

PWR プラントのレベル - 1 PSA ベンチマーク解析 (ステップ 3) 事故シーケンス解析と全体のまとめ

Benchmark Exercises on PWR Level-1 PSA (Step 3)
— Analyses of Accident Sequence and Conclusions —

丹羽 雄二 (Yuji Niwa)* 高橋 英明 (Hideaki Takahashi)†

要約 レベル 1 PSA の結果は、統計量を使用することによる本来の数値的揺らぎに加えて、各段階で行われる工学的知見に基づく仮定による不確定性を生ずる。この仮定による不確定性の把握を目的として、解析する標準問題、すなわちベンチマーク問題を 3 題設定した。本報告では、事故シーケンスに関するベンチマーク問題の解析を通して得られた知見について述べる。システム間の依存性の取扱いが PSA の不確性を発生しうる。またこれまで実施してきた他のベンチマーク問題も併せて、得られた種々の知見を整理する。

キーワード ベンチマーク, 事故シーケンス解析, システム間の依存

Abstract The results of level 1 PSA generate fluctuations due to the assumptions based on several engineering judgements set in the stages of PSA analysis. On the purpose of the investigation of uncertainties due to assumptions, three kinds of a standard problem, what we call benchmark exercise have been set. In this report, sensitivity studies (benchmark exercise) of sequence analyses are treated and conclusions are mentioned. The treatment of inter-system dependency would generate uncertainty of PSA. In addition, as a conclusion of the PSA benchmark exercise, several findings in the sequence analysis together with previous benchmark analyses in earlier INSS Journals are treated.

Keywords benchmark, accident sequence analysis, inter-system dependency

1. ベンチマーク問題 B の解析

1.1 事故シーケンスのモデル化

図 1 に、各ベンチマーク問題(1)の範囲を示す。ベンチマーク問題 B は、「破損蒸気発生器(SG)の隔離失敗」および「1次系の減圧失敗」の多重のヒューマンエラーからなる事故シーケンスである。本ベンチマーク問題の解析は、既に実施しているが(2)、本報告においては詳細イベントツリーの解析条件の見直しと、感度解析を実施した。

PSA における従来の人間信頼性解析(HRA)に対しては、次のような批判がある。

予期しないシナリオの可能性を増大させる「不適切な行為」としてのコミッションエラーが考慮されていない。事故時において様々に行われる意思決定

は得られた情報に基づいて行われることから、他のシナリオが発生していると見誤り、不適切な行為を行う要因として、計装系の故障等によるプラント情報に関した問題が重要となる。

同じ事故シーケンスカットセット中に複数のヒューマンエラーが含まれる場合、これらは独立な事象として取扱えない場合が多いであろう。この場合、確率的な依存性をどう評価するかが問題になる。同じ原因により複数の事象が影響を受ける場合や、その結果により他の事象が影響を受ける場合には、明確に依存性が存在するが、現在行われている HRA ではエラーの原因を追求しないため、依存性を考慮することは困難である。

本研究では、上記のような問題を検討するため、多重のヒューマンエラーを含んだシーケンスを対象とし、ヒューマンエラーの原因を検討しながら解析

* (株)原子力安全システム研究所 技術システム研究所

† (株)三菱総合研究所 総合安全研究センタ

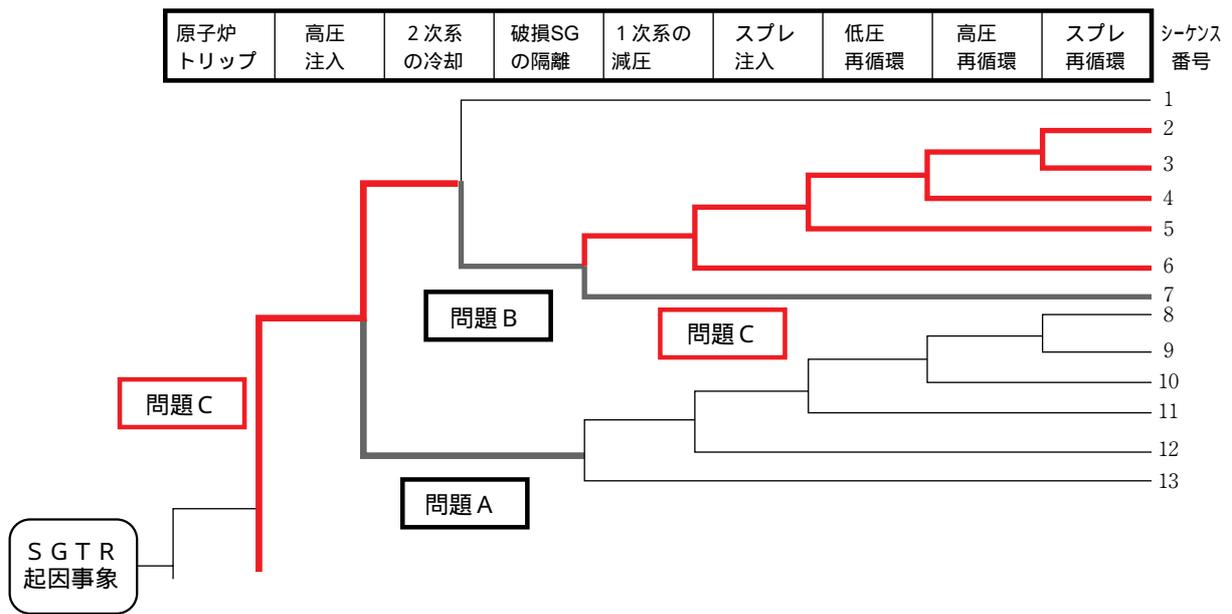


図1 ベンチマーク問題の設定

を実施した。但し、対象としている事故シーケンスならびに事故時の対応は、国によって、また個々のプラントにおける運用上の違いによって、異なったものとなり得るものであることに注意する必要がある。

図2に、「破損SGの隔離」と「1次系の減圧」に対して展開した詳細イベントツリーを示す。従来の一般的なスモールイベントツリーによる表現では、「破損SGの隔離」と「1次系の減圧」は、図1のように単純に2つのヘディングで表現される。しかし、実際には事故の原因や状況に応じて様々な認知と判断が関与することから、現実をこのように単純なツリーの形態で表すことには無理がある。このために、可能性のある状況を考慮の上、より詳細に展開したイベントツリーを構築した。詳細イベントツリーにおけるヘディングの内容は次のとおりであり、ハードウェア故障も含んだものとなっている。

- (1) 蒸気発生器伝熱管破損事故(SGTR)の認知
- (2) 破損SGの同定
- (3) タービンバイパス弁等の自動閉止
- (4) 自動閉止失敗時の手動バックアップ
- (5) 手動バックアップ操作の対象となる弁の正常動作
- (6) 破損SGの補助給水との隔離操作

- (7) 隔離操作の対象となる弁の正常動作
 - (8) ハードウェア故障の認知
 - (9) 一次系の減圧操作(加圧器逃し弁の開放)
 - (10) 加圧器逃し弁の正常動作
- これらのシーケンスについては、判断状況によって次の4つのケースに分類される。

- (A) 隔離すべき弁が故障により閉止しなかったが、閉止していないことが表示灯で確認された
- (B) 隔離すべき弁が故障により閉止しなかったが、閉止の確認をしなかったため、状況の正確な判断ができていない
- (C) 破損SG隔離操作上のエラー(行動エラー)により、隔離されなかった
- (D) 破損SGの同定に失敗した

これらの、シーケンスの対応については、図2において、円で囲まれたA, B, C, Dで表している。ヒューマンエラーに係わる上記の各ヘディングに対して、事象の進展状況と、ヒューマンエラーの形態および主要原因を検討し、この結果をHRAに反映した。ヒューマンエラーに係わる各ヘディングに対する検討の概要は次のとおりである。

ヘディング：SGTRの認知

SGTRにおいては、伝熱管の破損に伴う1次冷却

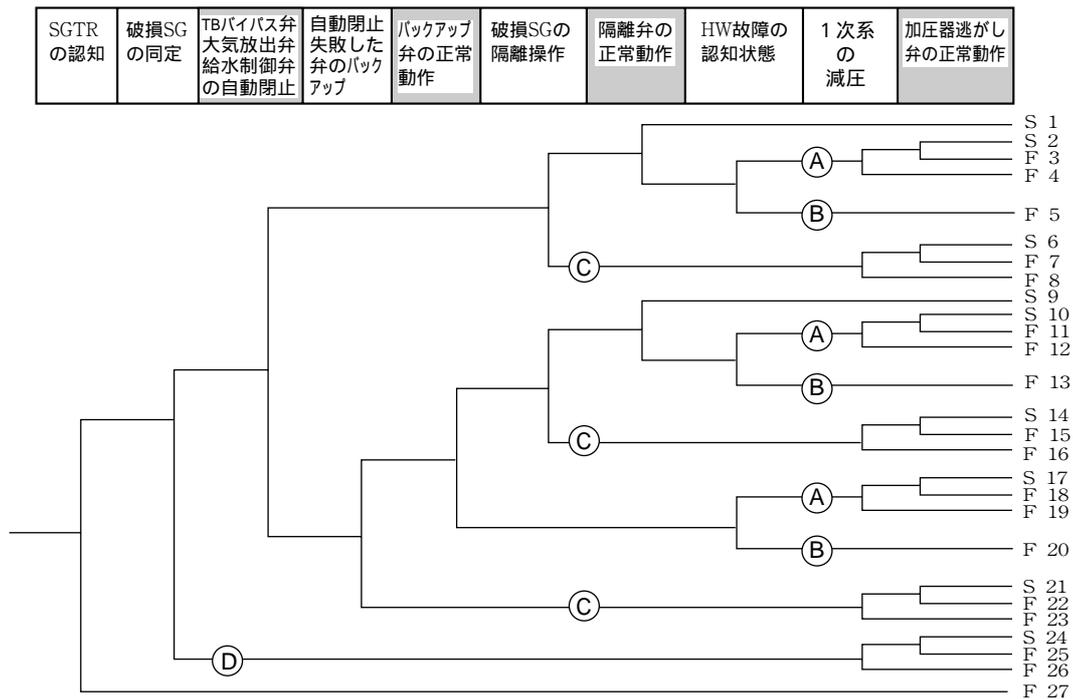


図2 SGTR時操作の詳細イベントツリー (OAET; Operator Action Event Tree)

材の流出により、1次系の減圧が始まる。1次系の減圧により、原子炉は「原子炉圧力低」または「過大温度 T高」信号によって自動停止する。また「原子炉圧力低」信号によるS I信号によって、非常用炉心冷却設備が作動する。更にSI信号の発信により給水隔離がなされ（給水制御弁の閉止）、補助給水ポンプが起動する。原子炉トリップ後は、タービンバイパス弁によって蒸気発生器の2次側の蒸気が復水器へと導かれ、2次側の圧力上昇が抑えられる。

運転員は、SGブローダウンモニタまたは復水器空気抽出器ガスモニタの線量率が上昇しているのを見て、SGTRの発生を確信する。「事故の認知に失敗し、誤った対応を選択する」主要な原因として、次のようなことが考えられる。

- 知識不足，不慣れ，訓練不足
- 計装系の故障
- 警報による混乱

しかし実際には、事象ベースの事故の代表例として訓練が良く実施されており、ハードウェア故障を仮定しなければ、認知失敗の確率は小さいものと期待できる。ハードウェア故障についても、どちらか

のモニタが健全であればよいことから、確率は小さい。LBBが存在せず急に伝熱管が破断した場合、または複数の伝熱管破断が発生して多数の警報が同時発信した場合にはSGTRの認知に失敗する可能性が高くなるが、このような事象の発生は無視できるほど小さいものと仮定する。以上のことから、「SGTRの認知に失敗する」重大な要因は考えられず、この確率は比較的小さいものと想定される。

ヘディング：破損SGの同定

破損SGの同定には、放射線管理課係員によるオフラインサンプリングの結果を判断の最終材料とすることが望ましい。しかしこのためには30分程度の時間がかかることから、事故の発生後にサンプリングにとりかかることによる同定は期待できない。実際には下記のパラメータで破損SGを同定することが要求される。

- (1) 各ループの「給水流量」と「蒸気流量」のミスマッチ
- (2) SGの水位上昇，圧力上昇
- (3) 補助給水流量ループ間の偏差

これらのうち、(1)が運転員間の認識では最も親

しんだパラメータと考えられる。流量ミスマッチの警報はあるが、1本破断のSGTRで警報が発生するかどうかは不明であるため、常に運転員による認知が必要であるとする。

(1)の認知方法により「状況の判断に失敗し、誤った対応を選択する」原因として、次のようなことが考えられる。

知識不足、不慣れ、訓練不足

計器の選択ミス

流量の偏差の読み取りミス

流量計等の故障

判断ミス

思いこみ、過信（シミュレータと違った挙動を示した場合、判断できると思っていたことができなくなる可能性がある）

SGTRの認知と同様に、事象ベースの代表例として訓練もよく実施されていることから、第1番目の要因の影響は小さいものと期待できる。計器の配置は特にミミック化はされていないが、流量偏差評価のための視認性はかなり良いものと考えられることから、第2および第3番目の要因の影響も小さいものと考えられる。また流量計等のハードウェア故障も、確率的には影響が小さいものと考えられる。

破損SGの同定に失敗するケースとしては、(1)の情報がシミュレータほど明確には得られず、これで(2)(3)の評価を忘れてしまうことが挙げられる。また計器（3ペン式のリコーダ）の公差を偏差と思いこみ、別のSGを破損SGと同定する可能性も考えられる。機器の計器の選択ミスや読み取りミス等の単純なミスよりも、これらの影響のほうが大きいものと考えられる。

ヘディング：自動閉止に失敗した弁の手動バックアップ

次の手動バックアップを行う。

(1) 主蒸気逃がし弁が再開止失敗した場合は、その元弁を閉止

(2) タービンバイパス弁が再開止失敗した場合には、主蒸気隔離弁を閉止

(3) 給水制御弁が自動閉止失敗した場合は、手動で閉止

手順書に従い、給水制御弁および主蒸気逃がし弁

は、コントローラにて閉止確認を行う。タービンバイパス弁はランプで確認する。これらの弁が自動閉止に失敗した場合に、「気がつかなかつたり、選択や操作の誤りによって、バックアップ操作に失敗する」原因として、次のようなことが考えられる。

知識不足、不慣れ、訓練不足

モニタライトの不適切なレイアウト等により、故障の判断が困難

心理的ストレス

SGTRの認知と同様に、事象ベースの代表例として訓練もよく実施されていることから、第一の要因の影響は小さいものと期待できる。対象弁の状態確認のためのモニタライトが存在し、プラントデザインの点でもかなり重視されたものとなっていることから、第二の要因の影響は小さい。弁の手動バックアップに失敗するケースとしては、タービンバイパス弁が非安全系の弁であること、および高い心理的ストレス条件下で、「モニタライトの確認を忘れる」ことが挙げられる。

ヘディング：破損SGの隔離操作

「不履行、選択や操作誤りによって、隔離操作に失敗する」原因として、次のようなことが考えられる。

知識不足、不慣れ、訓練不足

不適切なレイアウトや不明瞭なラベル

心理的ストレス

SGTRの認知と同様に、事象ベースの代表例として訓練もよく実施されていることから、第1番目の要因の影響は小さいものと期待できる。スイッチ類の配置は特にミミック化はされていないが、整理された配置となっていることから、第2番目の要因の影響も小さいものと考えられる。ストレスの影響以外、特殊な影響要因はない。

ヘディング：バックアップ用弁または隔離弁の動作不良の場合の、故障の認知

タービンバイパス弁等が自動閉止に失敗した際に、バックアップ操作を行っても弁の動作不良によってバックアップに失敗した場合、「そのことに気がつかない」原因として、次のようなことが考えられる。

確認しなかった

故障の判断が困難
 心理的ストレス
 表示灯等の故障
 思い込み，過信

破損SGの隔離が弁の動作不良によって失敗した場合、「そのことに気がつかない」原因も同様である。中央制御室で操作する弁は、表示灯により開閉状態が表示されるので、確認により故障の判断が可能である。現地弁は、表示灯が中央制御室に表示されないため、認知が不可能である。他の要因はすべてあり得るものである。

ヘディング：1次系の減圧操作

「状況の判断に失敗し、誤った対応を選択する」原因として、次のようなことが考えられる。

知識不足，不慣れ，訓練不足
 心理的ストレス
 肉体的ストレス
 時間的ストレス
 躊躇
 意図的な不履行

ストレス要因については、隔離操作の後にはすぐにRCSの冷却操作や減圧操作を実施しなければならず、これらが運転員への大きな心理的負荷となることから、SG水位等からパラメトリックに状況を判断する必要がある状況が発生した場合には、加圧器逃し弁の開操作による一次系の減圧の必要性を判断することは困難と考えられる。躊躇や意図的な不履行については、加圧器逃し弁の開放自身が、放射性物質閉じ込めの物理的障壁の1つであるRCSバウンダリを破る操作であるだけに、運転員にはこの操作に対して「ためらい」があることも予想できる。そのため、これが操作時期を誤るといった原因にもなりかねない。また同様の理由から、明らかに加圧器逃し弁を開放すべき状況が発生していない限り、むやみに実施はしない可能性があるものと考えられる。

これらを考慮すると、1次系の減圧操作を実施する各ケース（図2(A)~(D)）は、次のように考えられる。

(A)のケース（隔離弁が故障により閉止しな

ったが、閉止していない事が表示灯で確認された場合）では、上記の「ためらい」はあるものの、一次系の減圧操作を実施するという判断を行う状況が発生している。この場合の診断エラーの評価には、時間信頼性曲線のノミナル値の適用が妥当であろう。

(B)のケース（隔離弁が故障により閉止しなかったが、閉止の確認をしなかったため、状況の正確な判断ができていない場合）では、一次系の減圧操作を直ちに実施するという判断はできないものと考えられる。この場合の診断エラーの評価には、時間信頼性曲線の上限値の適用が妥当であろう。余裕時間は10分とする。この場合、診断エラーの確率は1.0となるが、判断が困難という状況を考えると、妥当な数値と考えられる。

(C)のケース（操作エラーにより隔離されなかった場合）では、状況の把握に基づき1次系の減圧操作を実施するという判断を行うことが期待できる。この場合の診断エラーの評価には、時間信頼性曲線のノミナル値の適用が妥当であろう。

(D)のケース（破損SGの同定に失敗した場合）では、必然的に適切な隔離ができていないということから、一次系の減圧操作を実施するという判断を行う状況が発生している。この場合の診断エラーの評価には、時間信頼性曲線のノミナル値の適用が妥当であろう。

「選択や操作の誤りによって、操作に失敗する」原因として、次のようなことが考えられる。

知識不足，不慣れ，訓練不足
 不適切なレイアウトや不明瞭なラベル
 心理的ストレス
 肉体的ストレス
 時間的ストレス

第1番目および第二の要因の影響は小さいと考えられるが、各種ストレス要因により、加圧器逃し弁による一次系の減圧操作を終了すべき条件になっていないにもかかわらず操作を終了してしまい、そのまま炉心温度のチェックが行われずに、炉心の再加熱が起こる可能性も否定できない。このような検討

に基づき，表 1 に HRA の際の解析条件をまとめた。

1.2 事故シーケンスの解析

作成したイベントツリー中の各ヒューマンエラー要素に対して，THERP手法による解析を実施した。表 2 に，図 2 の各シーケンスの進展確率をまとめた。全シーケンスの進展確率のうち約 3 分の 1 が，何らかのハードウェア故障が関係したシーケンスによるものとなった。このうちの 2 分の 1 以上はシーケンス 4，即ち，破損 SG の隔離操作は実施したが弁の故障によって隔離されず，このことに気がつかずに 1 次系の減圧操作を実施しないということによるものである。

表 1 に記載したとおり，ハードウェアの故障によって弁が閉じないということはモニタイトで確認でき，また確認すべきことが手順書で指示されているという解析条件を設定している。これらの条件により，ヒューマンエラーの確率評価において比較的小さな過誤率が算出されているが，それでも寄与率

シーケンス番号	進展確率	寄与割合	HW故障の関与
3	1.31E-6		Yes
4	8.12E-4	22.7%	Yes
5	6.70E-5	1.9%	Yes
7	3.55E-6		Yes
8	2.20E-3	61.6%	
11	6.47E-8		Yes
12	4.00E-5	1.1%	Yes
13	3.30E-6		Yes
15	1.75E-7		Yes
16	1.08E-4	3.0%	Yes
18	4.98E-8		Yes
19	3.08E-5	0.9%	Yes
20	2.54E-6		Yes
22	1.54E-7		Yes
23	9.49E-5	2.7%	Yes
25	1.78E-7		Yes
26	1.10E-4	3.1%	
27	1.00E-4	2.8%	
合計	3.57E-3	99.8%	32.5%

表 2 詳細イベントツリーの解析結果

	SGTRの認知	破損SGの同定	自動閉止した弁の手動ハックアップ	破損SGの隔離	HW故障の認知	1 次 系 の 減 圧 操 作		
						(A)	(B)	(C)
認知エラーの考慮 (1)許容診断時間 (2)上限/ミナル/下限	考慮する 30分 下限値	考慮する 30分 ミナル値	考慮しない	考慮しない	考慮しない	考慮する 10分 ミナル値	考慮する 10分 上限値	考慮する 10分 ミナル値
行動エラーを考慮する操作	なし	なし	1.スラップ等で閉止確認 2.主蒸気隔離弁の閉止(制御室操作)	1.電動補助給水ポンプ出口電動弁の閉止 2.補助給水量調整弁閉	1.モニタイトの確認	1.加圧器逃がし弁2/2第を強制開放(スラップリターンスイッチ) そのまま長時間保持(24Hr)		
PSF (1)手順書 (2)経験レベル (3)ストレスレベル (4)タリクレベル (5)当直長等による過誤の回復 (6)電動弁やHCVのためのスイッチに関するPSF (7)タリク間の依存性 (8)タリク間の依存性			ログリスト チェック欄あり 熟練 極度に高い 普通 考慮する (特に要請されたチェック) 2方向スイッチ機能別配置 スラップなし 保持必要 確認と操作 OM:高依存 CM:中依存 Step By Task	ログリスト 同左 熟練 極度に高い 普通 考慮する (特に要請されたチェック) 2方向スイッチ機能別配置 スラップなし 保持必要 MOVとHCV操作 OM:高依存 CM:中依存 Step By Task	ログリスト 同左 熟練 極度に高い 普通 考慮する (特に要請されたチェック) モニタイト	ログリスト チェック欄あり 熟練 極度に高い 普通 考慮する (特に要請されたチェック) 2方向スイッチ機能別配置 スラップによる侵害なし スイッチの長期保持必要		
エラーの主要原因	・知識不足 ・不慣れ ・訓練不足 ・計装系の故障 ・警報による混乱	・知識不足 ・不慣れ ・訓練不足 ・スラップ ・計装系故障 ・思いこみ	・知識不足 ・不慣れ ・訓練不足 ・不適切なレイアウト等 ・心理的ストレス	・知識不足 ・不慣れ ・訓練不足 ・不適切なレイアウト等 ・心理的ストレス	・スラップ ・心理的ストレス ・表示灯故障 ・思いこみ、過信	・知識不足、不慣れ、訓練不足 ・心理的ストレス ・時間的ストレス ・肉体的ストレス ・躊躇 ・意図的な不履行、不適切なレイアウト等		

表 1 人間信頼性解析における解析条件表

は大きい。更に、図2の「バックアップ弁の正常動作」のヘディングで弁の故障に共通要因故障を考慮した場合には、全確率の41%がハードウェア故障が関与したシーケンスによるものとなり、ヒューマンエラーの確率として評価結果の下限値を適用した場合には、全確率の78%がハードウェア故障が関与したシーケンスによるものとなった。

1.3 ベンチマーク問題Bの解析によって得られた知見

人的過誤による不確定性を評価するためのベンチマーク問題Bとして次のような知見が得られた。

知見1：THERPによる行動エラーの評価においては、特に次の取扱いの影響が大きい。
 ストレスレベル
 タスクの難易度（ステップバイステップタスクかダイナミックタスクか）
 エラーの回復（当直長等による回復の効果）
 これらの扱いにより、単独の要素によりファクター5程度の差異を生じ得る。

知見2：単一の事故シーケンス中に複数のヒューマンエラーが存在する場合は、それらの間の依存性をどのように仮定するかで、シーケンスの解析結果には大きな差異が生じ得る。従来の単純なイベントツリーをベースとしただけでは依存性を議論することは困難である一方、依存性をどういった形で反映するかによって、解析結果には大きな違いを生じ得る。

知見3：詳細なイベントツリーを構築することにより、状況の進展や必要な判断、およびヒューマンエラーとして考慮している範囲が分かりやすく表示され、従来のイベントツリーと比べて理解しやすい。またエラーの原因も検討しやすく、これによりヒューマンエラー間の依存性の問題も考えやすい。

知見4：従来のイベントツリーのレベルでは考慮し

ていない、ハードウェアの故障の影響（ハードウェア故障が原因となったヒューマンエラー生起を含んだシーケンスの存在）が、無視できない程度に存在する可能性がある。このようなシーケンスは図2のようなイベントツリーを検討すること、また表1に示した形でヒューマンエラー評価上の条件を検討・整理することによって評価することができる。

2. ベンチマーク問題Cの解析

2.1 事故シーケンスのモデル化

ベンチマーク問題Cは、複数のフロントラインシステムの失敗または成功の組み合わせで表現される事故シーケンスを対象としたものである。関係するフロントラインシステムの数が増えると共に、これらに関わるサポートシステムも増加し、ベンチマーク問題Aと比べてシステム間の相互作用が複雑になる。

ベンチマーク問題Cのモデル化に関わる系統は次のとおりである。

- (1) 高圧注入系(注入モードおよび再循環モード)
- (2) 補助給水系
- (3) 加圧器逃がし弁等
 - 格納容器スプレイ系(注入モードおよび再循環モード)
 - 低圧注入系(再循環モード)
 - 電源系
 - 工学的安全施設起動系
 - 補機冷却水系
 - 補機冷却海水系
 - 制御用圧縮空気系

ベンチマーク問題Cで初めて関係する各システムの成功基準ならびにバックアップに関するモデルの設定を以下に示す。

- (1) 高圧注入系(注入モード)
 - (a) 3台中1台の充てんポンプが起動し、運転を継続すること。
 - (b) 3ループ中2ループへの注入があること。
 - (c) ほう酸注入タンクのヒーターが機能して

- いること。
- (d) ほう酸注入タンクを通るルートが使えない場合、補助注入ラインによるバックアップが考慮できる。
- (2) 高圧注入系（再循環モード）
- (a) 2台中1台の余熱除去ポンプが起動し、運転を継続すること。
- (b) 2台中1台の余熱除去冷却器が機能していること。
- (c) 3台中1台の充てんポンプが運転を継続すること。
- (d) 注入時に開いているRWS Tからのライン上の電動弁が、再循環モードでは閉止すること。
- (e) ほう酸注入タンクのヒーターが機能していること。
- (f) ほう酸注入タンクを通るルートが使えない場合、補助注入ラインによるバックアップが考慮できる。
- (3) 格納容器スプレイ系（注入モード）
- (a) 4台中2台の格納容器スプレイポンプが起動し、運転を継続すること。
- (b) 4つのスプレイリングのうち2つのリングからスプレイがなされること。
- (4) 格納容器スプレイ系（再循環モード）
- (a) 4台中2台の格納容器スプレイポンプが運転を継続すること。
- (b) 4つのスプレイリングのうち2つのリングからスプレイがなされること。
- (c) 2台中1台の熱交換器が機能していること。
- (d) 注入時に開いているRWSTからのライン上の電動弁が、再循環モードでは閉止すること。
- (5) 補機冷却水系
- (a) 4台中2台の補機冷却水ポンプが起動し、運転を継続すること。3台中2台の熱交換器が機能していること。
- (6) 補機冷却海水系
- (a) 4台中2台の補機冷却海水ポンプが起動し、運転を継続すること。
- (7) 制御用圧縮空気系
- (a) 系統分離がなされている。

- (b) 1系統が使用不能になった時のタイライン手動開による回復操作を考慮する。
- (c) 2台中1台のコンプレッサーポンプが起動し、運転を継続すること。
- (d) 2台中1台のコンプレッサー用熱交換器が機能していること。
- (e) 雑用空気系によるバックアップは考慮しない。

図3に、サポートシステム間の依存関係を示す。図からわかるように、依存関係にはいくつかのループが生じている。本研究では、まずこれらの関係を正確に反映したフォールトツリーモデルを構築した。サポートシステムのフォールトツリーモデルの階層図を、図4に示す。各系統間の依存関係をこのような多重の階層関係でモデル化することにより、各フロントラインシステムのモデルに接続する際には、サポートシステム間に存在するループの影響がすべて反映されたものなる。

2.2 事故シーケンスの解析

ベースケースとして、前記のようなシステム間の依存関係を正確にモデル化したフォールトツリーの解析を行った。解析にあたって使用した各種データ（機器故障率、ファクター、待機除外確率、使命時間）は、Surryプラントを対象としたPSAレポート（NUREG/CR-4450 Vol.3, Rev.1）から引用した。共通要因故障のモデルはファクター法であり、共通要因故障を考慮する機器および故障モードは次のとおりである。

電動ポンプの起動失敗

電動弁の開失敗

電動弁の閉失敗

空気作動弁の開失敗

非常用DGの起動失敗

ストレーナの閉塞

使命時間は次のとおりである。

フロントラインシステムの注入モード：12時間

フロントラインシステムの再循環モード：24時間

補助給水系：6時間

試験の周期は次のとおり設定した。

定期試験を実施していると考えられる機器：

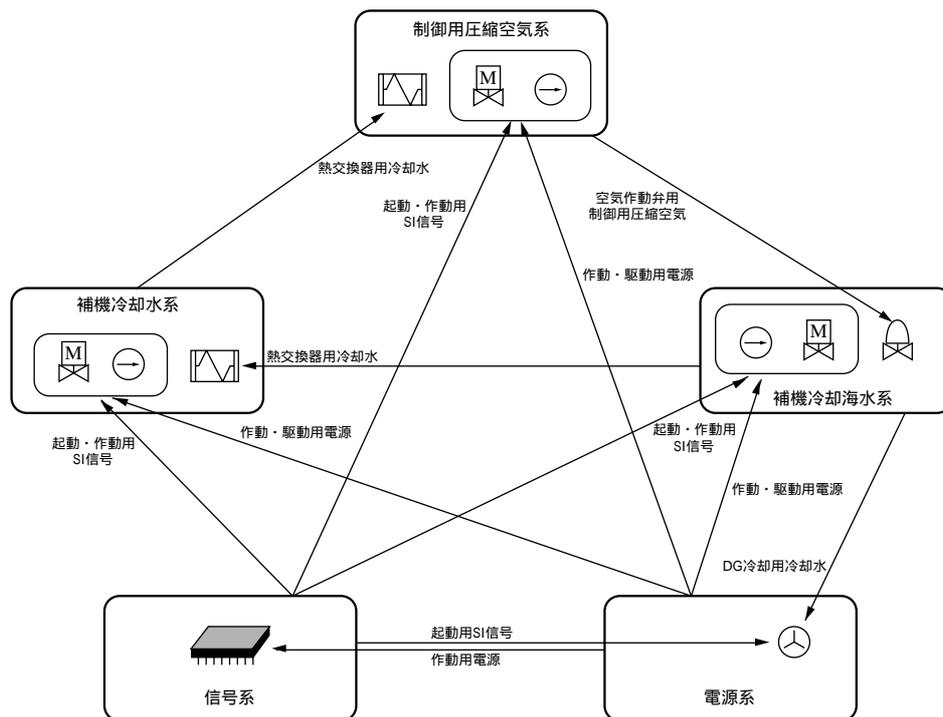


図3 サポート系間の関係

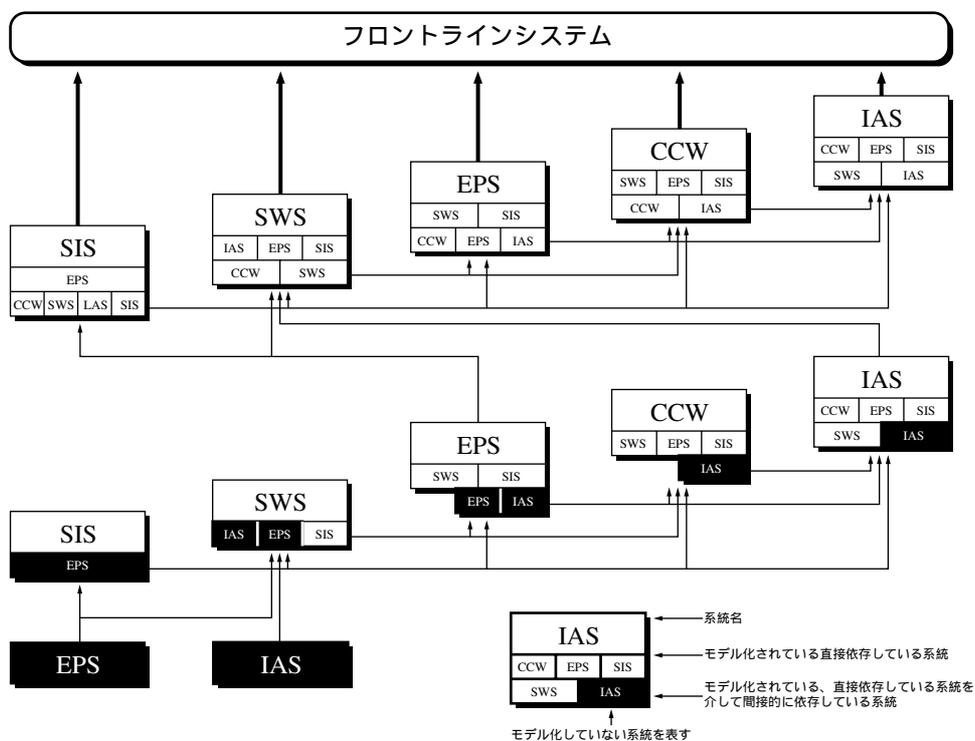


図4 サポート系間の依存関係

720時間

格納容器内にあるなど、試験が考えられない機器：8760時間

ヒューマンエラーについては、新たに次のエラーの評価を行った。

- (1) 各系統におけるポンプなどの試験時のヒューマンエラー
- (2) 事故時の、注入モードから再循環モードへの切替に係わるヒューマンエラー
- (3) 事故時の、制御用圧縮空気系のタイライン開操作に係わるヒューマンエラー

フォルトツリー解析によって得られた各フロントラインシステムのミニマルカットセット (MCS) を見ると、共通要因故障とヒューマンエラーの寄与が優勢であるが、サポートシステム中の機器故障の寄与も目立つものとなった。特に高圧注入系と格納容器スプレイ系の注入モードは、AC母線Aの機能喪失あるいは制御用圧縮空気系Aトレインの機能喪失によって失敗に至っている。これは、

- ・ AC母線A系統の機能喪失 補機冷却海水系の空気作動弁が閉 補機冷却水系熱交換器2基への冷却水が喪失 補機冷却水系による各種ポンプ等の冷却機能が喪失
- ・ 制御用圧縮空気系Aトレインが機能喪失 補機冷却海水系の空気作動弁が閉 補機冷却水系熱交換器2基への冷却水が喪失 補機冷却水系による各種ポンプ等の冷却機能が喪失



図5 Aトレイン交流電源故障の伝搬

と、影響がサポートシステム間で伝搬することが原因である。この影響の伝搬の様子を図5と図6に示す。

感度解析として、次の10ケースを実施した。

- (1) サポートシステム間の依存性関係を図7のように簡略化したケース
- (2) サポートシステム間の依存性をモデル化しないケース
- (3) サポートシステムの故障をモデル化しないケース
- (4) 各サポートシステムの故障を基本事象として扱うケース
- (5) 成功しているシステムの存在を反映しないケース
- (6) 高圧再循環への切替操作と格納容器スプレイ再循環の切替操作のヒューマンエラーの間に依存性を考慮するケース
- (7) 制御用圧縮空気系のタイライン開操作を考慮しないケース
- (8) 共通要因故障のデータとして Sequoyah IPE のデータを使用するケース
- (9) 共通要因故障を考慮する機器およびデータ共に Sequoyah IPE と同じくしたケース (MGL法を適用し、3重故障も考慮)
- (10) 全交流電源喪失の発生を考慮したケース

解析ケース(1)から(5)は、システム間の依存性に関する感度解析である。解析ケース(6)は、複数の系統に係るヒューマンエラーに関する感度解

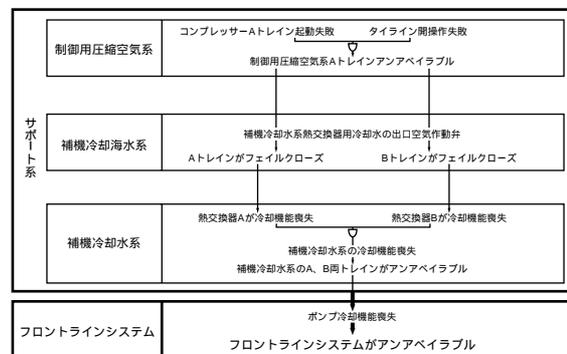


図6 計器用空気系故障の伝搬

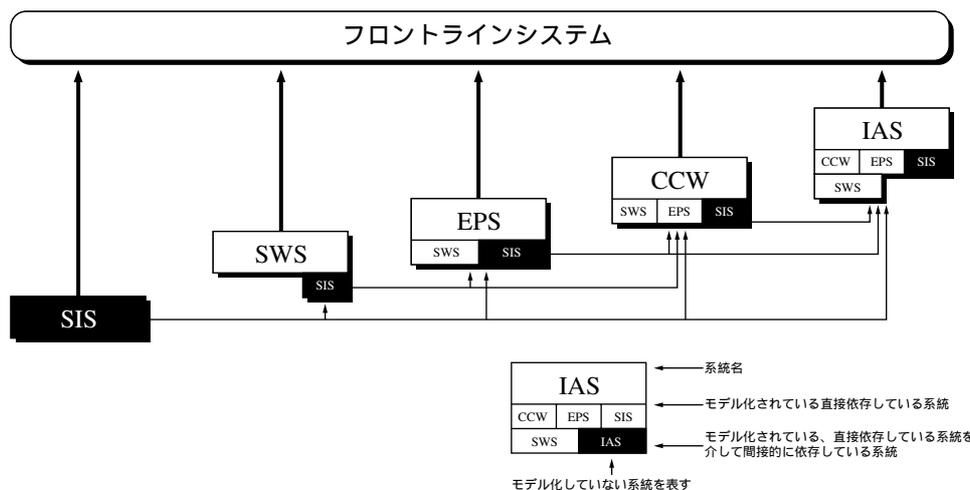


図7 簡略化されたサポート系

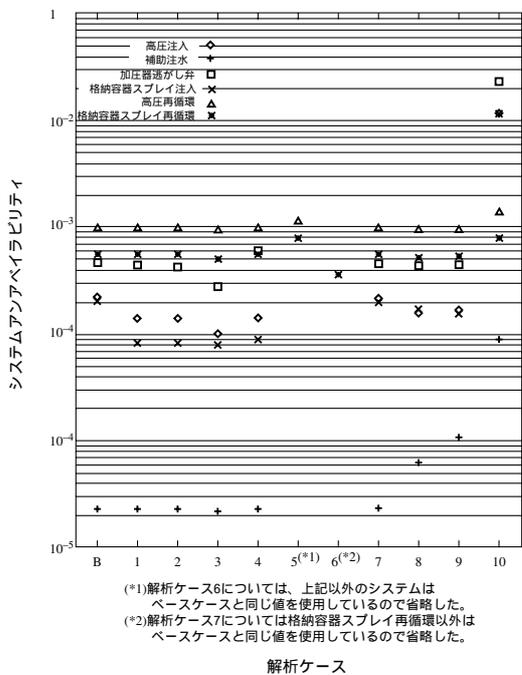


図8 シーケンス解析の結果
(フロントライン系のUnavailability)

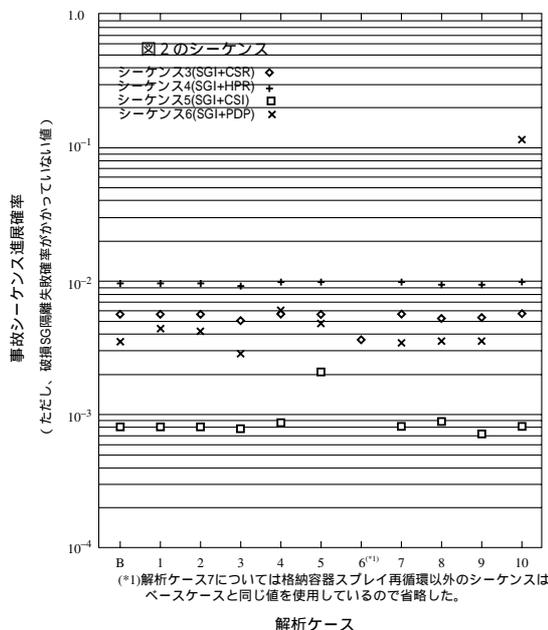


図9 シーケンス解析結果
(シーケンス毎の結果)

析，解析ケース(7)は，回復操作に関する感度解析である．解析ケース(8)と(9)は，共通要因故障に関する感度解析である．また解析ケース(10)は，モデルに関する感度解析である．解析結果を図8と図9に示す．システムによって，それぞれの影響の大きさに顕著な違いが見られる．

2.3 ベンチマーク問題Cの解析によって得られた知見

次のような知見が得られた．

知見1：成功しているシステムについては，そのことをモデル上で考慮する必要がある．モデ

ル化しない場合は、シーケンスによってはファクター2～3の過大評価となる結果を生じうる。

知見2：サポートシステムについても機器レベルでのモデル化をする必要がある。適切なモデル化をしない場合は、システムによってはファクター2～3過小評価となる結果を生じうる。

知見3：サポートシステム間の相互依存関係は、厳密に取扱うことが望ましい。簡略化したモデルを使用する時は、影響の大きいサポートシステム間の故障の伝播がモデル化されていることを確認する必要がある。厳密な取扱いをしない場合は、一般的に過小評価の結果を生ずる。但し、簡略モデルを適用した場合であっても、影響の大きい伝播経路を正確にモデル化していれば、評価結果には有為な差は生じない。

知見4：複数のシステムが関連する事故シーケンスであっても、共通要因故障とヒューマンエラーは事故の進展緩和を妨げるドミナントな要因である。従って、ベンチマーク問題AおよびBにおいて整理された知見はそのまま有効なものである。

3. PSAにおける解析結果の不確定性要因についての総合的な知見

3題のベンチマーク問題の解析を通して得られたPSA結果を報告または評価するにあたっての定性的なガイドラインを検討・整理した。3.1では、存在する不確定性を定量的に理解しやすいものとするとの観点から、PSAレポートへの記載内容を提案した。3.2では、逆に提出された解析結果を評価する側の留意点について整理した。

3.1 PSA実施結果の表示方法

PSA報告書には、様々な不確定要因に関してどのような取扱いを行っているかが明確にわかるような資料が添付されていることが重要である。特に次の要因については、解析結果への影響が大きいため、取扱いを明示する必要がある。

(1) データベース

- (a) 独立故障を考慮する機器故障モードの種類、機器故障率データ、待機除外確率、使命時間、点検周期、およびこれらのソースについて明示すること。
- (b) これらのデータを1つの表に整理する。この表には、実際に使用した数値に加えてジェネリックデータを併記することが望ましい。
- (c) 動的機器については、ジェネリックデータと一緒に図示し、これらの違いが明確に把握できるようにすることが望ましい。
- (d) プラント固有な故障データを使用している場合には、故障率の算出に使用したパラメータも明示することが望ましい。
- (e) 共通要因故障を考慮する機器故障モードの種類、システムの範囲、共通要因故障パラメータおよびそのソースについて明示すること。
- (f) これらのデータを1つの表に整理する。この表には、実際に使用した数値に加えてジェネリックデータを併記することが望ましい。
- (g) MCS中に現れる冗長な機器の同時故障の中で、共通要因故障を考慮していない機器および故障モードがあれば、その旨を明記する必要がある。できればこれに対する考察を加える。

(2) ヒューマンエラーの取扱い

- (a) 一般的にヒューマンエラーの値の不確定性が大きいことから、特に重要なヒューマンエラーについては、レビューにあたる第三者が同じ条件での解析を実施できるだけの情報を付記すること。
- (b) THERP手法を使用する場合には、本報告書の表1のような整理が望ましい。
- (c) 特に診断エラーの評価条件、行動エラーの評価におけるストレスレベル、タスク難易度、エラーの回復要素については感度が大きいので明示する必要性が高い。

- (d) MCS中に多重のヒューマンエラーの組み合わせがある場合には、それらを全て列挙すること。
- (e) ヒューマンエラー間の依存性を、エラーが発生する原因を検討の上で考慮する必要がある。原因を考慮することによって、様々な様相での依存性の存在が検討できる。
- (f) 場合によっては本研究で構築したような、ハードウェアの故障も考慮したシーケンスを展開する必要がある。
- (3) システム間のインターフェイスについてのモデル
- (a) システムモデルにおいて考慮されているシステム間の依存関係（フロントラインシステムとサポートシステム、およびサポートシステム間の）が、明確に示されていないなければならない。
- (b) 原子力プラントにおけるシステム間の依存関係は、かなり複雑である。システムによって、また設計によって、依存関係の複雑さやモデルの解析結果への影響が異なる。場合によっては単一の機器の故障が、複雑な影響経路を経て、冗長性を有しているはずのシステムや、複数のシステムの不動作を引き起こし得る。もしこのような故障があれば（MCSにより発見できる）、その影響経路について、明記する。
- (c) サポートシステムで簡略化した取扱いを行っているものがある場合には、現実の依存関係に対してどのような取扱いとなっているか、明記すべきである。
- (d) 簡略化したモデルを使用する場合は、影響の大きい故障の伝播がモデル化されていることを示す必要がある。
- (e) イベントツリーにおける成功システムの取扱いについてのモデルについて明確に示されていないなければならない。
- (f) イベントツリーにおいて成功しているフロントラインシステムが存在するという
- ことは、各サポートシステムの少なくとも1トレインは成功していることを意味している。特にサポートシステムへの依存性の影響が大きい場合には、各サポートシステムの少なくとも1トレインがアベイラブルであるという条件を反映する必要がある。
- 不確定性は、それが実際のところどこまでを考慮したものであるか曖昧なまま、不確定性幅というはっきりしない用語でもって示されることが多い。あいまいさを避けるため、特に上記の要因による不確定性について、次の観点からの考察が必要である。
- (4) 不確定性解析によって把握可能な範囲の把握
- (a) 解析結果には、通常点推定値に加えて不確定性解析結果が示されるが、この不確定性解析の範囲でカバーされる不確定性要因と、カバーできない不確定性要因を明確にすること。
- (b) モンテカルロ法を用いた通常の不確定性解析でカバーできる要因として、例えば機器故障率、待機除外確率、使命時間等がある。
- (c) 通常の不確定性解析でカバーできない要因として、例えば共通要因故障やヒューマンエラーの取扱い等がある。
- (d) カバーできると考えられる要因については、重要度の高い機器について、ジェネリックデータとの違いを明記し、ジェネリックデータを使用した際に生じる変化の方向（不確定性幅の上限の方向にずれるのか、下限の方向にずれるのか）を示す。
- (f) 機器故障率等のデータの中に相対的に特殊なものがないければ、機器故障率、共通要因故障パラメータ、待機除外確率、使命時間、および点検周期による不確定性は、通常行われる不確定性解析によって得られる上下限値の範囲でほぼカバーされると考えられる。しかし、次のような場合にはデータに対する感度が極めて大きく

なる場合があることに注意する必要がある。

- (g) 機器故障率データ間のバランスに変化があるような特殊なデータを一部の機器に使用する場合や機器故障率データと共通要因故障データのソースに違いがあり、これらの間のバランスが一般的に使用されているものと比べて著しく異なっている場合には、通常の不確定性解析ではなく、感度解析によって影響の大きさを把握する必要がある。独立故障率データと共通要因故障データとの間のバランス関係が特異な場合、共通要因故障パラメータの不確定性幅を大きくすることによって、必ずしも影響の適切な把握が可能とは限らない。

(5) 感度解析の実施

- (a) 感度解析においては、感度の大小を見るだけでなく、現実的な影響の方向（解析結果が大きい方向にずれるのか小さい方向にずれるのか）と度合い（不確定性解析の幅を超える影響を生じ得るのか否か）を把握し、特に影響の大きな不確定性要因を明確にする必要がある。
- (b) 不確定な解析条件が存在し（例えば人間信頼性解析における種々の解析条件等）、その影響が特に大きい場合は、感度解析を通して、通常の不確定性解析に使用する上下限幅を決定することも有効である。
- (c) ジェネリックデータを用いた解析結果も示され、解析結果に違いを生じる原因について考察を加えることが望ましい。比較的少数の重要度の高い機器のみで、違いが説明できる場合が多いであろう。

3.2 結果を解釈する際の留意点

レビューする側は、上記の不確定要因に対する記述が適切になされ、また資料が添付されているかどうかをチェックの上レビューする。特に次の点に留意する。

(1) 独立な機器故障率

ジェネリックデータと比べて特に大きな違いがあるもの、全体のバランスを崩すようなものがないか、もしある場合には解析結果にどのような影響をもつのか、感度解析によって影響の範囲が評価されているか確認する。

(2) 共通要因故障

(a) 一般的に使用されているデータと比べて特に大きな違いがあるものはないか、また独立な機器故障率との相対関係に大きな違いはないか。違いがある場合には、感度解析によって影響の範囲が評価されているか確認する。

(b) 解析結果に占める共通要因故障の寄与率はどの程度かを確認する必要がある。使用するデータによっては全体の5%以下の場合もあり得るし、95%以上の場合もあり得る。寄与率が極端な場合には、データのバランスの観点から正当性を検証する必要がある。

(c) MCS中に現れる冗長な機器の同時故障の中で、共通要因故障を考慮していない機器および故障モードがある場合には、そのことが明記されているか。できれば、その影響が無視し得るものか否かを検証する。

(3) 待機除外時間と使命時間

(a) 待機除外がアンアベイラビリティ要因として考慮されている機器では、一般に起動失敗確率と同等な値が適用されていることが多い。これが相対的に小さい場合には、単独のフロントラインシステムの解析結果にはファクター2～3程度の違いを生じ得る。待機除外時間のデータにより、不確定性幅の上下限のどの方向へのずれが見込めるのかを確認する必要がある。

(b) 起動後の運転失敗がアンアベイラビリティ要因として考慮されている機器では、一般に起動失敗による寄与と同等な値が

適用されていることが多い。従って使命時間の値に対する感度も比較的大きなものとなる場合が多い。運転失敗によるアンベイラビリティが相対的に小さいことにより、解析結果にはやはりファクター2～3程度の違いを生じ得る。使命時間のデータにより、不確定性幅の上下限のどの方向へのずれが見込めるのかを確認する必要がある。

(4) システム間のインターフェイスについてのモデル

- (a) システム間の依存性が、システムモデルにおいて正確に取扱われているか確認する。厳密な取扱いをしない場合は、一般的には解析結果は過小評価となる。しかし、影響の大きな故障の伝播を正確にモデル化しておけば、他の依存関係は簡略化しても、厳密なモデルの場合と同じ結果を得ることができる。簡略化したモデルが使用された場合には、影響の大きい故障の伝播がモデル化されていることを確認する必要がある。類似のプラントで既に厳密なモデル化による解析が行われており、この成果を反映して簡略化した場合には、簡略化の根拠として受容できるが、そうでなければ確認は困難である。
- (b) システム間の依存性を厳密に評価した場合には、複雑な波及経路を経て、一見現れそうにないMCSによってシステムの失敗やシーケンスの発生に至る場合がある。このような経路の存在は、厳密なモデルによる解析を実施せずには発見できないであろうことに留意する必要がある。

(5) 多重のヒューマンエラー間の従属性

- (a) 一般的にヒューマンエラーの値の不確定性の影響が大きいことに留意する必要がある。

ある。このため、重要なヒューマンエラーについては、感度解析によって影響を把握することが望ましい。

- (b) 特に、事故後の一連のシーケンスの中に運転員の多重の応答があったり、ヒューマンエラーのバックアップがあったりする場合、これらに対してどのような評価がなされているか、どのような原因によってヒューマンエラーの間の依存性が存在し得るのか等を確認する必要がある。多重のヒューマンエラーはイベントツリー上で複数のヘディングに分かれているとは限らないので、事故シーケンスのMCSにより、多重のヒューマンエラーの存在を確認する必要がある。

4. まとめ

単一の安全系の故障（ベンチマーク問題A）、人的過誤（ベンチマーク問題B）、シーケンス（ベンチマーク問題C）の感度解析から得られた知見を通じて、PSAの評価者が留意すべき事項を提案した。PSAの不確定性については、様々な定義があるが、解析者によって最も値が異なると言われるフォールトツリー解析のFTを固定することにより、見通しの良い結果が得られた。しかしながら、PSAの不確定性を論じる場合、本研究は端緒にすぎない。レベル2や外的事象の不確定性も含めて十分議論されなければならない問題である。

参考文献

- (1) 丹羽雄二 高橋英明, PWRプラントのレベル - 1 PSAベンチマーク解析 (ベンチマーク問題設定), INSS Journal No.1, 1994
- (2) 丹羽雄二 高橋英明, PWRプラントのレベル - 1 PSAベンチマーク解析 (ステップ2), INSS Journal No.2, 1995