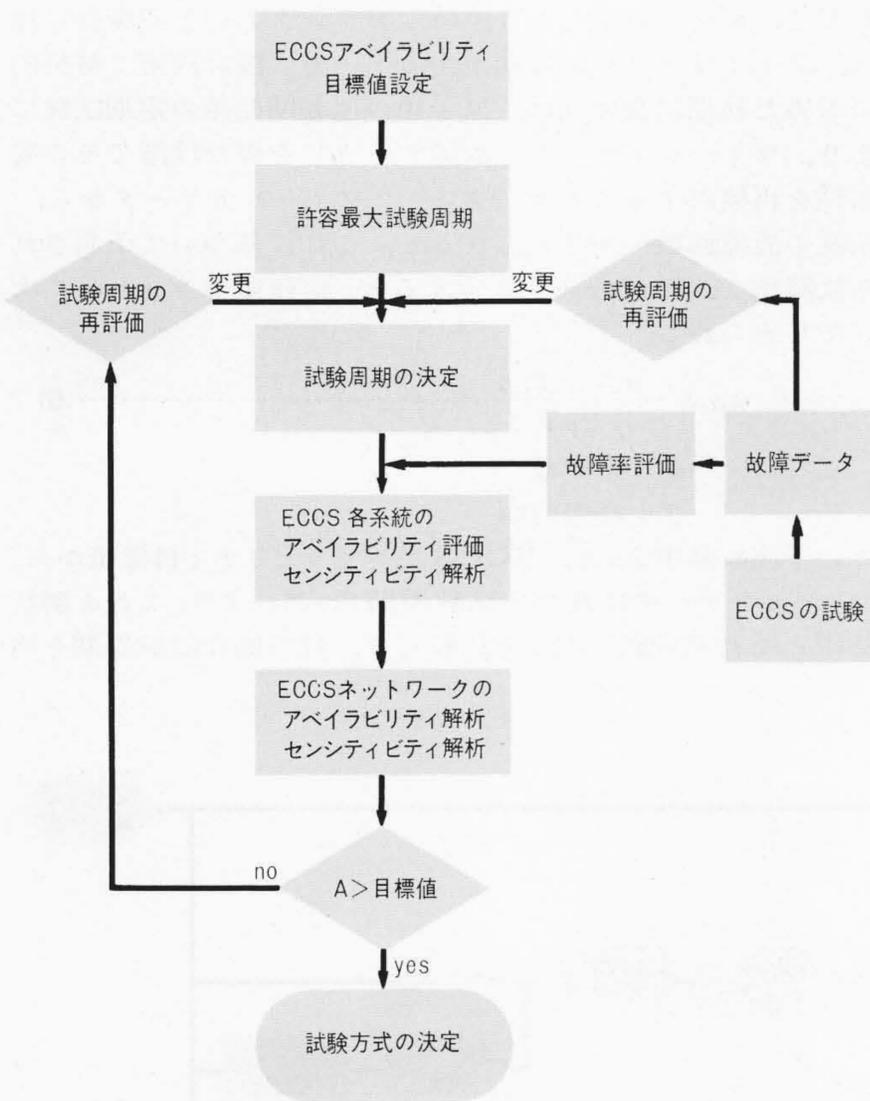


図3 ECCS信頼度評価フローチャート アベイラビリティ解析により, ECCSアベイラビリティが目標値を満足するように試験周期を決める。この結果は故障データにより再評価して, その妥当性を確認する。

Fig. 3 The Process of ECCS Availability Evaluation

で与えられる。

ここで系統 A, B, C, C' に同一の試験周期  $\theta$  を, E には別の値  $\theta'$  を適用すると, ネットワークのアベイラビリティ目標値を満足するための許容最大試験  $\theta, \theta'$  が決まる。

実際に ECCS 各系統に適用する試験周期(初期値)は工学的判断に基づいて決めるが,

- (1) 計算で求めた許容最大試験周期より短くする。
- (2) 試験により, 系統の摩耗を引き起こすほどの頻度は避ける。
- (3) 定期試験計画の組みやすい周期を選ぶ。

この結果, 各系統の初期試験周期は, 表2に示すようになる。このようにして決めた試験周期で, ECCS 各系統の作動性確認試験を実施することにより, ECCS ネットワークのアベイラビリティを目標値以上に維持することができる。

### 3.3 ECCS 構成機器のセンシティブティ

ECCS 各系統の構成機器が, ネットワークの信頼度に及ぼす影響を定量的に評価し, 構成機器の信頼度がバランスのとれたものであるかどうかを判定した。

解析は LOCA の破断規模に応じ, ECCS が成功に至る経路を現実的によく模擬したブロック線図に基づき, 次の仮定に従って行なった。

- (1) 構成機器の故障率  $\lambda$  は時間的に一定で, 指数分布に従う。
- (2)  $\lambda\theta \ll 1$  である ( $\theta$ : 試験周期)。
- (3) 各機器の故障は互いに独立である。

これにより, アベイラビリティは一般的に次式で与えられる。

$$\frac{1}{\theta} \int_0^{\theta} e^{-\lambda t} dt \approx 1 - \frac{\lambda\theta}{2} \dots\dots\dots (5)$$

ブロック線図の一例は, 図4に示すとおりである。これは

表2 ECCSの信頼度評価結果と保全計画への要求 ECCSのある系統が故障した場合でも、許容修理時間以内に修理を行なうが、残りの系統をより頻繁な周期で試験することによりECCSネットワークの信頼度低下を防止できる。

Table 2 Results of ECCS Availability Analyses and Surveillance Requirements

系 統 名	許容最大試験周期 (月)	初期試験周期 (月)	許容修理期間	頻 繁 な 試 験 周 期			
				HPCS 故障時	LPCS 故障時	LPCI 故障時	ADSロジック故障時
H P C S	6.4	3	3週間	—	2週間	3週間	2週間
L P C S	"	"	1ヶ月	2週間	—	"	—
LPCI ループA ループB ループC	"	"	3ヶ月	"	"	—	—
ADS ロジックA ロジックB	8.6	"	2ヶ月	"	—	—	—

設計基準事故時のECCS作動による炉心冷却達成までの成功パスを示したもので、並列系は冗長性を表わしている。

解析の結果、ECCS構成機器がネットワークのアベイラビリティに及ぼす影響（センシティブリティ指数）は、表3に示すようになった。同表中、センシティブリティ指数とは、機器のアンアベイラビリティを一定割合変化させた場合に、ECCSネットワークのアンアベイラビリティに与える変化量のことである。

この値は、各構成機器についてほぼ均一であり、単独の構成機器により、ネットワークのアベイラビリティが左右されることがない。したがって、ECCSネットワーク構成機器のトレードオフ（部品の交換）が十分なされ、バランスのとれた設計になっているといえる。

解析に用いた仮定の妥当性は、ECCSネットワーク構成機器のフィールドでの故障データを分析、検討することにより確認することができる。

4 ECCSの保全計画

4.1 試験方式と試験周期の妥当性の確認

ECCSでは、原子炉の運転中に定期的にその作動性を確認し、アベイラビリティ目標値の維持を図っている。この監視の対象となる機器は、ポンプ、弁、事故検出センサ、電磁リレーなどの動的機器である。動的機器の定期試験では、作動性の確認、性能の確認、目視検査などが行なわれる。

試験は、同じ機能を有する独立な系統については、完全に周期をずらした完全時差方式で実施する。すなわち、最終的な炉心冷却を施すHPCS、LPCSおよびLPCIについては各1ヶ月ずらして試験を実施し、LOCA後の原子炉減圧機能を有するHPCSとADSロジック2系統についても各1ヶ月ずらして試験を実施する。図5は、これを模式的に示した

表3 信頼度に及ぼす構成機器の影響 ECCS構成機器のセンシティブリティは小さく平均化されており、ECCSの設計は、バランスが十分とれている。

Table 3 Sensitivity of ECCS Component

ECCS 構成 機 器	センシティブリティ指数
HPCS	10 <sup>-8</sup> ~ 10 <sup>-6</sup>
LPCS	"
LPCI 各ループ	10 <sup>-8</sup> ~ 10 <sup>-7</sup>
事故検出ロジック	10 <sup>-10</sup> ~ 10 <sup>-8</sup>
通常AC電源	"
非常用ディーゼル発電機	"
DC電源	10 <sup>-11</sup> ~ 10 <sup>-8</sup>

ものである。完全時差方式を採用することにより、任意の時間帯に、作動性の確認された系統を平均して出現させることができ、同時に試験したり、時差をランダムにとる場合に比べ、アベイラビリティは向上する。一方、設計段階で解析的に求めた初期試験周期は、原子炉の運転開始後の定期試験により、フィールドデータ（故障データ）を得た段階でその妥当性を再検討することができる<sup>(1)</sup>。フィールドデータから、系統の故障回数rが与えられると、これに基づいて予測される故障率λ<sub>α</sub>はx<sup>2</sup>分布を仮定すると、信頼限界をαとして次式で与えられる。

$$\lambda_{\alpha} = \frac{x_{2r}^2 + 2, \alpha}{2nT} \dots\dots\dots(6)$$

ここに、 n：系統数  
T：経過時間

この予測故障率λ<sub>α</sub>と、ECCSアベイラビリティ目標値から、フィールドデータに基づく試験周期θ<sub>α</sub>が決まり、これと解析で求めた初期試験周期θを比較して、最終的な試験周期を再

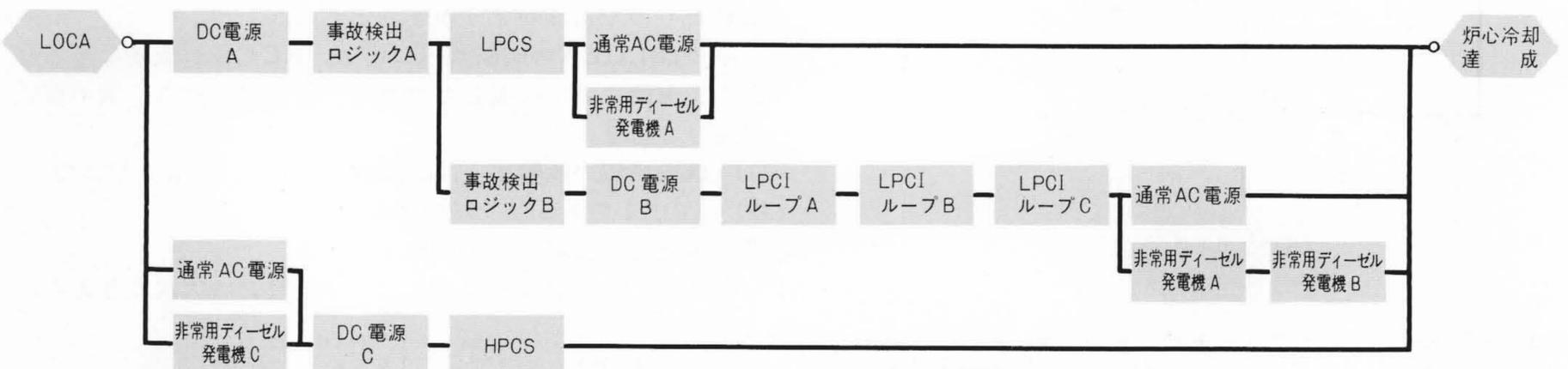


図4 設計基準事故時ECCSアベイラビリティブロック線図 ECCSの成功パスを示す。

Fig. 4 ECCS Availability Block Diagram for Design Basis Accident

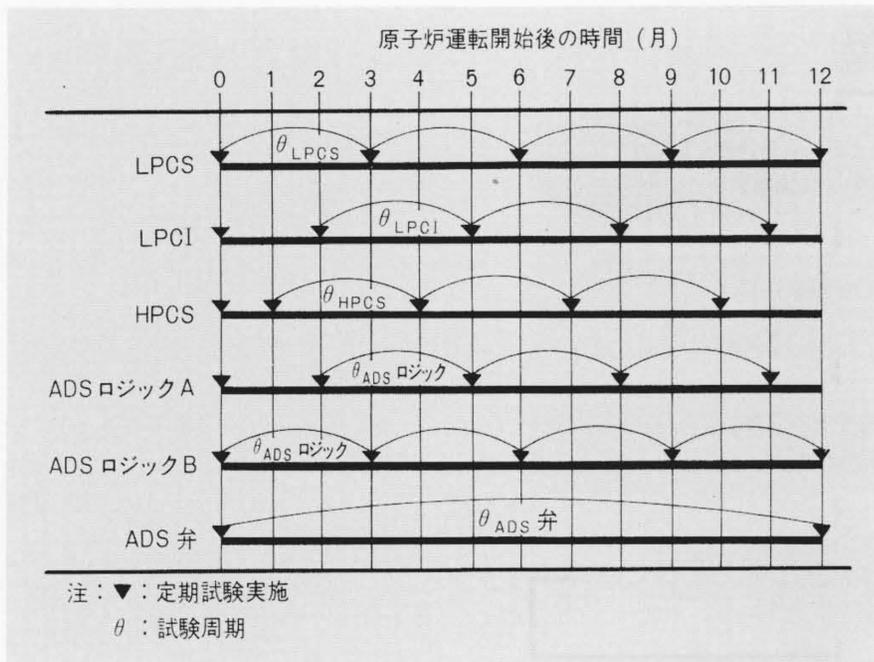


図5 ECCS 試験計画—完全時差方式 高圧作動系, 低圧作動系それぞれ1個月, 1系統の割合で試験をする。

Fig. 5 ECCS Test Schedule — Perfect Staggering

評価することができる。

たいていの場合、フィールドデータに基づく試験周期  $\theta_a$  は、解析で求めた  $\theta$  より長く、解析の保守性が再確認されるにとどまる。仮に  $\theta_a < \theta$  の場合でも、直ちに試験周期を  $\theta_a$  に見合った値に変更すれば、ECCS のアベイラビリティは、目標値以上に保持されることになる。

#### 4.2 ECCS 故障発見時の原子炉運転<sup>(2)</sup>

ECCS の定期的試験で、ECCS 構成機器の故障を発見した場合、原子炉運転員はその故障の内容と程度により次の運転モードのどれかを選択することができる。

- (1) 原子炉の運転を続けながら修理を行なう(運転モードA)。
- (2) 修理が完了するまで原子炉を停止する(運転モードB)。
- (3) 原子炉の運転は続けるが残りの正常な ECCS の試験をより頻繁に行なう(運転モードC)。

原子炉の運転を継続したまま ECCS の故障機器を修理し得る時間(許容修理時間)と、残りの ECCS の試験をより頻繁に行なう場合の試験周期は、

(a) ECCS の構成機器に故障を発見した場合、直ちに残りの系統についても試験を行ない、その作動性を確認していることを前提とする。

(b) ECCS の故障発見後、残った ECCS で期待されるネットワークのアベイラビリティが通常運転中に予想されるアベイラビリティを下回ることはないように、許容修理時間、または新しい試験周期を決定する。

という2点を満足するように決める。

解析の結果は、表2に示すとおりである。

原子炉運転員が、ECCS の定期試験で実際に構成機器の故障を発見した場合は、まず他の ECCS について直ちに作動確認試験を行ない、その作動性を確認し、さらに故障の修復に要する時間を見積る。この時間が解析で求めた許容修理時間より短ければ、修理をしながらプラントの運転を続けることができる(運転モードA)。

修理が完了すると、すぐに全系統を再度試験して修理による影響のないことを確認する。また、修理に要する時間が許容修理時間より長くなる場合は、修理が完了するまで原子炉を停止するか(運転モードB)、正常な側の ECCS の試験を頻繁に行ないつつ、原子炉運転を継続することができる(運

転モードC)。

このように、選択基準を設けることにより、ECCS の構成機器故障時に生ずるかもしれない信頼度低下と、原子炉の稼働率低下を防止することができる。

### 5 フィールドデータの評価<sup>(3)</sup>

ECCS の定期的な作動確認試験で蓄積されたフィールドデータを分析することにより、機器の適切な保全、部品交換を実施することができる。また信頼度解析に用いた仮定、故障率の妥当性も確認でき、妥当でない場合は直ちに試験周期の短縮などにより、アベイラビリティを目標値以上に保持することができる。検討のフローチャートは、図6に示すとおりである。

#### 5.1 故障率による評価

フィールドデータの蓄積が少ない場合は、(6)式に基づいて故障率を予測できる。データの蓄積が十分な場合は、故障率  $\lambda$  は次式で与えられる。

$$\lambda = \frac{\gamma}{nT} \dots \dots \dots (7)$$

ここに、 $\gamma$ ：故障回数

$n$ ：系統数

$T$ ：経過時間

この故障率が解析に用いた値と誤差の範囲を超える程度に異なる場合は、適用している試験周期を変更することにより、ECCS のアベイラビリティ目標値を確保することができる(4.1参照)。

また、その部品の故障率が、他の類似部品の故障率より誤差の範囲を超えて悪い場合は、図6に示すように適切な保全を施すか、部品の交換を行ない、信頼度低下を防止することができる。

#### 5.2 故障発生分布による評価

(1) 系統、機器になんらかの原因で、一時的に過酷な周囲条件、応力などが加わったため、故障が発生することがある(異常状態)。これらは、偶発的に起こる故障(指数分布)とは異なるため、故障発生分布をとると、指数分布より著しくずれた位置にピークを生ずる(図6参照)。

(2) 系統、機器の修理、交換が有効に行なわれていない場合は、部品の早期故障が発生し、故障回数と故障間隔の関係は、本来の偶発故障分布(指数分布)から外れて、故障間隔の短いところで故障回数のピークができる(図6参照)。

このような故障発生分布の評価をすれば、異常状態、早期故障を発見し、直ちに有効な部品交換を実施できるので、あらゆる機器を常に偶発故障期の状態におくことができる。また、信頼度解析に用いた仮定(故障が指数分布に従うという仮定—3.3仮定(1))も妥当となる。

### 6 確率論的安全評価

従来から安全評価では、原子炉での事故発生を前提とし、さらに、この事故に対応して設けられている安全設備に最悪の単一故障が起こると仮定して解析を行なっている。しかし、実際このような事態に至る確率はきわめて低く、事故発生により予想される災害結果(たとえば、敷地周辺被曝線量)を非常に過酷に評価することになる。現在、原子炉では、このような最悪の事故条件に対しても、原子炉周辺の住民に与える被曝線量が、国の目安線量を上回らないだけの十分な機能を持つ安全設備を設けているが、実際の原子炉安全設備は、このうえさらに高信頼度のものであり、事故発生確率をも考

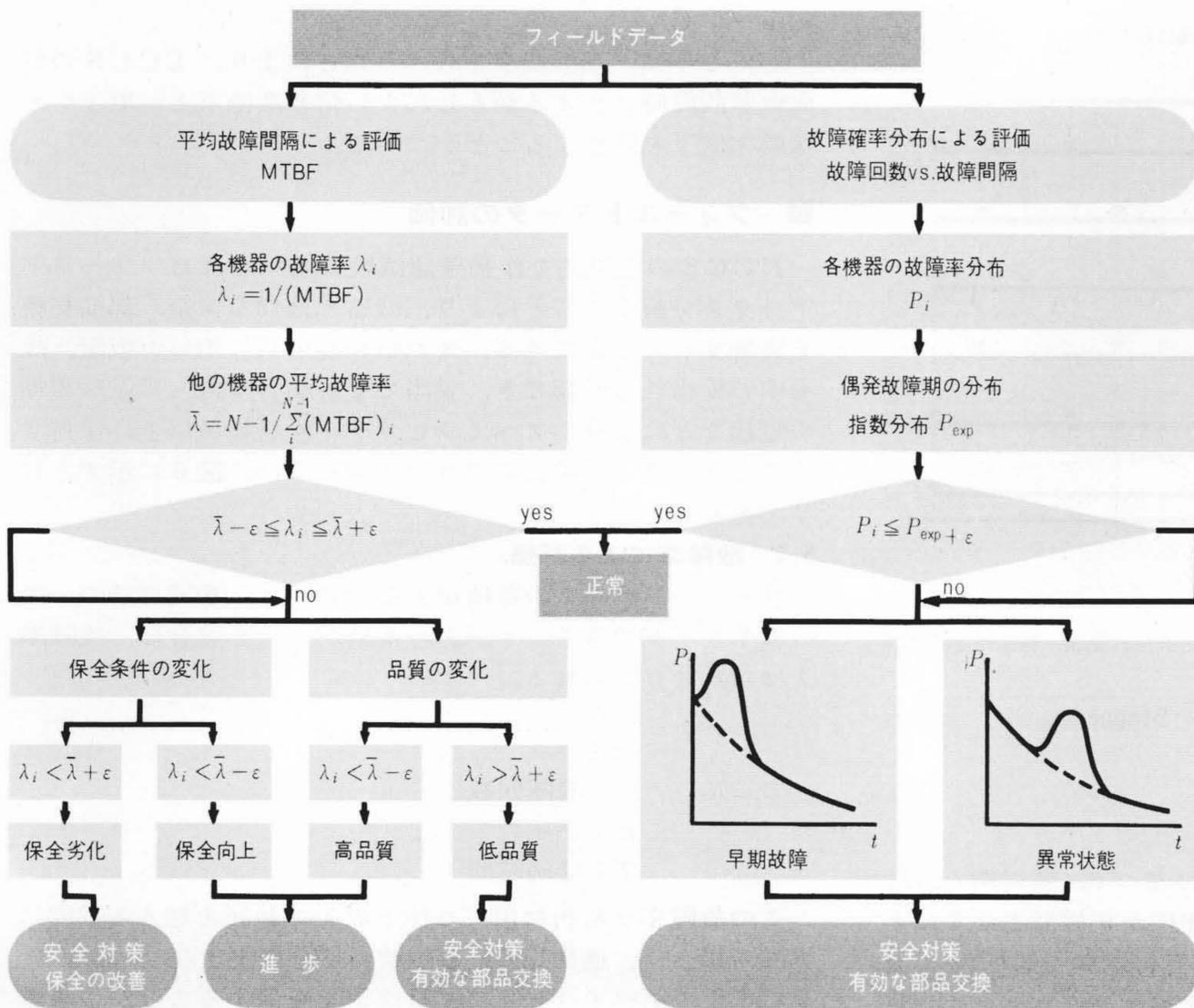


図6 故障データの評価 フィールドデータをこのように分析することにより、機器の適切な保全と部品交換を行なう。

Fig. 6 The Evaluation of Failure Data

慮に入れた現実的な災害結果は著しく微少なものと考えられる。

たとえば、設計基準事故について、それぞれの災害程度を全身被曝線量と被曝確率で評価した結果、事故の災害程度は自然のバックグラウンドで受ける被曝程度と比較しても、十分低いことが示されている<sup>(4)</sup>(図7参照)。

## 7 結 言

BWRの安全性を信頼度解析の面から考察したが、その結果、安全性にとって特に重要なECCSは十分な信頼性をもって、その機能を達成することが示され、以下のような結論

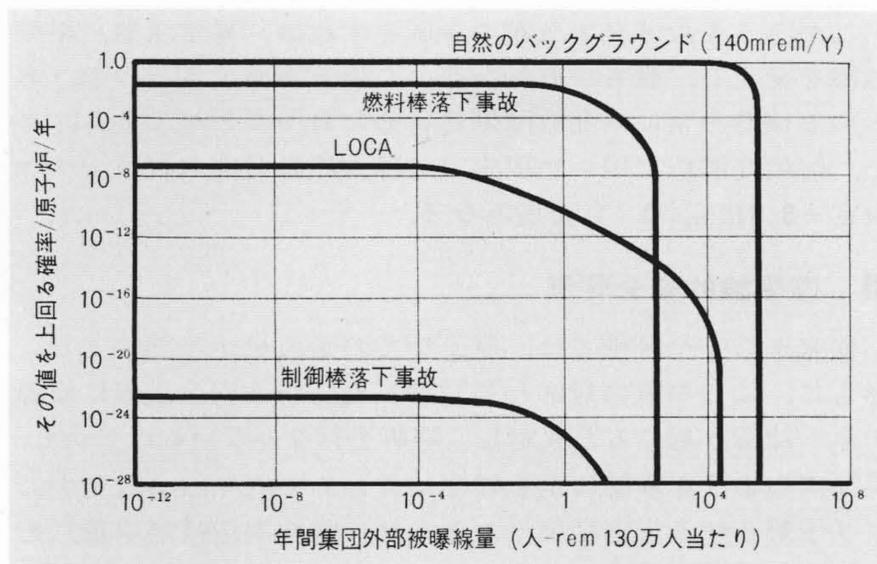


図7 設計基準事故とバックグラウンド放射能被曝量の比較 事故による被曝線量は、自然のバックグラウンドよりも十分小さいことが分かる。

Fig. 7 Comparison of Design Basis Accidents with Natural Background Radiation

を得た。

- (1) BWR-ECCSの故障解析の結果、原子力発電所の安全性および通常運転への影響が微少なことが定性的に示された。
- (2) ECCSのセンシティブリティ解析から、現在のECCSの設計はバランスのとれたものであり、さらに大幅な改良は必要としないことが定量的に明らかとなった。
- (3) 信頼性解析を応用して、系統の試験周期、許容修理時間などに十分保守的なECCSの保安規定を設けているので、系統の信頼度は、原子炉運転中も十分確保できることが分かった。
- (4) ECCS構成機器の故障率は、フィールドデータに基づき合理的に再検討してから、保全計画にフィードバックされるので、原子炉運転中のECCSの信頼度は十分に確保されることが明らかとなった。
- (5) 設計基準事故の確率論的評価によると、BWRの事故により放出される放射能が自然放射能を上回る確率は無視できる程度に低いことが明らかとなった。

## 参考文献

- (1) I. M. Jacobs, "Reliability of Engineered Safety Features as a Function of Testing Frequency", Nuclear Safety, 9, 303, (1968)
- (2) I. M. Jacobs, P. W. Marriott, "Guidelines for Determining Safe Test Intervals and Repair Times for Engineered Safeguards" GE APED-5736, (1969)
- (3) W. E. Vesely, "The Evaluation of Failure and Failure Related Data", USAEC ANCR-1024, (1971)
- (4) I. M. Jacobs, "Assessment of Risk in Reactor Safety", USAEC CONF-730304, 1, (1973)