2020 年 12 月 17 日
原子力エネルギー協議会

原子力発電所におけるデジタル安全保護回路のソフトウェア共通要因故障緩和対策に関する自律的対応の実施状況のご報告について

１．技術要件書の作成状況

- 10 月 6 日の「第 5 回発電用原子炉施設におけるデジタル安全保護系の共通要因故障対策等に関する検討チーム会合」以降，以下の観点で技術要件書の見直しを行っています。
  - 論理展開の明確化
  - 解説の追加による記載事項の充実化
- 現在，会内レビュー中（添付資料を参照）であり，技術要件書の発刊は、12 月 24 日（木）を予定（①）しております。

２．技術要件書発刊以降の予定について

- 技術要件書発刊にあわせて，各原子力事業者へ安全対策の実施を要求するとともに実施計画の作成を要求（②）しホームページへ掲載します。
- 原子力規制庁には、速やかに技術要件書を提出します。
- 各原子力事業者の安全対策の実施計画は 2020 年 3 月末を目途にホームページで公表（③）します。

※①～③は図１　対応フロー　の番号①～③に対応

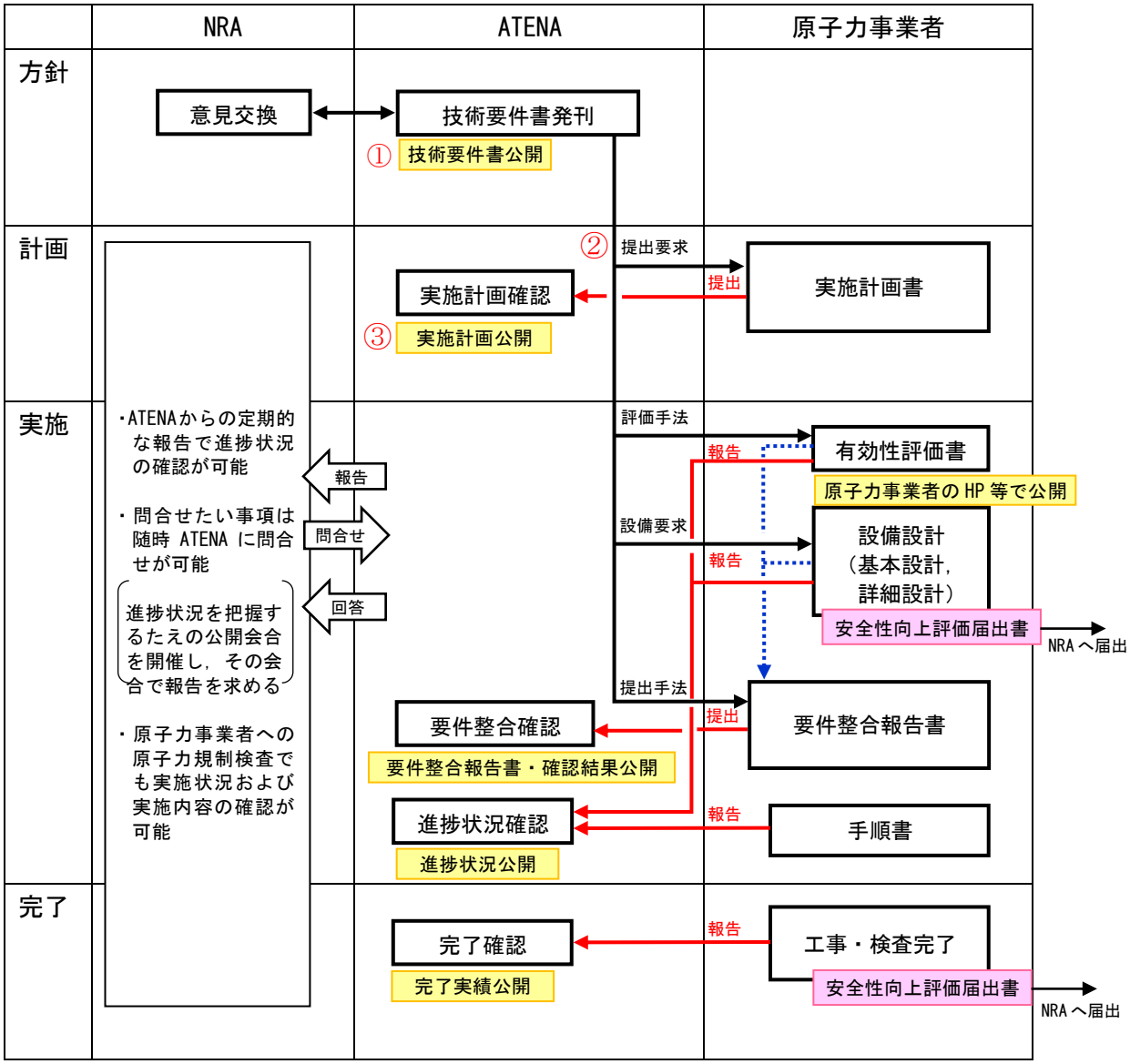

NRA
ATENA
原子力事業者
方針
意見交換
技術要件書発刊
① 技術要件書公開
計画
② 提出要求
提出
実施計画確認
③ 実施計画公開
実施計画書
実施
・ATENAからの定期的な報告で進捗状況の確認が可能
報告
・問合せたい事項は随時 ATENA に問合せが可能
問合せ
進捗状況を把握するたえの公開会合を開催し，その会合で報告を求める
回答
・原子力事業者への原子力規制検査でも実施状況および実施内容の確認が可能
評価手法
報告
有効性評価書
原子力事業者の HP 等で公開
設備要求
報告
設備設計
（基本設計，
詳細設計）
安全性向上評価届出書
NRA へ届出
提出手法
提出
要件整合確認
要件整合報告書・確認結果公開
要件整合報告書
報告
進捗状況確認
進捗状況公開
手順書
完了
報告
完了確認
完了実績公開
工事・検査完了
安全性向上評価届出書
NRA へ届出

図１　対応フロー

添付資料

ATENA 20-ME05 Rev.0

原子力発電所におけるデジタル安全保護回路のソフトウェア共通要因故障緩和対策に関する技術要件書

（案）

2020 年 12 月

原子力エネルギー協議会

【はじめに】

国内の原子力発電所においては，設備の信頼性及び保守性の向上を目的として，1980 年代頃から常用系設備にデジタル計算機を適用してきており，その良好な運転実績を踏まえ，1990 年代頃からは安全保護回路にもデジタル計算機を適用する事例が増えてきている。デジタル計算機では，設計上の要求機能がソフトウェアによって実現されることから，安全保護回路に適用するソフトウェアの信頼性を確保する取り組みとして，「実用発電用原子炉及びその附属施設の技術基準に関する規則の解釈」にて引用されている「安全保護系へのディジタル計算機の適用に関する規程」（JEAC4620-2008）及び「ディジタル安全保護系の検証及び妥当性確認に関する指針」（JEAG4609-2008）に基づき，ソフトウェアライフサイクル及び構成管理手法を含めた品質保証活動・検証及び妥当性確認を実施してきた。

これらの活動により，ソフトウェアに起因する共通要因故障（以下，「ソフトウェア CCF」という。CCF；Common Cause Failure）が発生し，多重化されたデジタル安全保護回路の機能が喪失する可能性は十分低く抑えられている。しかしながら，デジタル安全保護回路を設置した原子力発電事業者（以下，「事業者」という。）は，深層防護の観点で，より一層の信頼性向上を図るため，デジタル安全保護回路のソフトウェアを介さずに原子炉停止系統や工学的安全施設を作動できる多様化設備を自主的に設置してきた。

また，令和元年度第 33 回原子力規制委員会（2019 年 10 月 2 日開催）において，「発電用原子炉施設におけるデジタル安全保護系の共通原因故障対策等に関する検討チーム」（以下，「NRA 検討チーム」という。）が設置され，ソフトウェア CCF 対策の規制化に関する議論が進められてきており，本検討チームにおいて，原子力エネルギー協議会（以下，「ATENA」という。）は，参考書類 1～3 を提示し，原子力規制委員会及び原子力規制庁と議論をしてきている。

ATENA は，NRA 検討チームにおける議論及び国際水準を踏まえ，炉心の著しい損傷防止を重視し，運転時の異常な過渡変化又は事故（以下，「設計基準事故」という。）とソフトウェア CCF が重畳する可能性は極めて低いものの，ソフトウェア CCF 影響緩和対策として更なる対策を自主的，かつ計画的に行うことを ATENA のステアリング会議（2020 年 1 月開催）※で決定し，各事業者に対策の実施を要求した。

本技術要件書は，事業者が自主的にデジタル安全保護回路のソフトウェア CCF 影響緩和対策を行うにあたり，対策設備である多様化設備への要求事項及びその有効性評価手法を技術要件として示すことを意図して整備したものである。

各事業者は，本技術要件書に示した技術要件に従いソフトウェア CCF 影響緩和対策を自主的に整備する。また，ATENA は，事業者の取り組み状況を確認し，対策の確実な実施をフォローしていく。

さらに，ATENA は，海外動向等も参考にしながら，今後もソフトウェア CCF 影響緩和対策の技術検討を継続し，新知見が得られた場合は，本技術要件書を改定する等の必要な対応を

※ ATENA 会員の責任者クラスが委員として参加する会議体をいい，安全対策については，事業者の全会一致を必要としない方式で決定する。

行う。

本技術要件書の情報等の取扱いについては，以下のとおりとする。

（免責）

ATENA，ATENA 従業員，会員，支援組織等本技術要件書の作成に関わる関係者（以下，「ATENA 関係者」という。）は，本技術要件書の内容について，明示黙示を問わず，情報の完全性及び第三者の知的財産権の非侵害を含め，一切保証しない。ATENA 関係者は，本技術要件書の使用により本技術要件書使用者その他の第三者に生じた一切の損失，損害及び費用についてその責任を負わない。本技術要件書の使用者は，自己の責任において本技術要件書を使用するものとする。

（権利帰属）

本技術要件書の著作権その他の知的財産権（以下，「本件知的財産権」という。）は，ATENA に帰属する。本件知的財産権は，本件技術要件書の使用者に移転せず，また，ATENA の承諾がない限り，本技術要件書の使用者には本件知的財産権に関する何らの権利も付与されない。

改定履歴

改定年月	版	改定内容	備考
2020 年 12 月〇〇日	Rev. 0	新規制定	

目次

1. 序文

1.1 目的

本技術要件書の目的は，事業者が自主的にデジタル安全保護回路のソフトウェア CCF 影響緩和対策を行うにあたり，対策設備である多様化設備への要求事項及び有効性評価手法を技術要件として提示するとともに，手順書の整備及び教育・訓練の実施を要求するものである。

1.2 概要

デジタル安全保護回路のハードウェアは，4 区分の検出器，2 out of 4 回路，チャンネル間の独立性確保，運転中の試験可能性，自己診断機能による計算機の異常検知等，ハードウェアに対するランダム故障と共通要因故障に対してその安全機能に相応した十分に高い信頼性を確保してきている。

また，デジタル安全保護回路のソフトウェアについても，一度に一つのタスクのみ実行するシングルタスク処理を採用するとともに，実行中のタスクを中断する割り込み処理を行わないシンプルなソフトウェア構造の適用，可視化言語の適用により第三者による検証を容易にすること等，設計上の取り組みに加え，品質保証活動・検証及び妥当性確認により，十分に高い信頼性を確保してきており，ソフトウェア CCF の発生は十分低く抑えられている（参考書類 1 参照）。

しかしながら，特定できない不具合がソフトウェアに内在することを想定した場合に，同一のプラットフォームの使用下においては，ソフトウェア CCF が顕在化することにより，多重化されたデジタル安全保護回路が同時に故障し，安全保護機能が喪失するという可能性は否定できない。このようなソフトウェア CCF リスクに対し，各事業者は，デジタル安全保護回路を設ける場合には，ソフトウェア CCF の影響を受けない代替作動機能を有する多様化設備を自主的に設置してきた。これにより，運転時の異常な過渡変化又は設計基準事故とソフトウェア CCF が重畳した場合でも適切に事象を緩和することが可能になる。

NRA 検討チームの第 4 回公開会合（2020 年 1 月 29 日開催）において，事業者は，自主設置していた多様化設備に，安全系の自動起動及び警報を追加すること（添付書類 1 参照）により，運転時の異常な過渡変化及び設計基準事故の全事象で炉心損傷の防止が可能になるとの予備評価結果を示した（参考書類 3 参照）。

本技術要件書は，NRA 検討チームでの議論及び米国でのソフトウェア CCF 影響緩和対策要求を踏まえ，多様化設備への要求事項及びその有効性評価手法，並びに手順書の整備，教育及び訓練の実施要求について取りまとめたものである。

各事業者は，本技術要件書に示した技術要件に従い有効性評価，設備の基本設計・詳細設計を行い，ソフトウェア CCF 影響緩和対策を自主的に整備する。ATENA は事業者の取り組み状況を確認し，対策の確実な実施をフォローしていく。

本技術要件書には，技術要件に加え対策設備例及び有効性評価条件例を記載しており，

それらは各事業者の対策検討の進捗に合わせて詳細化されていくことから，本技術要件書も必要に応じて例示箇所等の更新を行うものとする。

また，ソフトウェア CCF に関する海外動向を注視し，新知見が得られた場合には本技術要件書への反映の要否を検討し，必要に応じて本技術要件書の改定を行うものとする。

1.3 適用範囲

デジタル安全保護回路のソフトウェア CCF 影響緩和対策に適用する。

1.4 用語の定義

本技術要件書における用語は次の定義による。

デジタル計算機	：コンピュータに内蔵されたソフトウェアによって制御され，人手の介入なしにデジタルデータの算術演算，論理計算等の計算を行う装置をいう。
デジタル安全保護回路	：安全保護回路とは，運転時の異常な過渡変化又は設計基準事故を検知し，これらの事象が発生した場合において，原子炉停止系統及び工学的安全施設を自動的に作動させる多重化された設備をいう。デジタル安全保護回路とは，安全保護回路のうち，ソフトウェアにより設定値比較機能，論理演算機能の全部又は一部を作動させるものをいう。
設定値比較機能	：既定の設定値と検出した信号値を比較する機能のことをいう。
論理演算機能	：設定値比較機能からの出力信号を受けて既定の論理演算を行い，原子炉停止系統や工学的安全施設の機器を作動させる，又は警報発信やランプ点灯させるための信号を出力するための論理演算を行う機能のことをいう。
ソフトウェア	：ソフトウェアとは，コンピュータを動かすプログラムのことをいう。ソフトウェアには，入出力の制御やハードウェアの管理等を担いコンピュータの基本的なコントロールを行うオペレーティングシステム（以下，「OS」という。），設計上の要求機能をコンピュータ上で実現するアプリケーション，アプリケーションを実行するためのデータベース，データ設定等がある。
ソフトウェアに起因する共通	：ソフトウェアの不具合により多重化されたデジタル

要因故障，ソフトウェア CCF（CCF；Common Cause Failure）	安全保護回路が同時に故障する状態をいう。
多様化設備	：運転時の異常な過渡変化又は設計基準事故が発生し，かつソフトウェア CCF により多重化されたデジタル安全保護回路がその安全保護機能を喪失した場合においても，安全保護回路の代替機能として，原子炉停止系統，工学的安全施設等を自動，又は手動により作動させ，設計基準事故の判断基準を概ね満足しながら事象を収束させるために必要となる設備をいう。
サポート系	：機器や系統の性能を発揮するために必要となる電源系，冷却系，空調系等の設備系統をいう。
プラットフォーム	：アプリケーションソフトウェアの実行を制御する OS やアプリケーションソフトウェア及びデータベースとのやり取りを管理するミドルウェア等をプラットフォームという。

（本頁以下余白）

2. ソフトウェア CCF について

2.1 ソフトウェア CCF 想定の範囲

ソフトウェア CCF を想定する設備の範囲は，デジタル計算機を適用した安全保護回路のうち設定値比較機能，論理演算機能とする。図 2.1－1 にソフトウェア CCF の発生を想定する範囲の例を示す。

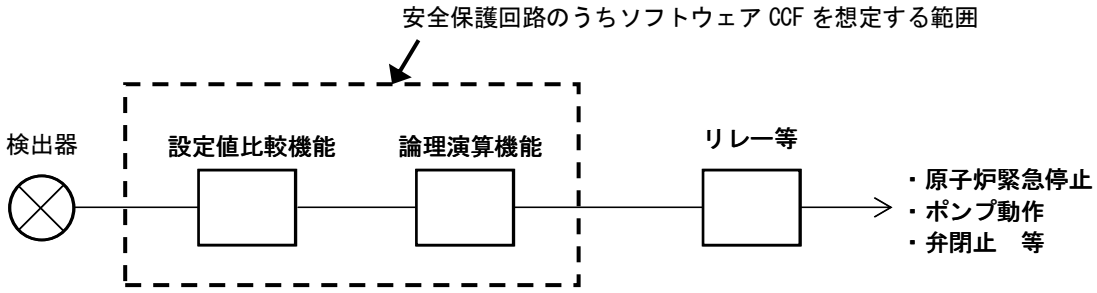


図 2.1－1　安全保護回路のうちソフトウェア CCF を想定する範囲（例）

2.2 ソフトウェア CCF 発生時の安全保護回路故障モード想定

デジタル安全保護回路のソフトウェアに不具合が潜在しているところで，運転時の異常な過渡変化又は設計基準事故が発生しデジタル安全保護回路の自動作動が要求された時に，その不具合が顕在化しソフトウェア CCF が発生することにより，原子炉停止系統，工学的安全施設等を自動起動する信号が出力されず，安全保護機能が喪失する状態を故障モードとして想定する。

なお，ソフトウェア CCF の発生により安全保護機能が喪失する場合においても，それ以前にデジタル安全保護回路の信号により起動，運転しているポンプ等の機器は，ソフトウェア CCF の影響を受けないものとして機器の作動状態の変化は想定しない。

（本頁以下余白）

3. 多様化設備要件

3.1 設置要求

デジタル安全保護回路を設ける場合には，代替作動機能を有する多様化設備を設置しなければならない。

ただし，ソフトウェア CCF が発生するおそれがない場合，若しくは運転時の異常な過渡変化又は設計基準事故が発生し，かつ安全保護回路の一部がソフトウェアにより作動するものがある場合で，当該ソフトウェアが機能しない場合を想定しても，他の安全保護機能が作動することにより設計基準事故の判断基準を概ね満足することが有効性評価により確認できる場合には，多様化設備を設けなくてもよい。

3.2 機能要求

多様化設備は，運転時の異常な過渡変化又は設計基準事故が発生し，かつソフトウェア CCF により安全機能が喪失した場合においても，設計基準事故の判断基準を概ね満足できるよう，原子炉停止系統，工学的安全施設等を自動，又は手動で作動させることができなければならい。

さらに，原子炉停止系統，工学的安全施設等を手動により作動させる場合には，運転員が必要な時間内に操作を開始し，判断基準を概ね満足した状態で事象を収束させることができるよう，運転時の異常な過渡変化及び設計基準事故の発生時に安全保護機能動作の異常の発生を認知し，必要な操作の判断を行える機能を設けなければならない。

3.3 多様化設備の範囲

多様化設備の範囲は，3.2 機能要求を達成するために必要となる，検出器，操作スイッチ，論理回路，指示計・警報等の計測制御設備とする（図 3.3－1）。

この計測制御設備の構成要素は，3.5 多様化設備への要求事項を満足する限り，デジタル安全保護回路のソフトウェア CCF 影響緩和対策として設けた設備以外の設備（安全保護回路の検出器及び操作スイッチ，重大事故等対処設備等）でも多様化設備として用いることができるものとする。

また，多様化設備の範囲は，安全保護回路のデジタル化の範囲等により異なるため，多様化設備としてどの設備を選定したか設計図書で明確にすることとする。

（本頁以下余白）

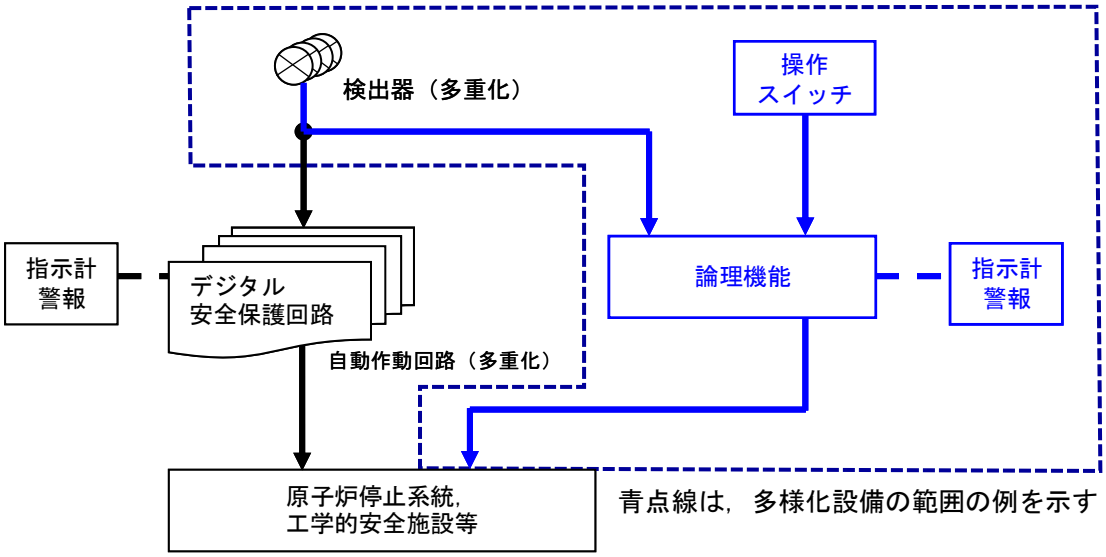


図 3.3－1　多様化設備の範囲

3.4 設計基本方針

多様化設備の設計基本方針は，設計基準事故対処設備及び重大事故等対処設備のもつ機能と異なり，ソフトウェア CCF に対応するための設備であることを踏まえ，以下のとおりとする。

デジタル安全保護回路は，十分に高い信頼度でソフトウェア設計がなされており，ソフトウェア CCF が発生する可能性は極めて小さく抑えられているため（参考書類 2），多様化設備は，運転時の異常な過渡変化又は設計基準事故が発生し，かつソフトウェア CCF により安全機能が喪失するという設計基準を超える事象に対応する設備であることから，多様化設備に対しては，設計上，単一故障を考慮しないものとする。

多様化設備は，設計上，火災・溢水あるいは外的影響（地震を除く）とソフトウェア CCF の重畳を考慮しないものとする。

多様化設備は，ソフトウェア CCF 発生時に安全保護回路の代替機能を有する設備であることから，耐環境性，耐震性，供給電源等は，安全保護回路と同等の条件で機能を発揮できる設計とする。

3.5 多様化設備への要求事項

3.5.1 多重性

多様化設備には，多重性は要求しない。

3.5.2 多様性

多様化設備自体には，多様性は要求しない。

多様化設備は，ソフトウェアを用いた安全保護回路に対して多様性を有した設備とすること。

なお，多様性を有した設備とは，アナログ設備等，ソフトウェア CCF によってデジタル安全保護回路と同時にその機能を喪失するおそれがないものをいう。

また，多様化設備に用いられるソフトウェア及びデジタル安全保護回路に用いられるソフトウェアにおいて，それらのソフトウェアに不具合が共通して内在する可能性がなく，かつその他ソフトウェア CCF が発生するおそれがないことが明らかである場合には，多様化設備にもソフトウェアを用いることができる。

3.5.3 耐環境性

多様化設備は，4. 有効性評価で対象とする運転時の異常な過渡変化又は設計基準事故とソフトウェア CCF が重畳する状態で想定される環境条件において，その機能を発揮できる設計とすること。

3.5.4 耐震性

多様化設備は，基準地震動 Ss による地震力に対し，機能維持する設計とすること。

3.5.5 供給電源

多様化設備は，外部電源が利用できない場合においても，非常用電源系又は重大事故等対処設備電源系のどちらか一方から給電できる設計とすること。

3.5.6 設備の共用

多様化設備は，二以上の発電用原子炉施設において共用しない設計とすること。また，相互に接続しない設計とすること。

3.5.7 試験可能性

多様化設備は，原子炉の運転中又は停止中に，試験又は検査ができる設計とすること。

3.5.8 安全保護回路への波及的影響防止

多様化設備は，多様化設備の故障影響により安全保護回路の安全機能が喪失しない設計とすること。

3.5.9 火災防護及び溢水防護

多様化設備が，火災・溢水の影響を受けたとしても，安全保護回路の安全機能を喪失させない設計とすること（参考書類 2)。

3.5.10 外的事象に対する防護

多様化設備は，想定される自然現象（地震を除く），人為による事象，蒸気タービン，ポンプ，その他の機器又は配管の損壊に伴う飛散物等に対して，多様化設備がそれらの

影響を受けない設計とすること又は多様化設備がそれらの影響を受けたとしても，安全保護回路の安全機能が喪失させない設計とすること。

3.5.11 操作性

多様化設備として手動操作設備が必要になる場合は，原子炉制御室に設置すること。また，原子炉制御室に設置する場合には，誤操作防止を考慮した設計とするとともに，操作結果が確実に確認できるよう配慮した設計とすること。

なお，有効性評価により，原子炉制御室以外での操作で対応可能であることが確認できた場合はこの限りではない。

3.5.12 監視性

多様化設備には，運転時の異常な過渡変化又は設計基準事故とソフトウェア CCF が重畳した事象の発生を認知できる警報，事象の判定及び対応操作の判断に必要な監視設備を原子炉制御室に設置すること。

また，多様化設備が自動で作動した場合には，その作動要因が原子炉制御室に表示される設計とすること。

（本頁以下余白）

4. 有効性評価

4.1 有効性評価の目的

有効性評価は，運転時の異常な過渡変化又は設計基準事故とソフトウェア CCF が重畳する場合に，炉心の著しい損傷を防止する上で，安全保護回路の代替機能を有する設備である多様化設備が有効であることを確認するものであり，具体的には，設計基準事故において使用される判断基準を概ね満足し，事象が収束することを解析等により確認することを目的とする。

4.2 評価すべき事象

安全保護回路を含む原子炉施設の安全設計の妥当性を確認するため，原子炉設置許可申請書では，「発電用軽水型原子炉施設の安全評価に関する審査指針」に基づき，運転時の異常な過渡変化及び設計基準事故の全事象について解析し評価を行っている。

多様化設備は，安全保護回路の代替機能を有する設備であることから，本有効性評価においても，運転時の異常な過渡変化及び設計基準事故の全事象を対象とする。

また，評価に際しては，ソフトウェア CCF が同じ影響を与える事象は，添付書類 2 に示す考え方でグルーピングをすることができる。さらに，判断基準に照らし合わせて影響の程度が軽微である事象，グルーピングしたグループ内の代表事象に包絡されることが定性的に評価できる事象，及びデジタル安全保護回路の動作を期待しない事象は解析を省略することができる。

なお，グルーピングを行う場合は，代表シナリオの包絡性（グループに含まれるシナリオの包絡性）を確認し，その妥当性を示すこと。

4.3 判断基準

有効性評価では，運転時の異常な過渡変化又は設計基準事故とソフトウェア CCF が重畳するという設計基準を超える事象に対し，ソフトウェア CCF 影響緩和対策により，炉心損傷防止が可能になることを確認することから，運転時の異常な過渡変化及び設計基準事故のいずれに対しても，判断基準は設計基準事故において使用される判断基準（「実用発電用原子炉及びその附属施設の位置，構造及び設備の基準に関する規則」（以下，「設置許可基準規則」という。）第十三条第一項第二号）を準用し，その判断基準を概ね満足することの確認を行う。

また，設備の健全性が別途確認されている原子炉格納容器の限界圧力，温度等の条件，及び炉心の著しい損傷防止が達成できることを適切に確認できる他の判断基準を用いてもよい。

4.4 解析に当たって考慮すべき事項

3.4 設計基本方針に示したとおり，運転時の異常な過渡変化又は設計基準事故とソフトウェア CCF が重畳する事象は，設計基準を超える事象であり，これらのプラント応答を

評価するにあたっては，安全設計の妥当性確認に用いる安全解析（運転時の異常な過渡変化又は設計基準事故）のような保守的評価ではなく，最も確からしいプラント応答を評価する観点から，重大事故等対処施設の有効性評価のような最適評価を基本的な考え方とする。すなわち，プラント初期条件，機器の作動状態の想定等の最適評価条件の考慮及び想定する事象を現実的に予測できる最適評価コードの使用により，運転時の異常な過渡変化又は設計基準事故に対する評価を行うことである。

ただし，ソフトウェア CCF が重畳する場合においても，保守的評価によって解析した結果が余裕をもって判断基準を満足する場合には，最適評価を行わず，保守的評価を採用してもよい。

4.4.1 解析にあたって考慮する範囲

有効性評価においては，事象発生前の状態として，通常運転範囲及び運転期間の全域を対象とすること。すなわち，サイクル期間中の炉心燃焼変化，燃料交換等による長期的な変動及び運転中に予想される運転状態を考慮すること。

解析は，想定した事象が，判断基準を概ね満足しながら，過渡状態が収束し，その後原子炉は支障なく安定状態へ移行できることが合理的に推定できる時点までを包含すること。

4.4.2 解析で想定する現実的な条件等

最適評価で想定する現実的な条件の例を以下に示す。

- 事象発生前のプラント初期条件は，設計値等に基づく現実的な値を用いる。その場合には，安全解析における解析条件との差異及び根拠を明確にすること。
- 事象発生によって生じる外乱の程度，炉心状態（出力分布，反応度係数等），機器の容量等は，設計値等に基づく現実的な値を用いる。その場合には，安全解析における解析条件との差異及び根拠を明確にすること。なお，作動設定点等については計装上の誤差は考慮しない。
- 誤操作が起因事象となる評価では，運転手順に基づく現実的な操作条件を用いる。その場合には，現実的な操作条件の根拠を明確にすること。

4.4.3 安全系機能に対する仮定

ソフトウェア CCF 発生時のデジタル安全保護回路，原子炉停止系統及び工学的安全施設を含む安全設備の作動状態については，以下を仮定すること。

- ソフトウェア CCF によりデジタル安全保護回路の機能が喪失し，原子炉停止系統及び工学的安全施設が自動作動しない。
- デジタル安全保護回路を経由しない，自動起動信号又は運転員が事象の発生を認知できる場合の手動起動信号により，原子炉停止系統及び工学的安全施設は作動可能とする（4.4.5 多様化設備に関連する条件 参照）。

・自動起動信号又は運転員の手動操作による，最も確からしいプラント応答を評価するため，安全機能を有する機器の単一故障は想定しない。

・安全機能のサポート系（電源系，冷却系，空調系等）は，起因事象との従属性がなく，かつソフトウェア CCF の影響を受けない場合は，起因事象が発生する前の作動状態を維持する。

4.4.4 常用系機能に対する仮定

常用系設備の機能は，以下を仮定すること。

・起因事象として外部電源の喪失を仮定する事象以外は，外部電源は利用可能とする。

・事象発生前から機能しており，かつ事象発生後も機能し続ける設備は，故障の仮定から除外する。

・常用系機能の喪失が起因となる事象が前提である場合は，当該事象を評価する際にはその機能を期待しない。

4.4.5 多様化設備に関連する条件

多様化設備に関連する条件を以下に示す。

(1) 機器条件

・多様化設備がもつ緩和機能の有効性を確認する観点から，多重性を要求しない多様化設備の単一故障は想定しない。

・多様化設備がもつ緩和機能の有効性を確認する観点から，多様化設備が代替作動させる原子炉停止系統，工学的安全施設等の故障及び誤動作が起因となる事象は想定しない。

・ソフトウェア CCF によりデジタル安全保護回路は，機能喪失するものの，多様化設備が代替し，利用可能である原子炉停止系統，工学的安全施設等を作動させることができるものとする。その際には，想定する起因事象及びソフトウェア CCF が発生した状態においても，原子炉停止系統，工学的安全施設等のサポート系（電源系，冷却系，空調系等）が利用可能であることを確認し，使用できない場合原子炉停止系統，工学的安全施設等は利用できないものとする。

(2) 操作条件

・運転員による手動操作をソフトウェア CCF 対策として期待することができる。ただし，有効性評価において運転員による手動操作を期待する場合には，原子炉制御室において運転員による事象の認知が可能であり，それに基づく操作手順書が整備され，運転操作訓練が適切に行われることによって，手動操作が適切に実施されることが前提となる。

・原子炉制御室での運転操作開始時間を現実的な想定としてもよい。その場合においては，運転員による事象の認知から運転操作開始までの時間を適切に考慮し，その根拠を明確にすること。

・原子炉制御室外における運転員による現場操作を考慮してよい。その場合においては，原子炉制御室における運転員による事象の認知から現場操作場所までの移動時間，及び現場操作場所に到着してから操作開始までの時間は適切に考慮し，その根拠を明確にすること。

4.4.6 解析に使用する計算プログラム及びモデル

(1) 有効性評価を行う場合は，運転時の異常な過渡変化又は設計基準事故の解析で用いる計算プログラム及びモデル又は最適評価コード及び現実的な計算モデルを使用すること。

(2) 使用する計算プログラム及びモデルは，適用範囲について，妥当性確認及び検証がなされたものであること。なお，許認可での使用実績により，計算プログラム及びモデルの確認がなされている場合には妥当性確認及び検証は不要である。

（本頁以下余白）

5. 手順書の整備と教育及び訓練の実施

5.1 手順書の整備

運転時の異常な過渡変化又は設計基準事故が発生した際に，デジタル安全保護回路の安全保護機能の喪失によって，原子炉停止系統及び工学的安全系施設が自動作動していないことを運転員が認知した場合に，その要因がソフトウェア CCF の重畳によることを判断した上で，必要な運転操作を実施し，判断基準を概ね満足した状態で事象を収束することができるための手順書を整備すること。

5.2 教育及び訓練の実施

運転員には，運転時の異常な過渡変化又は設計基準事故とソフトウェア CCF が重畳する事象に対して，整備された手順書に従い的確な対処をするために必要な力量を付与させるための教育及び訓練を，その対象・実施頻度を含め適切に計画し，実施すること。

（本頁以下余白）

6. 対策例

事業者は参考書類 3 に示す予備評価を実施しており，この結果に基づき検討した，多様化設備例を，添付書類 1 に示す。実際に採用する多様化設備は，事業者が本技術要件書に従い，有効性評価及び設備設計を行い決定するものである。

7. 参考文献

本技術要件書を作成するにあたり参考とした文献を以下に示す。

(1) NRC BTP7-19 GUIDANCE FOR EVALUATION OF DIVERSITY AND DEFENSE-IN-DEPTH IN DIGITAL COMPUTER-BASED INSTRUMENTATION AND CONTROL SYSTEMS REVIEW RESPONSIBILITIES REV7 AUGUST 2016

(2) NEI16-16 Guidance for Addressing Digital Common Cause Failure

(3) IAEA Safety Standards, Design on Instrumentation and Control Systems for Nuclear Power Plants, Specific Safety Guide No.SSG-39, IAEA APRIL 2016

(4) NUREG/CR-6303 Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems

(5) NUREG-0493 A Defense-in-Depth and Diversity Assessment of the RESAR-414 Integrated Protection System NRC MARCH 1979

(6) NRC Regulations Title 10, Code of Federal Regulations 50.55 Conditions of construction permits, early site permits, combined licenses, and manufacturing licenses. (10CFR50.55)

(7) Regulatory guide 1.152 CRITERIA FOR USE OF COMPUTERS IN SAFETY SYSTEMS OF NUCLEAR POWER PLANTS Revision2 January 2006

(8) A METHOD FOR EVALUATING DIGITAL CCF ACROSS AN INTERGRATED PLANT DESIGN, IAEA 2017

(9) Attachment Oconee Nuclear Station Defense-in-Depth and diversity Assessment for RPS/ESPS Digital Upgrade, Duke Power March 20, 2003

(10) ABWR Design Control Document Tier 2 25A5675AJ Chapter 7, Revision 6, February 2016

(11) 実用発電用原子炉及びその附属施設の位置，構造及び設備の基準に関する規則

(12) 実用発電用原子炉及びその附属施設の技術基準に関する規則

(13) 安全保護系へのディジタル計算機の適用に関する規程（JEAC4620-2008）

(14) ディジタル安全保護系の検証及び妥当性確認に関する指針（JEAG4609-2008）

(15) 安全機能を有する計測制御装置の設計指針（JEAG4611-2006）

(16) 安全機能を有する電気・機械装置の重要度分類指針（JEAG4612-2010）

（本頁以下余白）

解説

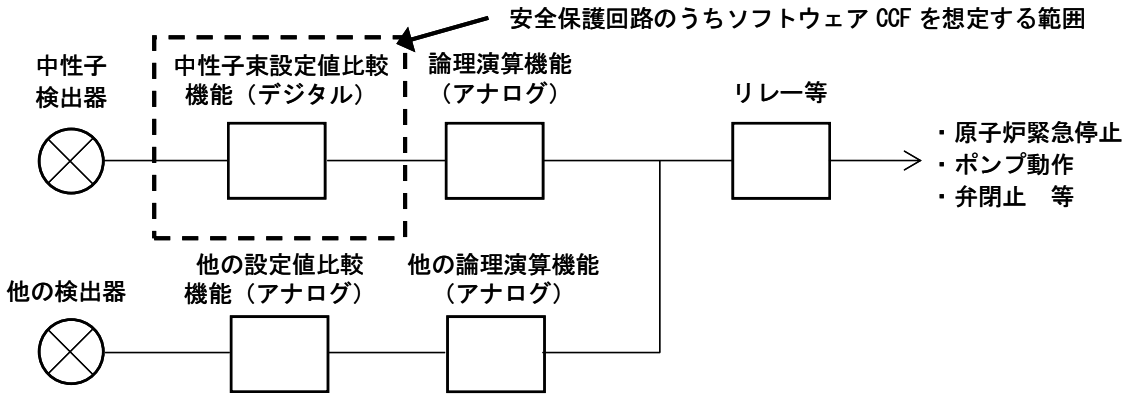
本技術要件書の適用にあたり，注意を必要とし，かつ技術要件書そのものの意義，解釈をより明確にしておく必要がある事項について，以下にその解釈を掲げることとした。

解説 2.1 ソフトウェア CCF 想定の範囲

安全保護回路の一部にデジタル計算機を適用した場合は，デジタル計算機を適用した範囲に対してソフトウェア CCF を想定するものとする。

（例－1）

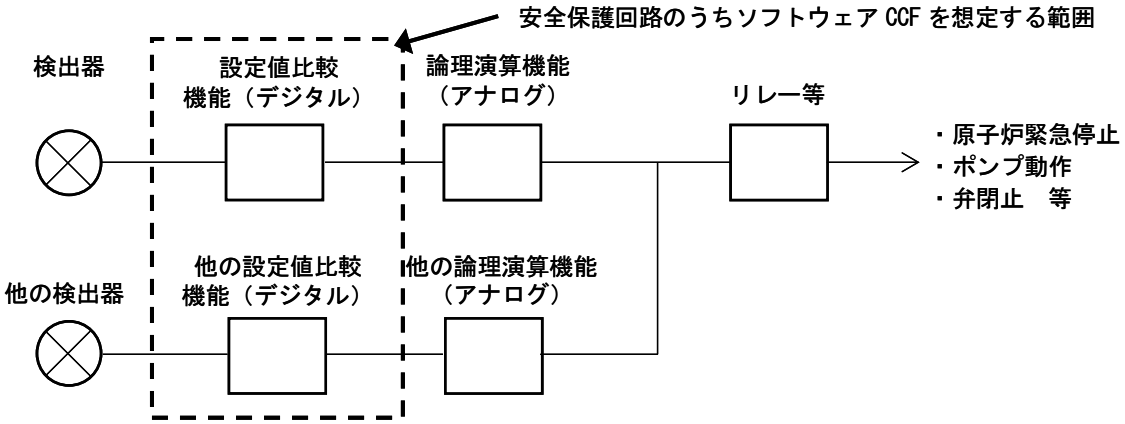
中性子計装にデジタル技術を適用した例を解説図 2.1－1 に示す。安全保護回路のうち，デジタル化された中性子束設定値比較機能に対してソフトウェア CCF の想定を行う。



解説図 2.1－1 デジタル中性子計装に対してソフトウェア CCF を想定する範囲の例

（例－2）

設定値比較機能にデジタル技術を適用した例を解説図 2.1－2 に示す。安全保護回路のうち，デジタル化された設定値比較機能に対してソフトウェア CCF の想定を行う。



解説図 2.1－2 設定値比較機能にデジタル技術を適用した場合のソフトウェア CCF を想定する範囲の例

解説 2.2 ソフトウェア CCF 発生時の安全保護回路故障モード想定

デジタル安全保護回路のソフトウェアの不具合により誤作動信号が出力される場合は，工学的安全施設の機器の作動，原子炉緊急停止等のプラント状態の変化を伴うことにより，運転員等に認知され，適切に対処可能であることから，故障モードとして想定しない。

これに対し，デジタル安全保護回路のソフトウェアの不具合が不作動側の場合は，運転時の異常な過渡変化又は設計基準事故が発生し自動作動要求があるまで，その異常を認知することが困難であり，ソフトウェア CCF 発生まで不具合の潜在が継続する可能性がある。

したがって，デジタル安全保護回路のソフトウェア CCF 影響緩和対策にあたっては，原子炉停止系統及び工学的安全施設を自動作動する信号が出力されず，安全保護機能が喪失する状態を故障モードとして想定するものである。

また，ソフトウェア CCF 発生以前にデジタル安全保護回路からの信号で起動し，その後運転を継続しているポンプ等の機器については，ソフトウェア CCF により自動作動する信号が出力されない故障モードのみ想定しているので，自動停止する信号も出力されず，ポンプ等の機器の運転状態は変化しないことから，ソフトウェア CCF による作動状態の変化は想定しない。

解説 3.1 設置要求

「ソフトウェア CCF が発生するおそれがない場合」とは，具体的には，安全保護回路がアナログで構成されている場合，あるいは安全保護回路がソフトウェアで構成されている場合で，ソフトウェア自身が多様性を有していること等によってソフトウェア CCF が発生するおそれがない場合をいう。なお，ソフトウェア自身が多様性を有しているとは，多重化されたデジタル安全保護回路内で異なるハードウェア・OS・アプリケーションで構成されたデジタル技術等を適用した場合をいう。

「運転時の異常な過渡変化又は設計基準事故が発生し，かつ安全保護回路の一部がソフトウェアにより作動するものがある場合で，当該ソフトウェアが機能しない場合を想定しても，他の安全保護機能が作動することにより設計基準事故の判断基準を概ね満足することが有効性評価により確認できる場合」とは，安全保護回路の一部がソフトウェアにより作動するものがあるプラントにおける対処方法の一つを示している。このようなプラントでは，安全保護回路にソフトウェアに依存しないアナログ回路等が存在しているため，ソフトウェアにより作動する一部回路が共通要因故障により機能しない場合において，運転時の異常な過渡変化又は設計基準事故が発生したとしても，安全保護回路の内のソフトウェアに依存しないアナログ回路等によってその事象を緩和できる場合がある。これを有効性評価により確認できる場合には多様化設備を設けなくてもよいものとする。

中性子計装にデジタル技術を適用した例を解説 2.1 ソフトウェア CCF 想定の範囲　例－1 に示したように，中性子束設定値比較機能（デジタル）以外の機能が，アナログ回路で構成されているので，ソフトウェア CCF の影響をうけることは無く，運転時の異常な過渡変化又は設計基準事故が発生した場合でも，中性子束設定値比較機能（デジタル）に係る中性子束高スクラム機能等以外の安全保護機能は正常に動作するため，有効性評価により事象を緩和できることを確認できる場合は，多様化設備を設けなくてもよい。

解説 3.2 機能要求

「設計基準事故の判断基準を概ね満足できる」とは，4.3 判断基準を参照のこと。

「必要な時間内」とは有効性評価において想定する事象が発生してから運転員による異常の発生の認知を含め多様化設備による緩和機能が作動するまでの時間的余裕をいう。（時間的余裕の考え方は，4.4.5 多様化設備に関連する条件(2)操作条件を参照のこと。）

また，時間的余裕の確保のために，緩和機能を自動的に作動させる機能を設ける場合がある。

解説 3.3 多様化設備の範囲

多様化設備は，原子炉停止系統，工学的安全施設等を作動させる機能を有する計測制御設備であり，安全保護回路のソフトウェアに対する多様性を含む要求事項を満足した複数の計測制御機能を統合したものであることから，多様化設備の範囲を設計図書で具体的に明確にしておく必要がある。

解説 3.4 設計基本方針

デジタル安全保護回路は，下記のように設計・製作段階よりソフトウェアの信頼性確保に努めることで，これまでにソフトウェア CCF を発生させることなく稼働していることから，十分に高い信頼度でソフトウェア設計がなされているといえる。

(1) ソフトウェアの信頼性確保としてのこれまでの取り組み

a. デジタル安全保護回路は，原子力施設で用いることを前提に開発・設計されており，定周期処理，シングルタスク構成，割り込み処理なしのシンプルなソフトウェア構造にするとともに，可視化言語の適用により第三者による確認，検証を容易としている。

b. デジタル安全保護回路に用いる OS は，入力処理，論理・演算処理，出力処理までの動作を定周期で制御するシンプルな機能をもつ OS を採用している。

c. OS は，デジタル安全保護回路は，JEAC4620/JEAG4609 に基づき，ソフトウェアライフサイクル及び構成管理手法を含めた品質保証活動・検証及び妥当性確認を実施している。

(2) 国内原子力施設のソフトウェア CCF 実績

NUCIA の登録情報及び国内プラントメーカーの記録を確認したところ，原子力施設に導入した，多重化されたデジタル制御装置のソフトウェア CCF 発生の記録はなく，PWR

及び BWR ともに，国内ではソフトウェア CCF はこれまで発生していない。

多様化設備は，運転時の異常な過渡変化又は設計基準事故が発生し，かつソフトウェア CCF により安全機能が喪失するという設計基準を超える事象に対応する設備であることから，安全機能を有する計測制御装置を対象とした「安全機能を有する計測制御装置の設計指針」（JEAG4611-2006）及び「安全機能を有する電気・機械装置の重要度分類指針」（JEAG4612-2010）における重要度分類には該当しない。

解説 3.5.1 多重性

多様化設備は，運転時の異常な過渡変化又は設計基準事故が発生し，かつソフトウェア CCF により安全機能が喪失するという設計基準を超える事象に対応する設備であり，単一故障は想定しないことから多重性は要求しない。

解説 3.5.2 多様性

3.5.1 多重性と同様の理由により，単一故障は想定しないことから，多様化設備そのものには多様性は要求しない。

「多様化設備に用いられるソフトウェア及びデジタル安全保護回路に用いられるソフトウェアにおいて，それらのソフトウェアに不具合が共通して内在する可能性がなく，かつその他ソフトウェア CCF が発生するおそれがないことが明らかである場合」とは，多様化設備に，例えば，デジタル安全保護回路とは異なるハードウェア・OS・アプリケーションで構成されたデジタル技術等を適用した場合をいう。なお，多様化設備に適用するデジタル技術の要件に関して，具体的な検討は今後実施していく。（参考書類 2　第 3 回検討チーム資料 2-2「多様化設備に対する主な意見」6 頁参照のこと。）

解説 3.5.4 耐震性

多様化設備は，運転時の異常な過渡変化又は設計基準事故が発生し，かつソフトウェア CCF により安全機能が喪失するという設計基準を超える事象に対応する設備であるため，耐震 S クラスは要求しない。しかしながら，ソフトウェア CCF 発生時の安全保護回路の代替機能を有する設備であるため，安全保護回路と同等の基準地震動 Ss に対して機能維持するものとする。

解説 3.5.5 供給電源

多様化設備は，運転時の異常な過渡変化又は設計基準事故とソフトウェア CCF が重畳した場合に，安全保護回路の代替機能を有する設備であるため，運転時の異常な過渡変化の一つである外部電源喪失時と同時にソフトウェア CCF が重畳した場合においても，その機能を維持する必要があることから，外部電源によらずとも非常用電源系又は重大事故等対処設備電源系どちらか一方からの受電により機能を発揮できるものとする。

解説 3.5.6 設備の共用

多様化設備は，個別の発電用原子炉施設において運転時の異常な過渡変化又は設計基準事故とソフトウェア CCF が重畳した場合に安全保護回路の代替機能を有する設備であることから，二以上の発電用原子炉施設において共用及び相互接続はしないものとする。

解説 3.5.7 試験可能性

「試験」とは，設備の特性を明確にすることをいい，「検査」とは，設備の試験等により機能・性能維持がなされていることを判断基準により合否判定することである。

多様化設備は，運転時の異常な過渡変化又は設計基準事故が発生し，かつソフトウェア CCF により安全機能が喪失するという設計基準を超える事象に対応する設備であるため，運転中の試験を必ずしも要求するものではない。

例えば，多様化設備は，原子炉の運転中において，指示計や警報表示窓の目視確認により，期待する機能が失われたことを確認した場合には，機能復旧後，動作確認ができるものとする。

また，原子炉停止中の定期事業者検査又は定期点検において，多様化設備の機能が維持されていることを確認できるものとする。

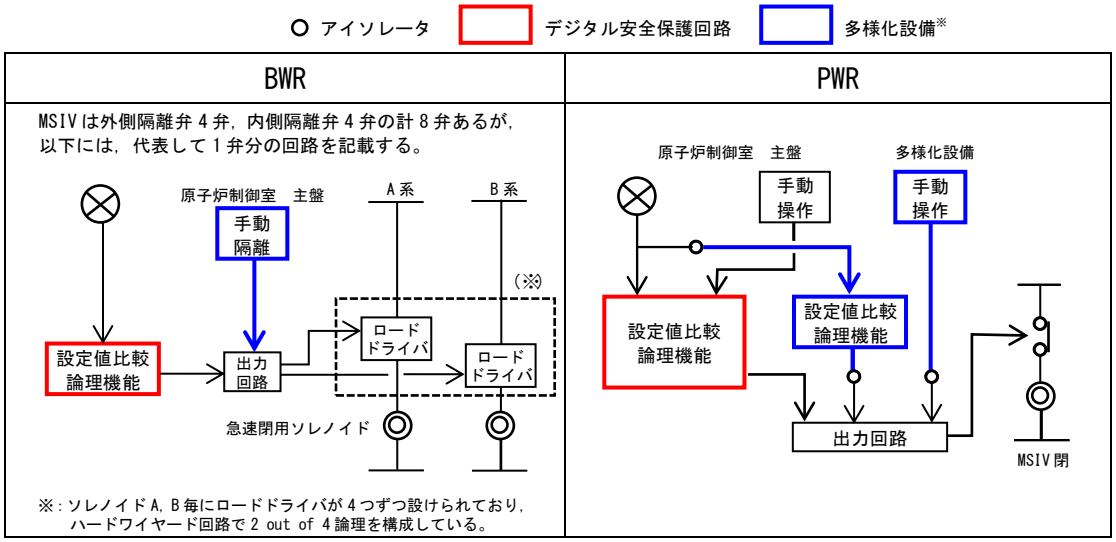
解説 3.5.8 安全保護回路への波及的影響防止

多様化設備は，ソフトウェア以外の共通要因によって安全保護機能と同時にその代替作動機能が損なわれる恐れがないよう考慮する必要があることから，アイソレータ，切替回路等による物理的方法，又は電気的な方法等により安全保護回路と互いに分離するものとする。

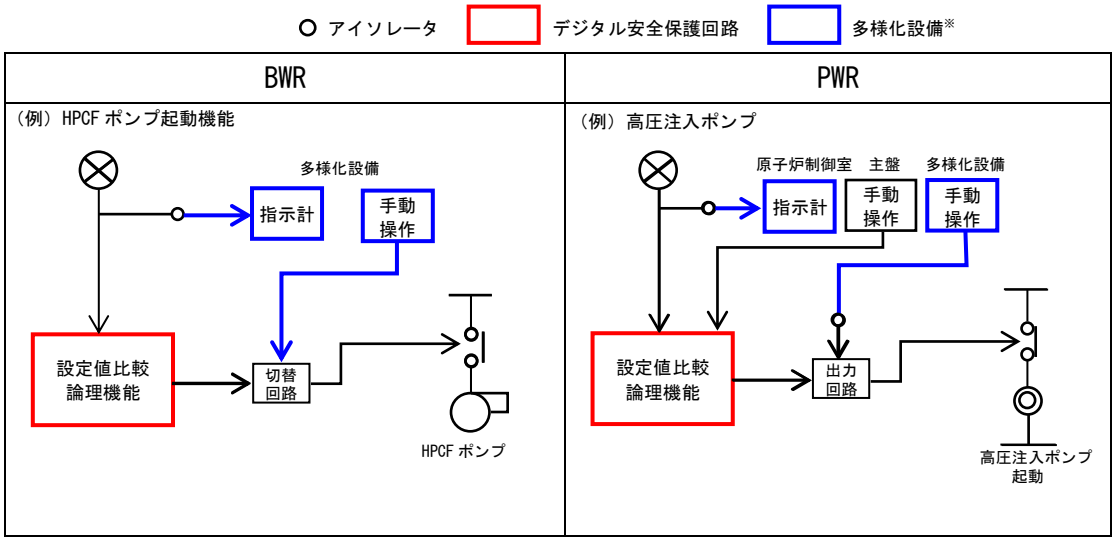
解説図 3.5.8－1～解説図 3.5.8－3 に，多様化設備の機能である MSIV 閉機能，工学的安全施設作動機能，ATWS 緩和設備機能と安全保護回路の分離例を示す。

（参考書類 2　第 3 回検討チーム　資料 2－3「令和元年 10 月 30 日発電用原子炉施設におけるデジタル安全保護系の共通要因故障対策等に関する検討チーム　第 1 回会合時のご質問回答」2 頁参照のこと。）

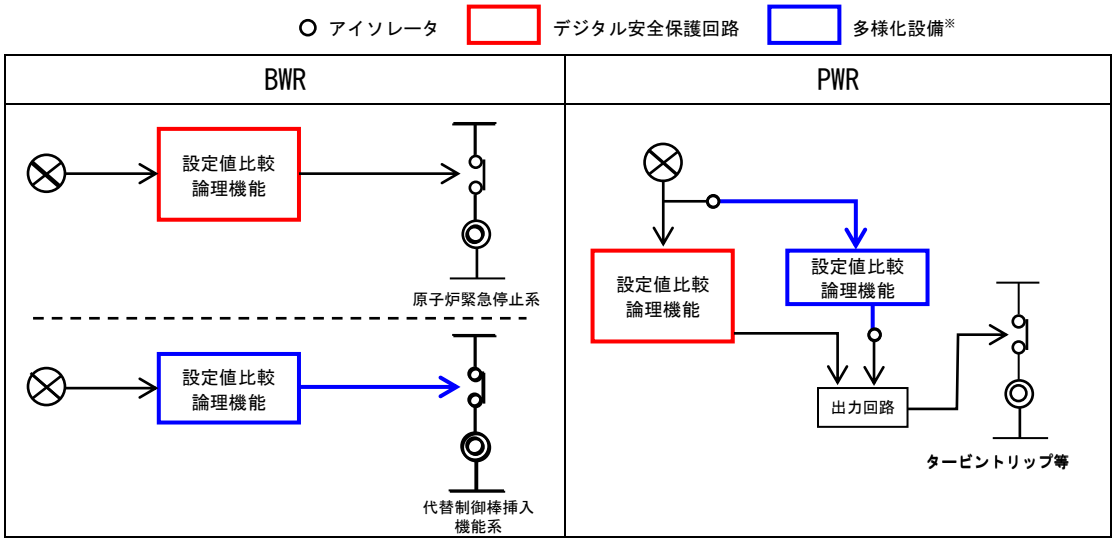
（本頁以下余白）



解説図 3.5.8－1　多様化設備と安全保護回路の分離例（MSIV 閉機能）



解説図 3.5.8－2　多様化設備と安全保護回路の分離例（工学的安全施設作動機能）



解説図 3.5.8－3　多様化設備と安全保護回路の分離例（ATWS 緩和機能）

※安全保護回路との共用部分を除く

解説 3.5.9 火災防護及び溢水防護

想定される火災・溢水に対して多様化設備と安全保護回路を分離，独立した設計とすることにより，多様化設備が機能を喪失しても安全保護回路の安全機能が同時に機能喪失させないものとする。

なお，火災・溢水による運転時の異常な過渡変化とソフトウェア CCF が重畳するリスクは十分小さいため，火災・溢水の発生に対しては，ソフトウェア CCF の重畳を考慮しない。（参考書類 2　第 3 回検討チーム資料 2-2「多様化設備に対する主な意見」2 頁参照のこと。）

解説 3.5.10 外的事象に対する防護

「想定される自然現象（地震を除く）」とは，原子力発電所の敷地の自然環境を基に，津波，洪水，風（台風），竜巻，凍結，降水，積雪，落雷，地滑り，火山の影響，生物学的事象又は森林火災等から適用されるものをいう。

「人為による事象」とは，敷地及び敷地周辺の状況をもとに選択されるものであり，飛来物（航空機落下等），ダムの崩壊，爆発，近隣工場等の火災，有毒ガス，船舶の衝突又は電磁的障害等をいう。

「蒸気タービン，ポンプ，その他の機器又は配管の損壊に伴う飛散物」とは，内部発生エネルギーの高い流体を内蔵する弁及び配管の破断，高速回転機器の破損，ガス爆発又は重量機器の落下等によって発生する飛散物をいう。なお，二次的飛散物，火災，化学反応，電気的損傷，配管の破損又は機器の故障等の二次的影響も考慮するものとする。

外的事象に対する防護対策例は，以下のとおり。

表　外的事象に対する防護対策例

事象	防護対策例
風（台風），竜巻，凍結，降水，積雪，火山の影響，生物学的事象，森林火災	外部事象に対して防護された建屋内に設置
津波，洪水，地滑り，ダムの崩壊，爆発，近隣工場等の火災，船舶の衝突	影響範囲に対して離隔を確保する等
落雷	耐雷設計
電磁的障害	耐電磁的障害設計
有毒ガス	ー（設備に対する影響モードなし）
航空機落下	ー（落下確率が十分低く考慮不要）
内部発生エネルギーの高い流体を内蔵する弁及び配管の破断	配管破損想定位置と離隔を確保する等
高速回転機器の破損	ー（回転機器側で飛散物が発生しない設計とする）

解説 3.5.11 操作性

運転時の異常な過渡変化又は設計基準事故とソフトウェア CCF が重畳した事象への対応に必要な手動操作設備及び操作結果を確認できる監視設備を多様化設備として原子炉制御室に設けるものとする。

なお，有効性評価により，対応操作までの時間余裕があり，現場での操作で対応可能であることが確認できたものはこれを許容する。

多様化設備の誤操作防止を考慮した設計例としては，例えば，多様化設備の手動操作設備は，運転員が容易に操作可能な場所に設置し，操作器具の配列，形状等の設計条件を同じ場所に設置された他の設備と同様とすることで操作が円滑に行われるよう留意すること。誤操作防止を考慮した設計とすること。なお，多様化設備に切替スイッチを設ける場合は，例えば「切替警報」，「アクセスカバー」等を設置することで，誤操作防止を実現するものとする。また，盤上に設置した指示計及び警報は，発電用原子炉施設の状態が正確かつ迅速に把握できるよう留意すること。

解説 3.5.12 監視性

多様化設備は，原子炉制御室において，運転員がソフトウェア CCF の発生を認識できる警報及び多様化設備が自動作動した場合に，作動したことが確認できる監視設備を設けるものとする。

また，解説 3.5.11 操作性と同様に，多様化設備の警報及び監視設備は，運転員が容易に確認可能な場所に設置し，警報及び監視器具の配列，形状等の設計条件を同じ場所に設置された他の設備と同様とすることで，運転員の習慣に適合した情報表示を行うものとする。

解説 4.1 有効性評価の目的

運転時の異常な過渡変化又は設計基準事故とソフトウェア CCF が重畳する事象は，設計基準を超えるものではあるが，炉心損傷の影響緩和よりも発生防止を重視することとし，有効性評価の判断基準としては「運転時の異常な過渡変化及び設計基準事故の全事象に対して炉心の著しい損傷防止」としている。炉心の著しい損傷防止を判断する具体的な基準として，最適評価の結果が設計基準事故において使用される判断基準を概ね満足することを例示している。「概ね満足する」とは，解析結果が設計基準事故の判断基準を超えた場合においても，他の判断基準により設計基準事故として満たすべき要件が満足されている場合をいう。

また，想定した事象が，判断基準を概ね満足しながら過渡状態が収束し，その後原子炉が支障なく安定状態に移行できることが，合理的に推定できる時点までを確認範囲とする。「合理的に推定できる時点」とは，例えば炉心の崩壊熱がプラントの徐熱能力を下回り，それ以降はプラントを安定状態に移行できることが推定できる時点のことである。

「解析等により確認する」とは，他の解析結果を基に合理的に類推し有効性を確認する場合も含む。

解説 4.2　評価すべき事象

有効性評価においては，運転時の異常な過渡変化及び設計基準事故の全事象を対象とし，具体的には，「発電用軽水型原子炉施設の安全評価に関する審査指針」に基づくものとする。 BWR 及び PWR における対象事象は以下のとおりである。

また，有効性評価における評価すべき事象のグルーピングの考え方を添付書類 2 に示す。

「運転時の異常な過渡変化」

1. 炉心内の反応度又は出力分布の異常な変化
   (1) 原子炉起動時における制御棒の異常な引き抜き（PWR，BWR）
   (2) 出力運転中の制御棒の異常な引き抜き（PWR，BWR）
   (3) 制御棒の落下及び不整合（PWR）
   (4) 原子炉冷却材中のほう素の異常な希釈（PWR）

2. 炉心内の熱発生又は熱除去の異常な変化
   (1) 原子炉冷却材流量の部分喪失（PWR，BWR）
   (2) 原子炉冷却材系の停止ループの誤起動（PWR，BWR）
   (3) 外部電源喪失（PWR，BWR）
   (4) 主給水流量喪失（PWR）
   (5) 蒸気負荷の異常な増加（PWR）
   (6) 2 次冷却系の異常な減圧（PWR）
   (7) 蒸気発生器への過剰給水（PWR）
   (8) 給水加熱喪失（BWR）
   (9) 原子炉冷却材流量制御系の誤動作（BWR）

3. 原子炉冷却材圧力又は原子炉冷却材保有量の異常な変化
   (1) 負荷の喪失（PWR，BWR）
   (2) 原子炉冷却材系の異常な減圧（PWR）
   (3) 出力運転中の非常用炉心冷却系の誤起動（PWR）
   (4) 主蒸気隔離弁の誤閉止（BWR）
   (5) 給水制御系の故障（BWR）
   (6) 原子炉圧力制御系の故障（BWR）
   (7) 給水流量の全喪失（BWR）

「設計基準事故」

1. 原子炉冷却材の喪失又は炉心冷却状態の著しい変化
   (1) 原子炉冷却材喪失（PWR, BWR）
   (2) 原子炉冷却材流量の喪失（PWR, BWR）
   (3) 原子炉冷却材ポンプの軸固着（PWR, BWR）
   (4) 主給水管破断（PWR）
   (5) 主蒸気管破断（PWR）

2. 反応度の異常な投入又は原子炉出力の急激な変化
   (1) 制御棒飛び出し（PWR）
   (2) 制御棒落下（BWR）

3. 環境への放射性物質の異常な放出
   (1) 放射性気体廃棄物処理施設の破損（PWR, BWR）
   (2) 主蒸気管破断（BWR）
   (3) 蒸気発生器伝熱管破損（PWR）
   (4) 燃料集合体の落下（PWR, BWR）
   (5) 原子炉冷却材喪失（PWR, BWR）
   (6) 制御棒飛び出し（PWR）
   (7) 制御棒落下（BWR）

4. 原子炉格納容器内圧力，雰囲気等の異常な変化
   (1) 原子炉冷却材喪失（PWR, BWR）
   (2) 可燃性ガスの発生（PWR, BWR）
   (3) 動荷重の発生（BWR）

解説 4.3 判断基準

設置許可基準規則第十三条第一項第二号に記載されている事項は以下のとおり。

第十三条第一項第二号：
設計基準事故時において次に掲げる要件を満たすものであること。

イ　炉心の著しい損傷が発生するおそれがないものであり，かつ炉心を十分に冷却できるものであること。

ロ　燃料材のエンタルピーが炉心及び原子炉冷却材圧力バウンダリの健全性を維持するための制限値を超えないこと。

ハ　原子炉冷却材圧力バウンダリにかかる圧力が最高使用圧力の一・二倍以下となること。

ニ　原子炉格納容器バウンダリにかかる圧力及び原子炉格納容器バウンダリにおける温度が最高使用圧力及び最高使用温度以下となること。

ホ　設計基準対象施設が工場等周辺の公衆に放射線障害を及ぼさないものであること。

このうち，イ項に係る具体的な判断基準として，「軽水型動力炉の非常用炉心冷却系の性能評価指針」に基づいて以下の基準を用いる。

(a) 燃料被覆管の温度の計算値の最高値は，1,200℃以下であること。

(b) 燃料被覆管のジルコニウム－水反応量の計算値は，酸化反応が著しくなる前の燃料被覆管厚さの 15%以下であること。

(c) 炉心で燃料被覆管及び構造材が水と反応するに伴い発生する水素の量は，原子炉格納容器の健全性確保の見地から，十分低い値であること。

(d) 燃料棒の形状の変化を考慮しても，崩壊熱の除去が長期間にわたって行われることが可能であること。

また，ロ項に係る具体的な判断基準としては，「発電用軽水型原子炉施設の反応度投入事象に関する評価指針」及び専門部会報告書「発電用軽水型原子炉施設の反応度投入事象における燃焼の進んだ燃料の取扱いについて」に基づく以下の基準を用いる。

(a) 燃料エンタルピーの最大値は 230cal/g・UO2 からペレット融点低下分相当のエンタルピーを差し引いた値を超えないこと。

(b) 浸水燃料の破裂に加えて，PCMI 破損による衝撃圧力等の発生を重畳しても原子炉停止能力及び原子炉圧力容器の健全性を損なわないこと。

解説 4.4.1 解析に当たって考慮する範囲

「通常運転範囲」とは，起動，通常運転，制御棒パターン調整等に伴う出力変更（BWR/ABWR）等のプラント運転状態を示す。

「運転期間」とは，サイクル運転中の初期から，末期までの炉心燃焼度変化の範囲を示す。

「燃料交換等による長期的な変動」とは，初装荷炉心から平衡炉心に至るまでの炉心特性の変化，新型燃料の採用に伴う移行炉心から平衡炉心までの炉心特性の変化等のことである。

有効性評価において想定する起因事象と運転時の異常な過渡変化及び設計基準事故において想定する起因事象は同一であることから，解析の対象とするプラント運転範囲，運転期間として選定する解析点は，運転時の異常な過渡変化及び設計基準事故の解析と同様となる。

また，多様化設備が原子炉停止系統，工学的安全施設等を代替作動することによって炉心損傷に至ることなく安定状態を達成するまでを解析範囲とすれば，その後は支障なく高温停止状態又は低温停止状態へ移行することが合理的に推定できるため，有効性評価

の解析範囲も，運転時の異常な過渡変化及び設計基準事故の解析範囲と同様となる。

解説 4.4.2 解析で想定する現実的な条件等

「事象発生前のプラント初期条件は，設計値等に基づく現実的な値を用いる」とは，最適評価における実設計の情報，運転実績の知見等を踏まえた，現実的な値及び操作条件の設定を意味し，重大事故等対処設備の有効性評価における解析条件と同様の考え方である。

設計値等に基づく現実的な運転条件の例を以下に示す。

通常運転時の定格原子炉熱出力，圧力，一次冷却材温度，原子炉水位（BWR/ABWR），炉心流量（BWR/ABWR），出力分布，反応度係数，崩壊熱，ヒートバランス

「事象発生によって生じる外乱の程度，炉心状態（出力分布，反応度係数等），機器の容量等は，設計値等に基づく現実的な値を用いる」とは，最適評価における実設計の情報，運転実績の知見等を踏まえた，現実的な値及び操作条件の設定を意味し，重大事故等対処設備の有効性評価における解析条件と同様の考え方である。

設計値等に基づく現実的な値の具体例を以下に示す。

・制御棒の異常な引き抜き（BWR/ABWR）
制御棒のギャング引抜本数（ABWR），連続引抜速度，現実的な炉心設計及び制御棒価値ミニマイザにより規定される制御棒引抜シーケンスを前提とした制御棒価値の想定

・制御棒落下の反応度投入事象（BWR/ABWR）
現実的な炉心設計及び制御棒価値ミニマイザにより規定される制御棒引抜シーケンスを前提とした制御棒価値の想定

・原子炉冷却材流量の喪失他（PWR）
減速材温度係数の現実的な設定，局所フィードバック効果の考慮

・線量影響評価
放射性物質の漏えい率（現実的な f 値，格納容器漏えい率等）の想定

また，現実的な操作条件の例としては，BWR/ABWR における制御棒の異常な引き抜きにおける操作が挙げられる。制御棒の異常な引き抜きは，運転員の誤操作により制御棒が連続的に引き抜かれることにより原子炉出力が上昇する事象である。ソフトウェア CCF により臨界近傍でも起動領域モニタ指示値が変動しないが，制御棒引き抜き操作は，複数人による監視が行われる手順となっており，起動領域モニタ指示値が変動しない・表示されない等の異常が見られた場合は複数人の運転員の監視によって異常を認知できる。その結果，運転員が操作ボタンから手を離し連続引き抜きを止める操作が行われることが期待される。このような操作は，通常運転中において手順に従い行われる現実的な操作条件の一つとして，解析条件に用いることができる。なお，これは運転員の制御棒操作手順の

順守による誤引抜発生防止策・監視による事象の影響緩和策であり，ソフトウェア CCF の影響緩和対策と位置付けられる。

解説 4.4.3 安全系機能に対する仮定

「安全機能のサポート系（電源系，冷却系，空調系等）は，起因事象との従属性がなく，かつソフトウェア CCF の影響を受けない場合は，起因事象が発生する前の作動状態を維持する」とは，サポート系自身が起因事象による影響を受けない場合で，事象発生以前から正常に運転しているサポート系は，ソフトウェア CCF の影響を受けない（2.2 節参照）ことから，運転状態を継続することをいう。

解説 4.4.4 常用系機能に対する仮定

「起因事象として外部電源の喪失を仮定する事象以外は，外部電源は利用可能」とは，有効性評価において，最も確からしいプラント応答を評価する観点から，常用系の機器に対して外部電源喪失等の追加の故障は想定しないことである。

「事象発生前から機能しており，かつ事象発生後も機能し続ける設備は，故障の仮定から除外」とは，ソフトウェア CCF は，デジタル安全保護回路に対して安全保護機能の喪失を想定するものであることから，常用系のデジタル制御装置に対して機能喪失等を想定しないことである。例えば，給水制御の運転継続（BWR/ABWR），制御棒駆動機構パージ水の考慮（BWR/ABWR）等がある。

「常用系機能の喪失が起因となる事象が前提である場合は，当該事象を評価する際にはその機能を期待しない」とは，起因事象及びそれに従属して，ある常用系機能が喪失する場合，当該の常用系設備が復旧し，利用可能となることは想定しないことである。例えば，起因事象及びそれに従属して外部電源が喪失する場合は，外部電源が復旧し利用可能となることを想定しない。

解説 4.4.5 多様化設備に関連する条件

「多様化設備が代替作動させる原子炉停止系統，工学的安全施設等の故障及び誤動作が起因となる事象は想定しない」とは，多様化設備の有効性を確認する観点から，多様化設備が代替作動させる系統又は機器の安全機能が喪失する起因事象を想定しないことである。例えば，ABWR においては，原子炉圧力容器に接続している種々の配管破断が想定されるが，多様化設備が代替作動させる高圧炉心注水ポンプが接続する配管の破断を起因事象として想定しないことである。

「原子炉制御室での運転操作開始時間を現実的な想定としてもよい」とは，設計基準事故の評価では，運転員が事象を認知してから操作判断をするまでの時間的余裕として少なくとも 10 分間の時間余裕（いわゆる「10 分ルール」という。）を見込むこととしているが，このルールを一律に適用する必要はなく，現実的な時間での運転操作を設定しても

よいということである。その理由は，運転時の異常な過渡変化又は設計基準事故とソフトウェア CCF が重畳する事象は，低頻度事象であり，最も確からしいプラント応答を評価する観点から，有効性評価においては，この保守的な 10 分ルールを一律に考慮する必要はないからである。

解説 4.4.6 解析に使用する計算プログラム及びモデル

評価に用いる計算プログラムは，例えば BWR/ABWR における運転時の異常な過渡変化の解析に用いる REDY コード，SCAT コード等，設計基準事故の解析に用いる SAFER コード等ではなく，ベストエスティメイトコード（想定する事象を現実的に予測できるコード）である TRAC 系コード等を使用してもよい。なお，TRAC 系コードは三次元評価解析コードであり，非断熱ドップラー効果，ボイドフィードバック効果を取り扱うことができる。

評価に用いる計算モデルは，例えば，崩壊熱モデルにおいては，設計基準事故解析で使用している保守的な GE+3σ式（無限照射）ではなく，より現実的な評価となる日本原子力学会崩壊熱推奨値，ANSI/ANS-5.1-1979 式，ORIGEN2 コードによる評価結果等を計算モデルとして使用してもよい。

解説 5.1 手順書の整備

・有効性評価で想定している現実的な操作条件を考慮する。
・デジタル安全保護回路の自動作動が要求されたときに原子炉停止系統及び工学的安全系施設が作動していないことを認知する手段を特定し，ソフトウェア CCF 事象を判断する手順を整備する。また，必要な手順書への移行の方法を明確化する。
・有効性評価で想定している現実的な時間での運転操作条件を考慮し，原子炉制御室内での運転員による手動操作並びに現場での運転員による手動操作及び現場へのアクセスルート，機器配置等について手順書に記載する。
・手順書は，過渡状態が収束し，その後原子炉が支障なく安定状態に移行し，安定状態が維持されるまでに必要な運転操作までを範囲とする。また，運転操作を行う場合の判断条件及び操作場所を記載する。
・プラント状態を監視するための計器，及びその設置場所を手順書に記載する。
・手順書の整備にあたっては，現行の手順書体系との整合性を考慮する。

解説 5.2 教育及び訓練の実施

・教育及び訓練の実施目的
運転員に対して，整備された手順書に従い，運転時の異常な過渡変化又は設計基準事故とソフトウェア CCF が重畳した場合に，原子炉停止系統及び工学的安全系施設が作動していないことを認知する手段とそれがソフトウェア CCF 事象であることの判断等について，的確に対処することができるように，有効性評価結果を活用した教育及び訓練を実施する。

・教育及び訓練の計画・実施

運転員に対して，整備された手順書の内容について習熟を図ることができるよう，教育及び訓練を計画・実施する。

・教育及び訓練の実施対象者

本要件書に示した技術要件に従い，ソフトウェア CCF 影響緩和対策を実施するプラントの運転員を対象に教育及び訓練を実施する。

添付書類 1

多様化設備例

多様化設備は，運転時の異常な過渡変化又は設計基準事故が発生し，かつソフトウェア CCF により多重化されたデジタル安全保護回路がその安全保護機能を喪失した場合においても，設計基準事故の判断基準を概ね満足できるよう，原子炉停止系統，工学的安全施設等を自動又は手動により作動させる機能及び操作，監視を行うために必要となる指示，警報機能を有するものであり，これらの例を以下に示す。

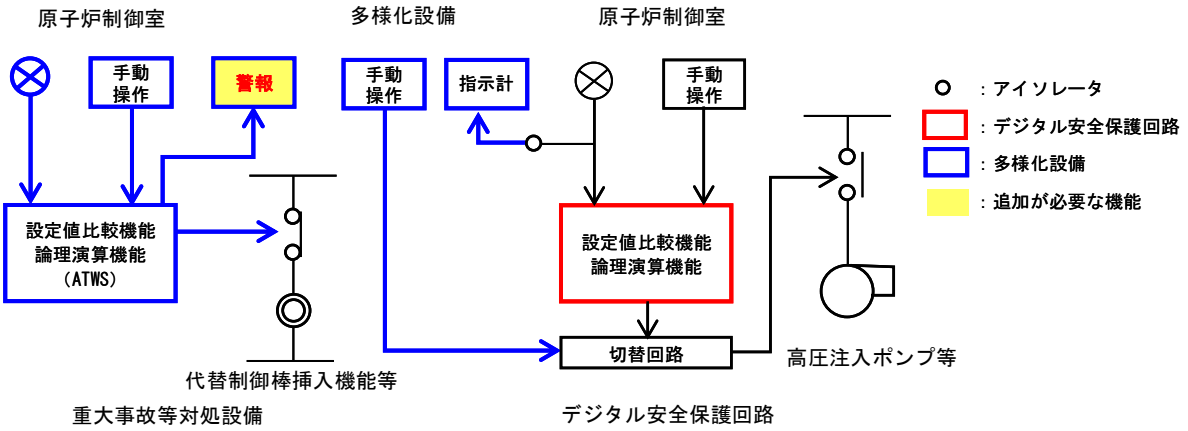
なお，これらの例は，NRA 検討チームの第 4 回公開会合（2020 年 1 月 29 日開催）において，事業者より予備評価結果に基づき示したものである。

ABWR の多様化設備の機能例を添付表 1－1 に，系統構成概略例を添付図 1－1 に示す。

添付表 1－1　多様化設備の機能例（ABWR）

	自動緩和機能	手動緩和機能	指示機能	警報機能
止める	・代替制御棒挿入（ARI）注 2 ・原子炉再循環ポンプトリップ注 2	・原子炉スクラム注 1	・原子炉水位注 3 ・原子炉圧力注 3 ・ドライウェル圧力注 3 ・高圧炉心注水系起動状態注 3 ・高圧炉心注水系系統流量注 3 ・主蒸気隔離弁の状態注 1 ・主要な隔離弁の状態注 1	・ARI 作動 ・原子炉水位低 ・原子炉圧力高
冷やす		・高圧炉心注水系起動注 3		
閉じ込める		・主蒸気隔離弁閉止注 1 ・主要な隔離弁閉止注 1		

注 1：安全保護回路
注 2：新規制基準施行後は，重大事故等対処設備として扱っている
注 3：自主対策設備
赤字：追加が必要な機能
黒字：既設のバックアップ機能



添付図 1－1　多様化設備の系統構成概略例（ABWR）

添付表 1－1 において，注 1 及び注 2 で示した機能は，安全保護回路及び重大事故等対処

設備で実現される機能であり，デジタル安全保護回路とは多様性を有した機能である。また，注 3 は，自主対策として既に設置済の機能であり，デジタル安全保護回路とは多様性を有した機能である。

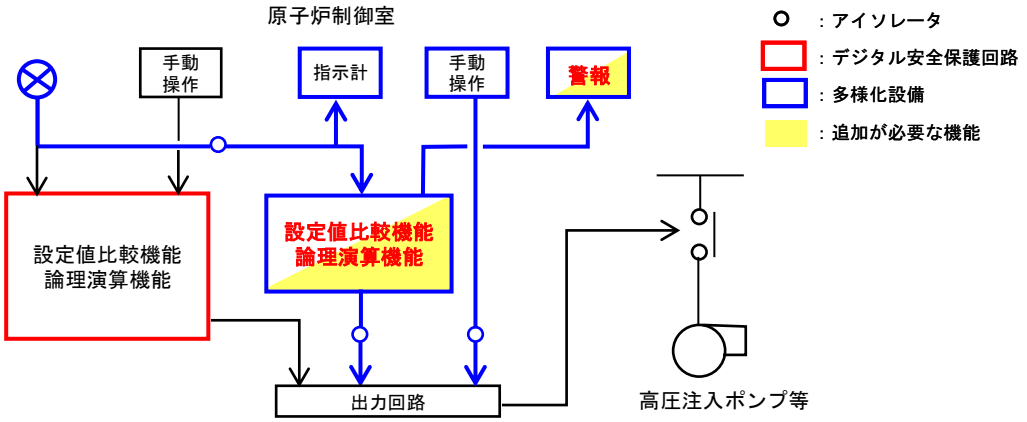
運転時の異常な過渡変化又は設計基準事故とソフトウェア CCF が重畳した事象の発生を認知できる警報として，添付表 1-1 の赤字で示す警報機能（添付図 1-1 に黄色で示す範囲）を追加する。

また，PWR の多様化設備の機能例を添付表 1-2 に，系統構成概略例を添付図 1-2 に示す。

添付表 1-2　多様化設備の機能例（PWR）

<table>
<tr><th></th><th>自動緩和機能注 1</th><th>手動緩和機能注 2</th><th>指示機能注 2</th><th>警報機能注 1</th></tr>
<tr><td>止める</td><td>・原子炉トリップ
・タービントリップ注 3</td><td>・原子炉トリップ
・タービントリップ</td><td rowspan="3">・中間領域中性子束
・加圧器圧力
・1 次冷却材圧力
・1 次冷却材低温側温度（広域）
・加圧器水位
・主蒸気ライン圧力
・蒸気発生器水位（狭域）
・格納容器圧力
・蒸気発生器 2 次側放射線
・対象補機の状態</td><td rowspan="3">・多様化設備作動
・加圧器圧力低（原子炉トリップ等）
・加圧器圧力高（原子炉トリップ等）
・蒸気発生器水位低（原子炉トリップ等）
・蒸気発生器水位異常高
・加圧器圧力異常低（高圧／低圧注入系作動）</td></tr>
<tr><td>冷やす</td><td>・補助給水起動注 3
・高圧／低圧注入系起動</td><td>・補助給水隔離／流量調節
・高圧注入系起動</td></tr>
<tr><td>閉じ込める</td><td>・主給水隔離
・主蒸気隔離注 3</td><td>・主給水隔離
・主蒸気隔離
・格納容器隔離</td></tr>
</table>

注 1：デジタル安全保護回路とは別の多様性を有した設備で実現する。
注 2：デジタル安全保護回路を経由しない，既設のハードウェア操作器や指示計等を流用する場合もある。
注 3：新規制基準施行後は，重大事故等対処設備として扱っている。
赤字：追加が必要な機能
黒字：既設のバックアップ機能



添付図 1-2　多様化設備の系統構成概略例（PWR）

運転時の異常な過渡変化及び設計基準事故の全事象に対し，ソフトウェア CCF 影響緩和

対策を講じるにあたり，大中破断 LOCA への対応として，添付表 1-2 の赤字で示す自動緩和機能と警報機能（添付図 1-2 に黄色で示す範囲）を追加する。

自動作動機能の設定値比較等は，デジタル安全保護回路とは多様性を有した設備で実現する。また，安全保護回路のデジタル化の範囲に応じて，デジタル安全保護回路を経由しない，既設のハードウェア操作器，指示計等を流用する場合もある。

（本頁以下余白）

添付書類 2

有効性評価における評価対象事象のグルーピングの考え方

＜BWR のグルーピングの例＞

「原子炉停止」,「炉心冷却」及び「放射性物質閉じ込め」の基本的安全機能別に事象のグルーピングの考え方を整理すると以下のとおりとなる。

（原子炉停止）

原子炉緊急停止系のバックアップとしての代替制御棒挿入機能（ARI）はハードワイヤードであり，原子炉圧力高信号又は原子炉水位低信号により自動作動する。したがって，運転時の異常な過渡変化又は設計基準事故の隔離事象及び非隔離事象については，いずれかの信号によりスクラムすることとなる。一方で，部分的な出力上昇であり，初期の炉心挙動が大幅に変動しない事象（制御棒の異常な引き抜き，制御棒落下）については，ARI 自動作動に期待することができない。また，制御棒の異常な引き抜き及び制御棒落下は燃料のエンタルピーを判断基準に用いているのに対し，それ以外の事象では燃料被覆管最高温度（PCT）を判断基準に用いており，着眼点が全く異なる。

したがって，評価対象とする事象は，反応度の異常な変化又は投入事象とそれ以外の事象の 2 種類に大別することができる。

反応度の異常な変化又は投入事象である，制御棒の異常な引き抜きと制御棒落下は，引き抜き速度（落下速度）及び反応度価値の違いを考慮し，これらも各々グルーピングできる。

（炉心冷却）

初期の原子炉水位低下速度と初期注水のタイミングが燃料のヒートアップに大きく影響するため，原子炉内の保有水が流出し，初期の原子炉水位低下速度が極めて早い原子炉冷却材喪失事象（LOCA）と LOCA 以外の事象では事象進展が大きく異なる。したがって，評価対象とする事象は LOCA と LOCA 以外の 2 種類に大別することができる。

（放射性物質閉じ込め）

放射性物質閉じ込め機能に係る事象は，環境への放射性物質の異常な放出と原子炉格納容器内圧力，雰囲気等の異常な変化があるが，いずれも以下のとおり定性的な評価が可能である。

－環境への放射性物質の異常な放出

燃料集合体の落下等は，それら事故の影響の拡大は限定的であり（事故発生以降の放出インベントリの増加はない），ソフトウェア CCF により放射能放出抑制機能が低下しても，それ以上の影響の拡大には至らず，概ね判断基準を満たすと判断できる場合

【放射性気体廃棄物処理施設の破損，主蒸気管破断，燃料集合体の落下，原子炉冷却材喪失，制御棒落下】

－原子炉格納容器内圧力，雰囲気等の異常な変化

原子炉格納容器内圧力，雰囲気等の異常な変化に挙げられる事象は，評価の着眼点が安全保護回路及び工学的安全施設の自動起動ではなく，事故後長期における運転員による手動起動（格納容器スプレイ手動起動，可燃性ガス処理系（FCS）手動起動等）及び当該の系統能力の確認並びに格納容器に掛かる荷重に対する耐性の確認（動荷重の発生）が主眼となる事象であり，ソフトウェア CCF による影響が小さく，概ね判断基準を満たすと判断できる場合

【原子炉冷却材喪失，可燃性ガスの発生，動荷重の発生】

第 1 回　NRA 検討チーム公開会合（2019 年 10 月 30 日開催）資料

1. 開催日　2019 年 10 月 30 日
2. ATENA が提示した会合資料は以下のとおり。

資料2

デジタル安全保護回路のソフトウェアに起因する共通要因故障対策

2019年10月30日
原子力エネルギー協議会

目 次

1．デジタル化する意味・目的

アナログ制御装置は、技術の進歩・変遷による部品の生産中止や製造者の減少による保守性の低下や拡張性の限界が課題になりつつあったことから、1980年代半ば以降、原子力分野への保守性向上を目的としてデジタル制御装置の適用を進めてきた。

【計測制御装置のデジタル化への変遷】

年　代	1970年代	1980 年代	1990年代	2000 年代～
対象設備	アナログ制御装置	⇔ デジタル制御装置	⇔ デジタル安全保護回路	
主要構成部品	トランジスタ等	IC	LSI	

部品形状の変遷

2．原子力施設に導入しているデジタル化技術

【原子力施設に導入してきたデジタル化技術】	【デジタル化の効果】	
・アナログ回路からの置換 ・自己異常診断技術、保守ツールの導入	保守性の向上	安全保護回路への適用
・多重化されたコントローラ	運転信頼性の向上	安全保護回路への適用
・監視・操作系へのVDU※の採用 ・タッチオペレーションの採用 ・光多重伝送の採用	監視操作盤、ケーブル空等の省スペース化、プラント運転の支援拡大	安全保護回路への適用
・原子力利用を前提に開発・設計 －シングルタスク処理（シンプルな構造） －定周期処理（シンプルな機能） －ソフトウェアのV&Vの実施 －可視化言語の適用	ソフトウェア信頼性向上	安全保護回路への適用

※：VDU(Visual Display Unit)の略。フラットディスプレイ及び監視用画面を指す。

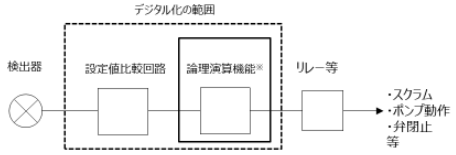
3．デジタル安全保護回路のデジタル化（1/2）

	PWR	BWR
当初からデジタル化されている原子力施設	泊3	柏崎刈羽6,7 浜岡 5 志賀 2 島根3 大間
既設設備（アナログ）をデジタル更新（計画含む）した原子力施設	高浜1,2,3,4 大飯3,4 美浜 3 伊方3 川内1,2 玄海3,4 敦賀2	－

3．デジタル安全保護回路のデジタル化（2/2）

国内原子力施設における安全保護系のうち、デジタル化の範囲は、設定値比較回路や論理演算機能の部分である。

自動作動系におけるデジタル化の範囲（例）



※：工認ガイドにおける安全保護回路の範囲

4．ソフトウェア信頼性向上に対する取組（1/2）

6

■ソフトウェアの信頼性確保としてのこれまでの取組み
・デジタル安全保護回路は，原子力施設で用いることを前提に開発・設計されており、定周期処理，シングルタスク構成，割り込み処理なしのシンプルなソフトウェア構造にするとともに，可視化言語の適用により第三者による確認，検証を容易としている。

・OSは入力処理、論理・演算処理、出力処理までの動作を定周期で制御するシンプルな機能を有する。

ソフトウェア構造（例）

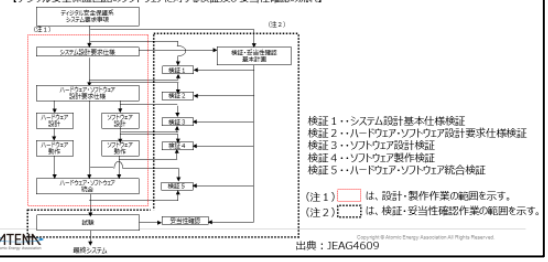
4．ソフトウェア信頼性向上に対する取組（2/2）

7

■ソフトウェアの信頼性確保としてのこれまでの取組み
・デジタル安全保護回路は，JEAC4620／JEAG4609に基づき、ソフトウェアライフサイクル及び構成管理手法を含めた品質保証活動・検証及び妥当性確認（V&V）を実施している。

■これまで原子力施設に導入したソフトウェア起因の共通要因故障※実績
PWR/BWRともに、ソフトウェアに起因する共通要因故障（以下、「CCFという）はこれまで発生していない
※：ソフトウェアによって機能する電子計算機の不作動又は誤動作による、多重化された制御装置の同時機能喪失

【デジタル安全保護回路のソフトウェアに対する検証及び妥当性確認の流れ】

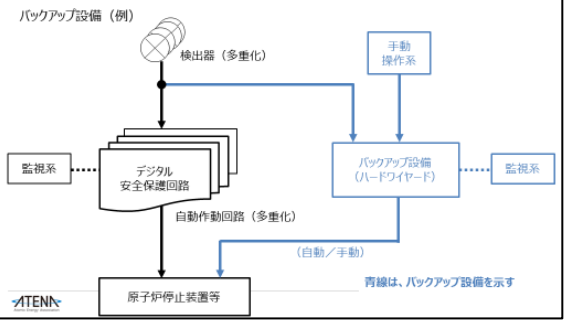


出典：JEAG4609

5．デジタル安全保護回路ソフトウェアCCFへの取り組み（1/2）

8

デジタル安全保護回路に搭載するソフトウェアは、設計・製造段階より信頼性を確保しているが、**より一層の信頼性向上を目的として、自主的にバックアップ設備を設けてきた。**



5．デジタル安全保護回路ソフトウェアCCFへの取り組み（2/2）

9

■バックアップ設備（例）

	自動作動系	操作系（手動）	監視系
ABWR	・原子炉スクラム※ ・原子炉再循環ポンプトリップ※	・原子炉スクラム ・主蒸気隔離弁閉止 ・主要な隔離弁閉止 ・高圧炉心注水系起動	・原子炉水位 ・ドライウェル圧力 ・主蒸気隔離弁の状態 ・主要な隔離弁の状態（原子炉冷却材浄化系，原子炉隔離時冷却系の内側隔離弁） ・高圧炉心注水系起動状態 ・高圧炉心注水系系統流量

	自動作動系	操作系（手動）	監視系
PWR	・原子炉トリップ ・タービントリップ※ ・主給水隔離 ・補助給水起動※	・原子炉トリップ ・タービントリップ ・主給水隔離 ・補助給水隔離／流量調節 ・高圧注入系起動 ・格納容器隔離	・中間領域中性子束 ・加圧器圧力 ・１次冷却材圧力 ・１次冷却材低温側温度（広域） ・加圧器水位 ・主蒸気ライン圧力 ・蒸気発生器水位（狭域） ・格納容器圧力 ・蒸気発生器２次側放射線 ・対象補機の状態

※は、新規制基準施行後は、重大事故等対処設備として扱っている。

6．現状バックアップ設備の設計の考え方、スペック

10

■バックアップ設備の設計（新規制基準適用後の現状仕様）

		ABWR	PWR
バックアップ設備（操作系（手動）、監視系）	安全重要度	常用系並みの設計	常用系並みの設計
	耐震性	Cクラス 但し、実力としては以下の通り 操作系：Ss機能維持 監視系：Ss機能維持（ドライウェル圧力、原子炉水位 以外）	Cクラス 但し、操作系はSs地震動による誤動作防止
	多重性	なし	なし
	耐環境性	事故時条件下で機能維持	事故時条件下で機能維持
	操作監視場所	中央制御室	中央制御室他
バックアップ設備（自動作動系）	安全重要度	重大事故等対処設備	重大事故等対処設備
	耐震性	Ｓｓ機能維持	Ｓｓ機能維持
	多重性	作動回路への信号（原子炉圧力、原子炉水位）を多重化	回路二重化（単一の回路の故障による誤動作防止）
	耐環境性	事故時条件下で機能維持	事故時条件下で機能維持
	設置場所	中央制御室	中央制御室他

7．デジタル安全保護回路でCCFが発生した場合の現状の対処

11

- デジタル安全保護回路で異常が発生し、装置の故障を示す警報が中央制御室に発報された場合には、警報の内容及び装置の状態を確認し、社内規定類に基づき必要な措置を実施するとともに、保安規定の運転上の制限に定める所要系統数を満足していないと判断した場合は、保安規定に定める措置を実施する。

- CCF対策も含めて、デジタル安全保護回路が全て作動不能となった場合には、バックアップ設備による原子炉トリップ、隔離弁閉止、高圧注入等を行う対応が可能である。

8．安全保護回路デジタル化の今後の見通し

12

【ABWR】
・安全保護回路はデジタル化されている。

【BWR5】
・安全保護回路はデジタル化されていない。
・現段階で安全保護回路のデジタル化の計画はない。

【PWR】
・安全保護回路のデジタル化を進めている。

9．PLD等新たなデジタル機器・技術の実機適用の計画について

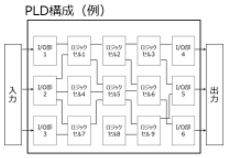
13

・FPGA ※1 等のPLD ※2は、マイクロプロセッサや通信コントローラ等のインターフェース回路において、信号変換装置の一部デバイスとして既に適用されている。（部品として扱っている）

・事業者として現状、デジタル安全保護回路をPLD等の新たな技術で実現する計画は無い。

・PLDはマイクロプロセッサとは異なる構造であるため、バックアップ設備に適用してマイクロプロセッサとの多様性を確保することができると考える。

PLD構成（例）



※１：FPGA：Field-Programmable Gate Array
PLDの一種

※２：PLD： Programmable Logic Device
マイクロプロセッサとは異なり、OS等のソフトウエアで動作するのではなく、I/O部、ロジックセル（論理・演算回路）の組み合わせや配線のデータを予め書き込むことにより、目的に応じた機能を実現することができる特徴がある。

・I/O部：外部との信号のやりとりを行う素子
・ロジックセル（論理・演算回路）：ANDやORのロジック回路

１０．基本方針（バックアップ設備義務化）に対する見解、検討にあたっての要望

14

１．これまで事業者が自主的に備えてきたCCF対策の規制化にあたっては、効果的に安全性を高める観点から、以下のような点について考慮が必要と考えている。

・CCF対策に関する規準は、デジタル技術の進展を踏まえ将来的にバックアップ設備をデジタル化する可能性や、アナログをはじめとした従来技術の衰退の可能性も踏まえ、実施方法の詳細（仕様規定）でなく、要求性能水準の規定（性能規定）を前提に検討が進められること

・性能については、これまでデジタル安全保護回路のソフトウェアが備えてきた高い信頼性や、設計想定事故を超える事象への対応としてATWS対策を重大事故等対処設備として備えてきた状況を踏まえ、安全上の重要度（例えば、CCFを含め、バックアップ機能を期待する想定起因事象の発生頻度等）を考慮した検討が進められること

・設備追加等の対策が必要な場合は、適切な経過措置期間が設けられること

２．原子力産業界としても、効果的に安全性を高めるために必要な、ソフトウェアCCF対策の性能及び当該性能を満たすための仕様について検討を進めるので、今後の会合を通じて意見交換を進めたい。

ATENA

第 3 回　NRA 検討チーム公開会合（2019 年 12 月 4 日開催）資料

1. 開催日　2019 年 12 月 4 日
2. ATENA が提示した会合資料は以下のとおり。

（資料 2-1）

資料２－１

デジタル安全保護回路のソフトウェアに起因する共通要因故障への対応の考え方について

2019年12月4日
原子力エネルギー協議会

1

はじめに

- 安全保護回路は、設計基準事象に対する原子炉の安全機能を確保するために重要な設備であり、この信頼性を高め、原子炉の安全確保を確実にすることは、ATENAとしても重要と考えている。
- 本資料では、安全保護回路の信頼性向上の取り組み、並びに、本検討会合の課題であるデジタル安全保護回路のソフトウェアCCFのリスクに関するATENAとしての考え方を述べる。

2

1．デジタル安全保護回路の信頼性向上の取り組み

3

デジタル化の意義

- 原子力産業界は、これまで、アナログ方式による安全保護回路に対し、信頼性向上や保守性の向上の目的でデジタル化を進めてきた。

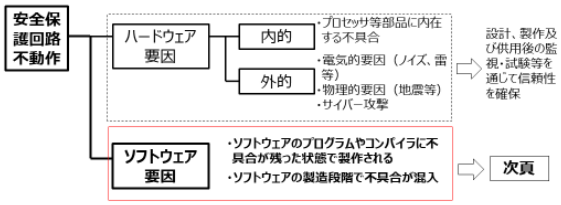
		アナログ装置	デジタル装置
安全保護回路		 【特徴】部品数多い、消費電力大（劣化影響）	デジタル化 ⇒  【特徴】部品数少ない（マイクロプロセッサ使用）
信頼性	論理演算方式	（例）1 out of 2 twice	2 out of 4
信頼性	ハードウェア故障＊（アンアベイラビリティ）	10^{-4}/demand 程度	10^{-6}/demand 程度
保守性	経年変化	あり	ソフトは経年変化なし

＊：トピカルレポート「ディジタル安全保護系設備の基本仕様と設計プロセス」（HLR-113）のスクラム失敗確率より引用

4

ソフトウェア故障に対する信頼性向上対策（1/2）

- デジタル化に伴い、ハードウェアの信頼性は向上する。
- 一方、デジタル安全保護回路は、アナログ回路と異なり、ハードだけでなくソフトウェアに起因する故障（不具合）が内在する可能性あり。このため、デジタル安全保護回路は、ハードだけでなく、ソフトウェアの故障の防止の取り組みを行うことで、安全保護回路全体の信頼性を確保してきている。



5

ソフトウェア故障に対する信頼性向上対策（2/2）

- ソフトウェアに起因する故障への対応として、故障発生要因を踏まえ、設計開発段階より、以下のような対策を講じている。

設計開発	ソフトウェアの不具合を作り込ませないための対策	・ソフトウェアの構造の単純化 ・視認性の向上（プログラム言語） ・コーディング作業の人の介在の不要化 ・FMEA評価に基づき自己診断機能の設計 ・各段階で、第三者による図書ベースの確認（検証）＊
製造・検証	ソフトウェアの不具合が作り込まれてないことを確認する対策	・各段階で、第三者による図書ベースの確認（検証）及び設計の妥当性確認（V&Vの実施）＊
運転・保守	定期的な確認	・定期検査時、マスターROMによるコンペアチェックを実施 ・安全保護系機能試験・設定値確認試験の実施 ・自己診断機能の実施、ソフト・ハードの健全性確認

＊：設置許可基準規則24条6項の要求への対応として実施

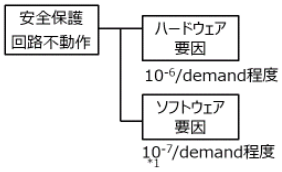
6

2．ソフトウェアCCFリスクの考え方

7

デジタル安全保護回路の信頼性について

- 安全保護回路内では、供用中、10msec～200msec程度の周期でデマンドが発生しているが、ソフトウェアCCFに起因する故障は、これまでのデジタル安全保護回路の稼働期間中で一度も発生していない。
- ソフトウェアに起因する故障は、以下のとおり、10^{-7}/demandオーダー程度の水準にまで低減されている。このため、**ソフトウェアCCFが発生する可能性は極めて小さく、ソフトウェアCCFは、プラント設計基準として想定するよりも、設計上の残存リスクとして捉えることが適切と考える。**

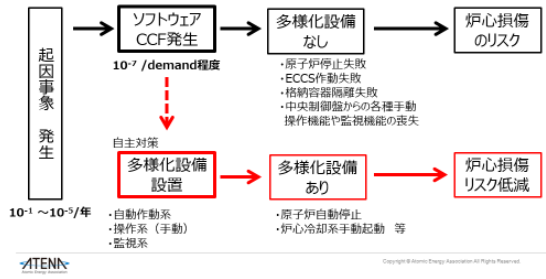


＊1：EPRIレポート（1016731）における米国の20年間の安全系デジタル故障の要因分析結果（総故障の2%がソフトウェア要因故障）を踏まえ、保守側に、総故障の1割をソフトウェア要因故障と設定。

8

ソフトウェアCCFへの備え

- ソフトウェアCCFが発生した場合に想定される安全機能への影響を踏まえ、これまでの国内プラントにおけるデジタル安全保護回路の設置にあたり、ソフトウェアCCFに対する自主的な緩和対策として、多様化設備を備えてきた。



9

ソフトウェアCCFに対する多様化設備の有効性

- 過渡事象又は事故とソフトウェアCCFが同時に発生した場合、安全保護回路が機能喪失した状態で過渡事象又は事故に対応する必要がある。このような状況下で、自主対策で設置している多様化設備で対応を実施した場合、下表のような結果となる。
- 大中破断LOCAに関しては、決定論的評価の観点からは課題があるものの、起因事象発生頻度（10^{-5}/年程度）及びソフトウェアCCFの発生確率（10^{-7}/demand）との重畳であることを踏まえると、残存リスクは十分小さいと言える。

事象		BWR	PWR
制御棒系	過渡	手順上制御棒操作はノッチ操作であり、評価想定の連続引き抜きは実施しない	原子炉停止：自動停止により対応可能。炉心冷却：補助給水系の自動作動により対応可能。
	事故(RIA)	制御棒引き抜け時にはラッチ機構があるなど、制御棒落下のシナリオが現実的には想定し得ない	
過渡（制御棒系以外）		原子炉停止：自動停止により対応可能。炉心冷却：炉心損傷までの時間余裕あり。HPCFの手動操作により対応可能。	
事故（LOCA以外）			
事故（LOCA）	小	原子炉停止：自動停止により対応可能。炉心冷却：過渡と同様、手動操作により対応可能。ただし、過渡と比べて時間余裕が小。	原子炉停止：自動停止により対応可能。炉心冷却：高圧注入系の手動操作により対応可能。
	中	同上	炉心冷却：手動操作による対応不可。
	大破断	炉心冷却：小中破断LOCAと同様、手動操作により対応。ただし、小中破断LOCAと比べて更に時間余裕小。	

10

ソフトウェアCCF対策（残存リスクに対する考え方）

- ソフトウェアCCFの残存リスクに対する対応の考え方については、以下のとおり。
  - ◎状態１⇒２（ソフトウェアCCFの発生）の防止のため、デジタル安全保護回路に係る信頼性確保対策を実施する。
  - ◎状態３に至るような残存リスクをゼロにすることはできないため、当該リスクレベルが適正水準になるよう、状態３⇒４に係る緩和戦略も考慮の上、状態１～３全体で効果的な対策を検討する。

11

3．デジタル装置規制に関する海外の動向

12

デジタル装置規制に関する海外の動向

- 米国規制は、ソフトウェアCCFに対する評価に関する審査方針を定めている。また、これまでの供用実績等を踏まえ、ソフトウェアの信頼性や安全上の重要性にフォーカスした審査方針とするよう近代化を図っている段階にある。

【（参考）米国のデジタル規制経緯】
- 1979年　Westinghouse社の安全保護回路にCCFの懸念があるため、多様性評価（D3評価）を行うことを、審査方針として規定。
- 1990年代　第三世代炉でデジタル装置を導入する動向にあることを踏まえ、DC審査の方針として、デジタル装置のソフトウェアCCFの発生防止及び万一の発生に備えた多様化対策を求める方針を定めるとともに、既設プラントにも展開。
- 2000年代　オコニー発電所のデジタル化審査。この審査経験等を踏まえ、審査方針に、最適評価の概念（単一故障を想定しない、非安全系のクレジットを可とする等）が追加。
- 2016年～　規制の近代化対応として、以下の観点から審査方針の見直しを検討中。
  - ソフトウェアの信頼性を元に、CCFの考慮を排除することを可とするプロセスの導入
  - 安全上の重要性の考慮（グレーデッドアプローチ）
  - 多様化設備に代わる措置の扱い（例：運転監視(LBB)を前提とした大破断LOCA向け設備対策の除外　）

- 米国以外を見ると、多様化設備を考慮する必要がある対象起因事象については、炉心損傷頻度への寄与度を踏まえ、大破断LOCAを除外する等の絞込みを行っている国（英国他）が見られる。

13

米国のデジタルI&C規制に関する議論状況（11/22 ACRSの状況）

◎米国規制諮問会議（ACRS：Advisory Committee on Reactor Safeguards)の結果

日時　11/21（木）10時～14時頃　　出席者：　ACRS、NRR、NEI、EPRI

内　容　以下のとおり、規制当局及び産業界がプレゼン。**特に、ソフトウェアの信頼性や、ソフトウェア故障＝「CCF」とならないようにするためのポイントについて議論が行われた。**

- NRC：デジタルI&Cに関する標準審査計画（SRP）であるBTP7-19の改訂ドラフトを紹介（主な改訂ポイントは以下のとおり）。また、今後、2020年第三四半期に最終改訂版を発行することを目指し、BTPの見直しを進め、パブコメやACRSの付議を行っていくことを説明。
  - ○ グレーデッドアプローチの導入（I&Cの重要度を踏まえ、ソフトウェア信頼性の確認方法を分類。深層防護評価までを行うのは、安全上重要なカテゴリーのみ。）
  - ○ CCFの考慮を除外可とするプロセスの追加（設計の属性（多様性）の違いを考慮　等）
- NEI：**適切なCCF対策を行えば、必ずしも多様化設備を設置する必要はないことについて議論することが重要**であり、**具体的には、以下のアイテムが重要との意見を提示。**
  - ○ ソフトウェア品質確保プロセス（設計等）、同時故障を誘発するトリガー、運転経験
  - ○ ソフトウェア設計（設計要求、属性、設計プロセスの品質保証等）
  - ○ 産業界のベストプラクティスの活用
- EPRI：過去のデジタルI&Cに関する研究成果（デジタルI&C故障の要因分析結果、信頼性向上活動の効果、リスクインサイトの活用可能性等）を説明。

14

４．今後の議論の進め方

15

今後の公開会合における議論の進め方について

- 今回、現状のデジタル安全保護回路が有するソフトウェアの信頼性の水準を示した。
- また、ソフトウェアCCFが発生した場合のプラント安全への影響や多様化設備の有効性について、今回は概略評価を示したが、別途安全解析を実施の上、詳細な評価結果を示す。
- 今後、これらの評価結果や、規制化に伴う以下のような影響も踏まえ、深層防護全体でバランスが取れた効果的な安全対策を検討することが重要と考えている。
  - ○ デジタル安全保護回路から多様化設備への配線等分岐に伴う回路全体の更なる複雑化の影響（追加的に考慮すべきリスクを生み出す虞）
  - ○ デジタル安全保護回路未導入プラントのデジタル化判断への影響

【今後の議論の進め方（提案）】

- ATENAとしては、上記のとおり、現状のデジタル安全保護回路の信頼性も踏まえ、深層防護全体で見て、デジタル安全保護回路に対しどのような対策を講じることが安全の観点から効果的か考え方を整理するので、次回以降の会合にて議論したい。

16

参考資料

デジタル安全保護回路の ソフトウェア信頼性向上施策について

17

１．ソフトウェア信頼性向上施策

18

用語の定義

・安全保護回路：
安全保護系 を構成する装置のうち、安全保護回路（論理演算機能（作動（起動）回路））及び設定値比較回路とする

・ソフトウェアCCF：
安全保護回路に実装されているソフトウェアの不具合によって、多重化された安全保護回路の機能が喪失する事象

19

ソフトウェア信頼性向上施策

３つの施策によりソフトウェアの設計・製作・運用の高信頼度を担保

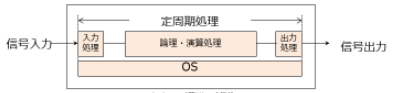
（１）高信頼設計・製作

（２）自己診断による異常検出

（３）工場試験・定期的な試験・保守

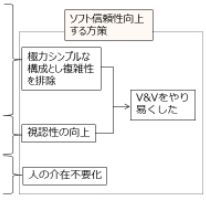
20

高信頼設計・製作



ソフトウェア構造（例）

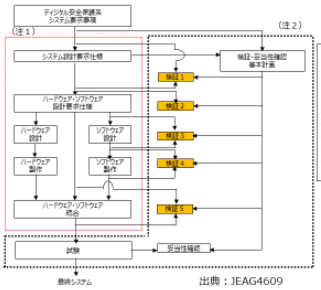
（１）設計・製作
a．OS
・定周期処理
・スケジュール管理だけのシンプルな構成
・信頼性のあるOSを使用
・非同期処理（Ⅰ～Ⅳ系）
b．アプリケーションソフトウェア
・シングルタスク（マルチタスクなし）
・割り込みなし
c．言語
・POL（Problem Oriented Language）の採用
・可視化言語（画面上でAND/OR のマクロを結線）
・POLで作成した制御回路を自動的に機械語へ変換する（コーディング作業不要）
d．自己診断によるソフト異常検出



21

V&Vの実施

デジタル安全保護回路におけるCCF対策に加えて、V&Vを実施



・各設計段階で第３者による図書ベースの確認（検証）

検証１‥システム設計基本仕様検証
検証２‥ハードウェア・ソフトウェア設計要求仕様検証
検証３‥ソフトウェア設計検証
検証４‥ソフトウェア製作検証
検証５‥ハードウェア・ソフトウェア統合検証

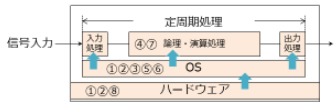
(注１) □ は、設計・製作作業の範囲を示す。
(注２) ⬚ は、検証・妥当性確認作業の範囲を示す。

出典：JEAG4609

自己診断による異常検出

22

自己診断機能により異常動作を早期検知し、警報による告知とともに他装置への影響防止が可能



診断箇所	No.	診断機能	診断対象	診断内容	検出部	警報発報
マイクロプロセッサ部(CPU・メモリ)	①	ウォッチドッグタイマ	計：アプリケーションの周期監視 ハードウェア：計の周期監視	プログラムの演算異常検出	ハードウェア計	○
	②	パリティチェック	メモリ	メモリの異常検出	ハードウェア	○
	③	ゼロ除算	アプリケーション	ゼロ割演算が発生した場合の演算の異常検出	計	○
	④	相互診断	アプリケーション(制御系関)	独立２重系システムにおいて，１系と２系の入力・出力の構差監視	アプリケーション	○
通信部プロセス入出力部	⑤	誤り検出コード	伝送信号	データ伝送時の送受信状態のチェックを行い伝送異常検出	計	○
	⑥	伝送受信中断	伝送信号	データ伝送信号を一定時間内に得られない場合の伝送路異常検出	計	○
	⑦	合理性チェック	入力信号	入力信号が所定レンジを逸脱した場合の異常検出	アプリケーション	○
共通	⑧	構成機器の異常診断	構成機器	ハード機器の異常検出	ハードウェア	○

工場試験や定期的な試験・保守

23

（１）開発・検証
a．ハードウェア検証
PLD等を含めたハードウェアとして全機能試験

b．ソフトウェア検証
構造試験(White Box Test)
性能試験（処理性、応答性、制御性）

c．ハードウェア・ソフトウェア組合せ検証
ハードウェアと組み合わせた状態で、カード、ユニットの全機能を確認

（２）製造・検証
a．工場試験（単体試験、組み合わせ試験）
・模擬信号入力によるインターロックの動作確認
・構成制御試験（制御系切替等）

b．現地での確認
・ソフトウェア復元（工場出荷ソフトウェア）
・インターフェイス試験（補機動作等）
・系統試験、起動試験

（３）定期的な試験・保守
a．定期検査時の確認
・マスターとのコンペアチェック
（ロジックに変化がない事の確認）
・模擬信号による機能試験（スクラム等）

b．月例テスト（サーベランス）による確認
・安全保護系論理回路の機能検査を実施

・ソフトウェアが工場出荷時の状態を保持していることを確認。
・現地試験や定期検査時にインターロック動作を確認。

24

２．ソフトウェアCCFの要因と評価

ソフトウェアCCFの要因と評価

25

（１）ソフトウェアCCFの発生要因とそれを低減するための対応（対策、検知）と、自己診断を考慮すると、**ソフトウェアCCFが起きる可能性は極めて低い**と言える。

ソフトウェアCCFの発生要因

ソフトウェアの構成要素からソフトウェアCCFの発生要因は以下に分類できる。

◆基本ソフトウェア(OS)
・コンパイラ等の開発環境に内在する不具合
・基本ソフトウェア(OS)に内在する不具合

◆アプリケーションソフトウェア
・アプリケーションソフトウェアに内在する不具合

対応(対策、検知)

高信頼設計・製作
ｼﾝﾌﾟﾙな構成、実績あるｿﾌﾄの適用、ｼﾝｸﾞﾙﾀｽｸ、可視化言語の採用、POLｰﾂﾙの自動生成など

検証・試験
開発検証試験、V&V、工場試験、現地試験、月例テスト、定期試験など

検知
自己診断機能によるソフトウェア異常動作を検知

（２）運転実績に基づく信頼性評価
多重化された制御装置（原子力安全保護系、原子力常用系、火力）の国内運転実績は、6.8×10^{8}時間程度におよび、この間ソフトCCFは発生していない。仮に、0.5回が発生したとするとソフトCCF発生頻度は、6.4×10^{-9}/年と評価できる。

（資料 2-2）

資料２－２

多様化設備に対する主な意見

2019年12月4日
原子力エネルギー協議会

1

項　目

１．多様化設備の信頼性確保の考え方（火災、溢水）

２．デジタル安全保護回路に対する代替機能

１．多様化設備の信頼性確保の考え方（火災、溢水）

2

【規制骨子案　抜粋（10/30公開会合）】

・**共通要因によって安全保護機能と同時にその代替作動機能が損なわれるおそれがない**よう適切な手段を講じること

【補足】「適切な措置を講じたもの」とは、安全保護回路の作動が要求される場合において**安全保護機能と代替作動機能が同時に損なわれない**よう、**物理的方法その他の方法によりそれぞれ互いに分離**することをいう。設計基準事故等の起因となる事象に対して、**その起因事象の影響を考慮しても安全保護機能に期待することなく多様化設備により適切に対処**できるよう設計すること。例えば、ある想定される火災区域での**火災により設計基準事故等が発生する場合には、その火災に対して安全保護回路と多様化設備が同時に機能喪失しないよう設計**すること

・許可基準規則（略）**第8条【内部火災】、第9条【溢水】・・によって安全保護機能と同時にその代替作動機能が損なわれるおそれがないよう適切な手段を講じる**こと

【補足】**第12条【安全施設】のうち、第2項（多重性又は多様性及び独立性）については（略）適用しない**

【上記を踏まえた信頼性確保の考え方（意見）】

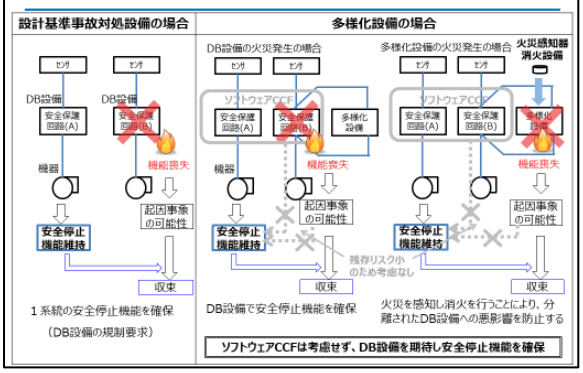
ソフトウェアCCFは設計上の残存リスクであり、火災等に伴う起因事象の発生と重畳するリスクは十分小さいため、火災等の発生に対しては、CCFは考慮せず、設計基準事故対処設備（DB設備）で安全機能を確保できるように対策を講じるものとする。

◎火災・溢水が発生しても、**DB設備で安全停止機能を確保**する

◎多様化設備が、火災・溢水の影響を受けたとしても、**DB設備の安全機能への影響防止を図る**

火災防護の考え方

3



内部溢水防護の考え方

4

設計基準事故対処設備の場合	多様化設備の場合
機器想定破損による溢水の影響 センサ　センサ DB設備　DB設備 安全保護回路　安全保護回路 機器 機能維持　機能維持 堰設置等の対策により、同時に安全停止機能を損なわない	機器想定破損による溢水の影響 センサ　センサ DB設備　DB設備 安全保護回路　安全保護回路　多様化設備 機器 機能維持　機能維持 DB要求と同じく、1系統のDB設備の安全停止機能を確保する ソフトウェアCCFは考慮せず、DB設備を期待し安全停止機能を確保
消火水による被水の影響 センサ　センサ DB設備　DB設備 安全保護回路　安全保護回路 機能維持 被水防止の対策により、同時に安全停止機能を損なわない	消火水による被水の影響 センサ　センサ DB設備　DB設備 安全保護回路　安全保護回路　多様化設備 機能維持

2．デジタル安全保護回路に対する代替機能

5

【規制骨子案　抜粋（10/30公開会合）】

・ソフトウェア起因の共通要因故障により、多重化されたデジタル安全保護回路がその保護機能を喪失した場合において、

A）安全保護回路とは異なる動作原理の機構により、

B）原子炉停止系統及び工学的安全施設を

C）自動的に、又は原子炉制御室から手動により作動させることができること。

【補足】「A）安全保護回路とは異なる動作原理の機構」とは、**ソフトウェアを用いることなく作動させることができるものなど、ソフトウェアに起因する共通要因によってデジタル安全保護回路と同時にその機能を喪失するおそれがないもの**をいう。

【要求事項の考え方（意見）】

A）は、**ソフトウェアを用いた設備であっても、ソフトウェアに起因する共通要因故障によってデジタル安全保護回路と同時にその機能を喪失するおそれがないものについては、代替機能に含まれ**るものと考える。

＜具体的な構成例＞

①デジタル制御回路を使用していない機器　（例：ハードワイヤード）

②デジタル制御回路を使用しているが、デジタル安全保護回路とは共通部分を有しないもの

次頁

2．デジタル安全保護回路に対する代替機能

6

デジタル安全保護回路と**共通の設計の部分が無い**デジタル制御回路であれば、代替作動機能を有する設備として適用可能と考えられる

デジタル安全保護回路：アプリケーション①（論理・演算処理）／OS①／ハードウェア①

異なる設計・製作

代替作動機能を有する設備（例）：アプリケーション②（論理・演算処理）／OS②／ハードウェア②　アプリケーション③（論理・演算処理）／FPGA

異なるハード・OS・アプリケーションで構成された装置

CPUを使用した装置に対し、FPGAのみで構成された装置

＜参考＞米国デジタルI&C審査基準で示されている、ソフトウェアCCFを除外することを認めるクライテリア（BTP7-19 rev.8　3.1.1より抜粋）

・多重性を担う**他の機能と多様性**が図られている（**異なるデジタル技術の採用**）

・**共通又は共有化されたリソース（例：電源、メモリ、バス、通信モジュール等）を持たない**

・使用される技術は高い信頼性があり、期待される期間において継続的に利用可能である

・継続的な運転可能性を検証するために、定期的なサーベイランスクライテリアが使用される

（資料 2-3）

資料２－３

令和元年10月30日
発電用原子炉施設におけるデジタル安全保護系の共通要因故障対策等に関する検討チーム
第１回会合時のご質問回答

2019年12月4日
原子力エネルギー協議会

第１回会合時のご質問内容

1

1．多様化設備がどのように接続されているのか具体的に示してほしい
（多様化設備の接続状況、安全保護回路の多重化等）

2．デジタル安全保護回路の異常検知について詳細を示してほしい
（自己診断機能と異常検知と警報の関係等）

2

1．多様化設備がどのように接続されているのか具体的に示してほしい
（多様化設備の接続状況、安全保護回路の多重化等）

のご回答

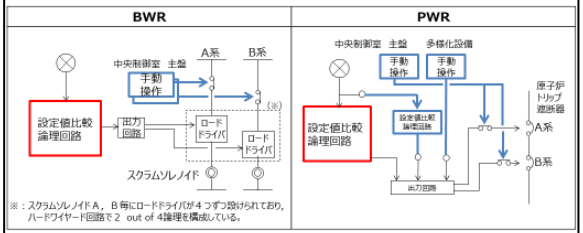
多様化設備の構成（1/4）

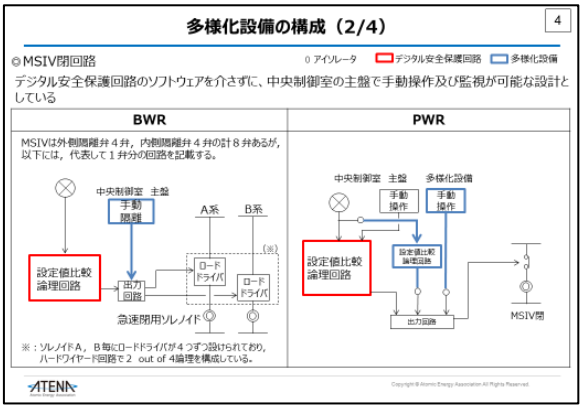
3

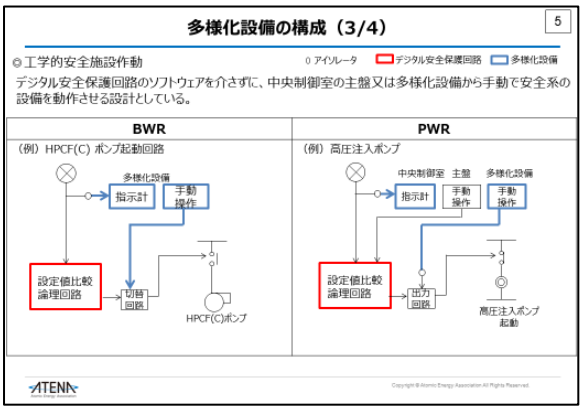
◎原子炉スクラム／トリップ

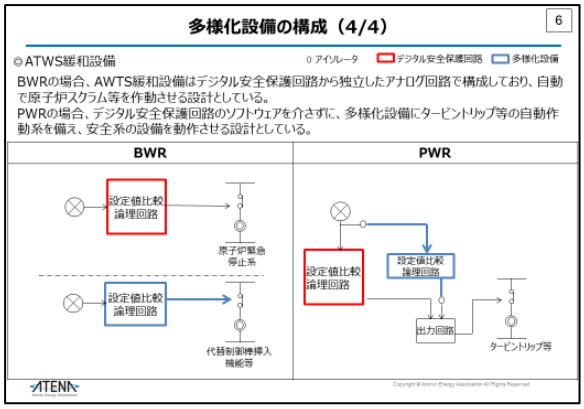
0 アイソレータ　デジタル安全保護回路　多様化設備

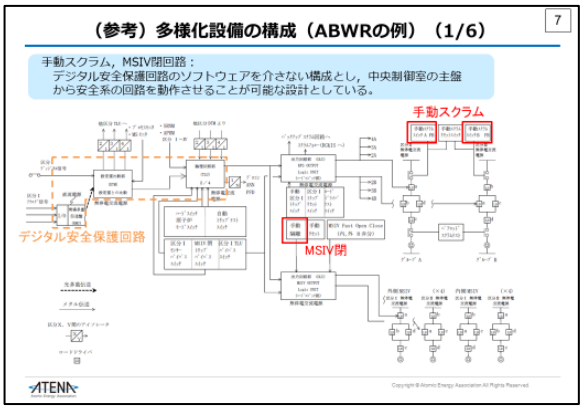
デジタル安全保護回路のソフトウェアを介さずに、中央制御室の主盤から手動でスクラム／トリップを作動させることが可能な設計としている（PWRの場合，多様化設備からの操作も可能）。
また、PWRについては、デジタル安全保護回路とは別に、多様化設備に自動トリップ回路を備え、自動で原子炉トリップを作動させることが可能な設計としている。

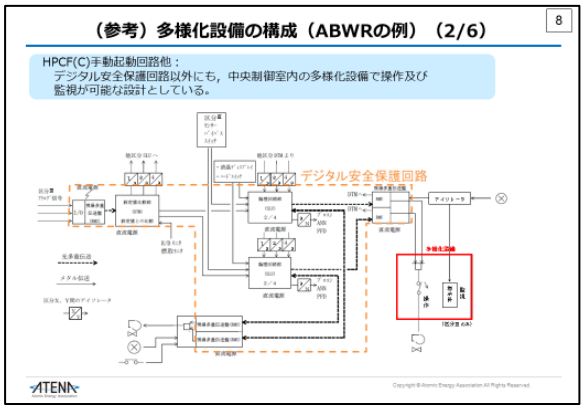


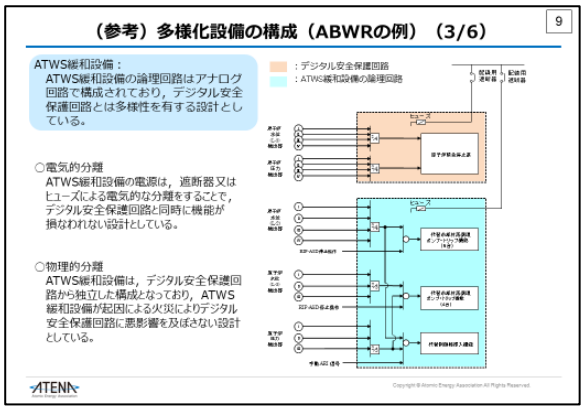


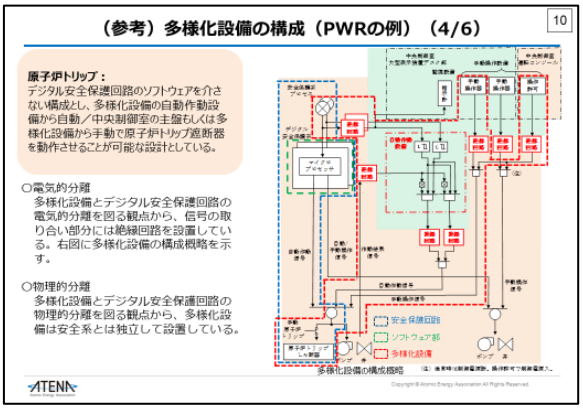


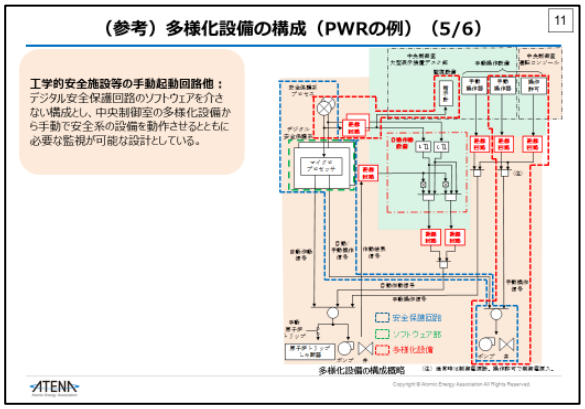








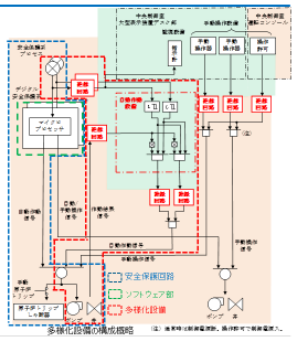




（参考）多様化設備の構成（PWRの例）（6/6）

12

ATWS緩和機能：
デジタル安全保護回路のソフトウェアを介さない構成とし、多様化設備の自動作動設備から安全系の設備を動作させる設計としている。



多様化設備の構成概略

13

2．デジタル安全保護回路の異常検知について詳細を示してほしい
（自己診断機能と異常検知と警報の関係等）

のご回答

自己診断機能と異常検知・警報との関係に関する説明（1/4）

14

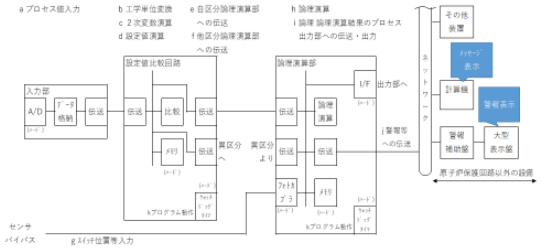
●「プロセス値入力～設定値比較～論理演算～出力」までの各機能に対して、故障モード分析に基づいた自己診断機能により、異常が発生した場合には警報を発報する機能を有している。
次頁以降に構成例と診断項目、診断対象、検出部、及び警報発生の有無について示す。

●自己診断は、異常発生個所と異なる正常な検出部で監視することから、中央制御室に警報として告知できる。警報設備に対する伝送異常が発生した場合でも、受信側設備で異常を検知し、警報等の発報により運転員は認知できる。

●自己診断機能及びV&V、工場試験、定期試験により、異常が未検出で残存する可能性は低いと考えられるが、想定外事象として「OS異常、コンパイラ異常等」時に自己診断が検出できない場合には、ソフトウェアCCFの可能性を否定できないものの、原子力以外の他分野を含む運用実績によりOS、コンパイラの信頼性は極めて高いと言えるので、ソフトウェアCCFとして残存するリスクは小さいと考える。

自己診断機能と異常検知・警報との関係に関する説明（2/4）

15



原子炉緊急停止系における構成（例）

自己診断機能と異常検知・警報との関係に関する説明（3/4）

16

【自己診断項目　例　（1/2）】

部位	機能	NO	項目	自己診断 診断対象	自己診断 検出部	運転員への告知	V&V/工場試験/定期試験/保守	ソフトウェアCCFとしての異常が未検出で残存する可能性（×は無しを表す）	備考
a	プロセス値入力	1	プロセス入力装置異常（基板構成、ＡＩ/ＤＩ回路）	構成機器	ハードウェア	○警報	○実施	× HW起因、自己診断可	
		2	入力上下限オーバ	入力信号	アプリケーション	○警報	○実施	× HW又はプロセス起因、自己診断可	
		3	ＡＤコンバータの変換エラー（断線、特定ビットエラー）	ADコンバータ	ハードウェア	○警報	○実施	× HW起因、自己診断可	
b	工学単位変換	4	変換式・定数プログラムエラー	－	－	△ 指示値、プロセス異常により異常認知	○実施	× 試験で検出可	
		5	制御命令チェック（異常制御命令チェック）	ＣＰＵ	ＯＳ	○警報	○実施	× 自己診断、試験で検出可	
		6	ＣＰＵゼロ割発生	アプリケーション	ＯＳ	○警報	○実施	× 自己診断、試験で検出可	
		7	格納保存・読出異常（メモリチェック）	メモリ	ハードウェア	○警報	○実施	× HW起因、自己診断可	
c	2次変数演算		4,5,6,7による						
d	設定値演算		4,5,6,7による						
e	自区分論理演算部への伝送	8	データ化け	伝送信号	ＯＳ	○警報	○実施	× 自己診断、試験で検出可	
		9	伝送停止	伝送信号	ＯＳ	○警報	○実施	× 自己診断、試験で検出可	
		10	データ更新異常	伝送信号	ＯＳ	○警報	○実施	× 自己診断、試験で検出可	

自己診断機能と異常検知・警報との関係に関する説明（4/4）

17

【自己診断項目　例　（2/2）】

部位	機能	NO	項目	自己診断 診断対象	自己診断 検出部	運転員への告知	V&V/工場試験/定期試験/保守	ソフトウェアCCFとしての異常が未検出で残存する可能性（×は無しを表す）	備考
f	他区分論理演算部への伝送		8,9,10による						
g	スイッチ位置等入力		1による						
h	論理判定		4,5,6,7による						
i	論理判定結果のプロセス出力部への伝送・出力		伝送：8,9,10による						
		11	プロセス出力装置異常（基板構成、ＡＯ/ＤＯ回路）	構成機器	ハードウェア	○警報	○実施	× HW起因、自己診断可	注1)
j	警報等への伝送		伝送：8,9,10による						
k	プログラム動作								
	周期動作	12	ウォッチドッグタイマ	ＯＳ アプリケーション	ハードウェア ＯＳ	○警報	○実施	× 自己診断可	注2)
	ＣＰＵ異常	13	ＣＰＵ命令チェック	ＣＰＵ	ＯＳ	○警報	○実施	× HW起因、自己診断可	
	想定外動作（ＯＳ異常、コンパイラ異常等含む）	14	アドレス範囲チェック ウォッチドッグタイマ	アプリケーション	ＯＳ	○警報	○実施	× 自己診断可	
			上記で検出できない場合	－	－	△ 指示値、プロセス異常により異常認知	－	× 試験で未検出の場合 残存の可能性あるが他分野を含めた実用実績等により残存するリスクは小さいと考える	

注1) Fail Safe動作が必要なものは伝送や出力装置異常の場合ソフトウェアによらず安全側に動作する。
注2) これらの異常の場合、Fail Safe動作が必要な機能については、ソフトウェアによらず安全側に動作する。

参考書類 3

第 4 回　NRA 検討チーム公開会合（2020 年 1 月 29 日開催）資料

1. 開催日　2020 年 1 月 29 日
2. ATENA が提示した会合資料は以下のとおり。

資料1

デジタル安全保護回路のソフトウェアCCFの影響評価と対策

2020年1月29日
原子力エネルギー協議会

1

目 次

2

1．はじめに

3

（1）デジタル安全保護回路のソフトウェアCCF対策検討の位置づけ

デジタル安全保護回路のソフトウェアCCF対策については、

① ソフトウェアCCFは、ソフトウェアに対する信頼性向上の取り組み（高信頼設計、設計・製作時のV&V、定期試験等）により、十分な発生防止対策が取られており、ソフトウェアCCFが発生する可能性は極めて低く抑えられていること（12/4のATENA会合資料）

② 過渡及び事故の発生時に、ソフトウェアCCFが重畳発生する可能性はさらに低いものの、事象発生時の影響が大きいことから影響評価を実施したところ、自主で備えた多様化設備は、殆どの過渡事象及び事故に対し、有効であるとの結果が得られた。（添付資料1及び2）

③ なお、上記ソフトウェアCCF対策により炉心損傷が防止できない場合でも、格納容器破損防止対策により環境への大量の放射性物質の放出は防止することができる。

以上より、安全上の緊急性は高くないと考えるものの、深層防護を重視し、対策の検討を実施した。

4

2．影響評価（1/2）

（1） 想定事象
ソフトウェアCCFにより安全保護機能が喪失している状態で、単一の過渡・事故事象（いずれも全事象が対象）を想定する。

（2） 評価方法
過渡及び事故と「ソフトウェアCCFによる安全保護機能の喪失」が重畳発生した場合に、現実的な評価により、多様化設備の有効性を評価する。

主要な評価条件（例）を下記に示す。
- デジタル安全保護回路を経由しない自動もしくは手動起動信号で、原子炉停止系及び工学的安全施設は利用可能
- 安全設備の単一故障は想定しない
- 外部電源喪失事象以外の事象では外部電源は利用可能
- 外部電源喪失及び給水流量の全喪失事象以外の事象では給水系の運転は継続する
- サポート系（冷却水・空調）については、起因事象が発生する前の作動状態を維持する
- 現実的な評価をする際に必要に応じて、ベストエスティメイトコードを使用する

5

2．影響評価（2/2）

（2） 評価方法（前頁からの続き）
- 事象発生前の初期状態としては、ノミナル条件（出力、水温など）とする
- 制御棒誤引き抜き過渡・落下事故において、運用を考慮した現実的な制御棒価値を想定する（BWR）
- 中央制御室での運転操作時間は現実的に考慮する（１０分ルールは適用しない）
- 時間余裕の範囲で現場操作を想定する
- 多様化設備の性能を確認する観点から多様化設備の故障は想定しない

（3）影響評価（予備評価）
BWRの影響評価は添付資料１を、PWRの影響評価は添付資料２を参照

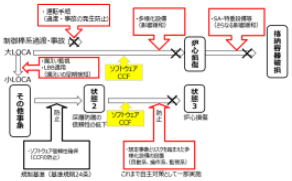
6

3．デジタル安全保護回路のソフトウェアCCF対策

7

（1）対策の検討

・影響評価の結果、ソフトウェアCCFと過渡・事故が重畳した場合でも、以下の対策により事象の収束は可能である。
・評価の過程で抽出された対策は以下のように、深層防護の幅広い階層に渡るものとなる
【対策1】警報等の事象発生の認知手段の充実（早期検知）
【対策2】事象発生時の手順の整備（認知・判断・行動）
【対策3】BWRの起動時の制御棒の異常な引き抜きの発生防止・緩和（運転員による手動引抜阻止の教育と徹底）
【対策4】PWRの大LOCAの発生防止・緩和（LBB適用、注水系自動起動、SA設備による格納容器破損防止）



8

（2）対策の選択

○抽出した対策の選択に当たっては、以下のような観点を考慮する
a.深層防護のバランスに配慮すること
b.実行可能な対策であること（費用対効果があること）
c.当該対策の実施により安全性を阻害する要因を持ち込まないこと
d.国際的な対策水準を考慮すること

○これらを考慮した場合の代表プラントに対する対策は以下のようになる

【対策1】【対策2】は早期検知と迅速な対応の観点から重要であり、上記の観点を満足する必須対策となる
【対策3】運転員による制御棒操作手順の順守で確実に発生防止が図られ、かつ監視により事象発生の影響緩和が可能である
【対策4】は既に格納容器破損防止対策がとられているものの、影響緩和としてより前段の炉心損傷防止を重視し、SI自動化を対策とする

9

（3）BWR及びPWRの対策（1/4）

BWR（ABWR）対策方針・対策

1．対策方針
デジタル安全保護回路のソフトウエアCCFと過渡・事故の重畳を想定し、デジタル安全保護回路が機能喪失した場合においても、多様化設備により安全停止機能を損なうおそれのない設計とする。

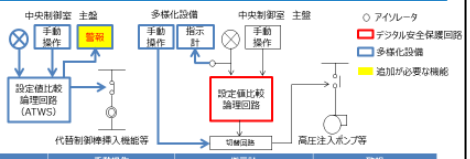
2．対策
手順書整備の他、以下の対策を採用する。

警報機能：　ARI作動
原子炉水位低
原子炉圧力高

10

（3）BWR及びPWRの対策（2/4）

BWRの設備対策案



自動機能	手動操作	指示計	警報
・原子炉スクラム※ ・原子炉再循環ポンプトリップ※	・原子炉スクラム ・主蒸気隔離弁閉止 ・主要な隔離弁閉止 ・高圧炉心注水系起動	・原子炉水位 ・原子炉圧力 ・ドライウェル圧力 ・主蒸気隔離弁の状態 ・主要な隔離弁の状態 ・高圧炉心注水系起動状態 ・高圧炉心注水系系統流量	・ARI作動 ・原子炉水位低 ・原子炉圧力高

黒字：既設のバックアップ機能
赤字：追加が必要な機能
※：新規制基準施行後は、重大事故等対処設備として扱っている。

11

（3）BWR及びPWRの対策（3/4）

PWR対策方針・対策

1．対策方針
デジタル安全保護回路のソフトウェアCCFと過渡・事故の重畳を想定し、デジタル安全保護回路が機能喪失した場合においても、多様化設備により安全停止機能を損なうおそれのない設計とする。

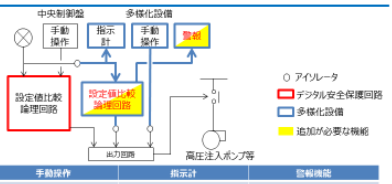
2．対策
手順書整備の他、以下の対策を採用する。

自動機能：　自動SI「起動」
警報機能：　加圧器圧力異常低（SI作動）

12

（3）BWR及びPWRの対策（4/4）

PWRの設備対策案



自動機能	手動操作	指示計	警報機能
・原子炉トリップ ・タービントリップ※ ・主給水隔離 ・補助給水起動※ ・主蒸気隔離※ ・高圧／低圧注入系起動	・原子炉トリップ ・タービントリップ ・主給水隔離 ・補助給水隔離／流量調節 ・主蒸気隔離 ・高圧注入系起動 ・格納容器隔離	・中間領域中性子束 ・加圧器圧力 ・１次冷却材圧力 ・１次冷却材低温側温度（広域） ・加圧器水位 ・主蒸気ライン圧力 ・蒸気発生器水位（狭域） ・格納容器圧力 ・蒸気発生器２次側放射線 ・対象補機の状態	・多様化設備作動 ・加圧器圧力低（原子炉トリップ等） ・加圧器圧力高（原子炉トリップ等） ・蒸気発生器水位低（原子炉トリップ等） ・蒸気発生器水位異常高 ・加圧器圧力異常低（高圧／低圧注入系作動）

黒字：既設のバックアップ機能
赤字：追加が必要な機能
※：新規制基準施行後は、重大事故等対処設備として扱っている。

13

4．ATENAの取り組み方針

（1）ATENAの取り組み方針（1/2）

14

1. これまでのソフトウェアに対する信頼性向上の取り組みにより、ソフトウェアCCFが発生する可能性は極めて低く抑えられている。
   また、深層防護の観点から過渡・事故発生時にソフトウェアCCFが重畳する場合を想定したとしても、決定論的安全評価手法で評価すると、これまで自主対策で備えた多様化設備によって、殆どの過渡・事故に対して、炉心損傷防止が可能であると評価される。

2. 一方、大中破断LOCAとソフトウェアCCFの重畳については、現状の多様化設備では炉心損傷に至ると評価される。これらの炉心損傷の発生確率は十分低いものの、会合での議論や国際的な対策水準を踏まえ、炉心損傷防止を重視し、更なる対策を行うことが適切であるとの結論に至った。

3. その他の安全性向上対策も輻輳する中で、産業界として安全上の優先度を考慮し、自律的に且つ計画的に取り組んでいく。

（1）ATENAの取り組み方針（2/2）

15

4. 産業界が自律的に取り組む場合、ATENAのガバナンスのもと、16 に示すプロセスで進めていく。

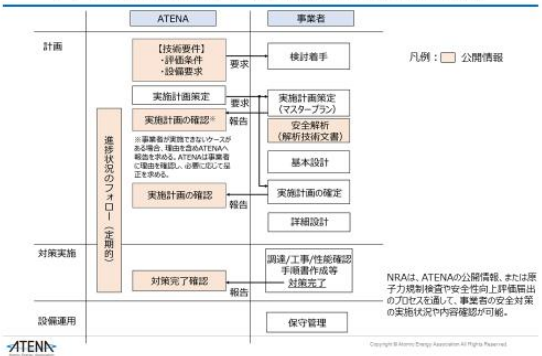
（1）ATENAは、評価条件と設備要求（以下、「技術要件」という）を纏め、安全解析及び基本設計を各事業者が合理的且つ早期に対応できるようにする。

（2）ATENAは各事業者へ実施計画の提出を要求し、実施計画を公開する。また、進捗をフォローし、進捗状況及び対策完了状況を公開する。

5. ATENAは、海外動向も参考にしながら、多様化設備へのデジタル設備の適用性等を含め技術的検討を継続していく。

（2）安全対策の検討／実施／運用の自律的プロセス（例）

16



（3）実施時期の考え方

17

1. ATENAは、技術要件を2020年5月末を目途に作成し、各事業者へ提示すると共に公開する。

2. BWR及びPWR事業者は、技術要件を基に安全解析に着手し、それぞれ解析技術文書として纏める。その結果に基づき、各事業者は具体的に実施する対策を確定するとともに、詳細設計及び対策設備の調達を行う。

3. 工事実施時期は事業者毎に異なるが、再稼働時期を踏まえて、以下とする。
   （安全解析に2年程度要すると想定。設備改造は１回の定検で工事可能と想定。）

   対象プラント：デジタル安全保護回路導入済プラント及び
   導入予定プラント（部分デジタル化プラントも含む）

・再稼働済み、もしくは
   2023年度までに再稼働するプラント；2023年度以降の最初の施設定検時
・2023年度以降に再稼働するプラント；　再稼働時期までに実施

（参考）ATENA技術課題の解決プロセス

18

ATENAは、以下のプロセスで技術課題を解決する。

- ATENAが取り組む課題については、ステアリング会議にて決定する。
- 課題の技術検討は、産業界の専門家で構成したワーキンググループで行う。
- 取り纏めた検討結果（安全対策）をステアリング会議で決定し、各事業者は決定内容にコミットする。また、ATENAは技術レポート等を公開する。
- ATENAは安全対策の実施を各事業者に要求し、各事業者は現場の対策を実行する。
- ATENAは各事業者の対策実施状況をフォローし、公開する。

添付資料　1

BWRにおけるデジタル安全保護回路の
ソフトウェアCCFを前提とした影響評価
（予備評価結果）について

BWRにおけるデジタル安全保護回路の ソフトウェアCCFを前提とした影響評価 （予備評価結果）について

東京電力ホールディングス株式会社
東芝エネルギーシステムズ株式会社
日立GEニュークリア・エナジー株式会社
株式会社グローバル・ニュークリア・フュエル・ジャパン

1

事象想定の考え方（解析のグルーピング）

- ソフトウェアCCFの影響を確認する観点から類似する事象をグルーピング
- 影響の程度が軽微であることが定性的に評価できるものは解析を省略

【止める】RIA、RIA以外の2種類に大別

- ARIは炉圧高又は水位低で自動起動。したがって、過渡及び事故の隔離事象及び非隔離事象については、いずれかの信号によりCR挿入
- 一方で、部分的な出力上昇で初期の炉心挙動が大幅に変動しない事象（CR誤引抜き、CR落下）は、ARI自動起動に期待できない
- また、解析の着眼点も全く異なる（PCTではなくエンタルピーで判断）

【冷やす】LOCAとLOCA以外の2種類に大別

- 初期の水位低下速度と初期注水のタイミングが以降のヒートアップに大きく影響
- これにより、概ね全ての過渡事象（CR誤引抜きを除く）及び事故の一部は、LOCA以外の事象として代表することができる

【閉じ込める】定性的な評価が可能

- 燃料集合体の落下などは、それら事故の影響の拡大は限定的であり（事故発生以降の放出インベントリの増加はない）、CCFにより放射能放出抑制機能が低下しても、それ以上の影響の拡大には至らない
  【主蒸気管破断、燃料集合体の落下、原子炉冷却材喪失、放射性気体廃棄物処理施設の破損】
- 「原子炉格納容器内圧力、雰囲気等の異常な変化」に挙げられる事象は、デジタル安全保護回路の自動起動の影響は支配的でなく、評価の着眼点が運転員による手動起動（格納容器スプレイ手動起動、FCS手動起動など）及びその系統容量確認が主眼となる。加えて、事象の認知から操作までの時間に十分な余裕が確保され、また、単一故障想定がない場合、影響は小さい
  【原子炉冷却材喪失、可燃性ガスの発生】

2

事象想定（解析対象事象）

事象	原子炉停止系統作動信号	工学的安全施設作動信号	解析のグルーピング
【運転時の異常な過渡変化】			
原子炉起動時における制御棒の異常な引き抜き	原子炉周期短	—	RIA（RIE）
出力運転中の制御棒の異常な引き抜き	—	—	
原子炉冷却材流量の部分喪失	—	—	LOCA以外
外部電源喪失	CV急開	—	
給水加熱喪失	中性子束高（熱流束相当）	—	
原子炉冷却材流量制御系の故障	中性子束高	—	
負荷の喪失	CV急開	—	
主蒸気隔離弁の誤閉止	MSIV閉	—	
給水制御系の故障	MSIV閉	—	
原子炉圧力制御系の故障	MSIV閉	—	
給水流量の全喪失	水位L3	L2RCIC（補給水機能）	
【設計基準事故】			
原子炉冷却材喪失	水位L3 or D/W圧力高	水位L1.5 or D/W圧力高（高圧系） 水位L1 or D/W圧力高（低圧系） 水位L1 and D/W圧力高（ADS）	LOCA
原子炉冷却材流量の喪失	炉心流量急減	—	LOCA以外
制御棒落下	APRM高	—	RIA（RDA）

無断転載・転載禁止

解析の前提条件

解析コード：ベストエスティメイトコードの使用（TRAC系コード）
- 現行の事故解析コード（SAFER）は、炉心ヒートアップについて保守的なモデル（ホットチャンネル）となっており、時間余裕を評価する観点でノミナルの出力分布を仮定するため
- ARI動作はスクラムが従来解析より若干遅れることから、核熱結合動特性計算を行っているTRAC系コードは現実的な解析となる
- 給水継続を想定する場合、給水制御系のロジックをモデル化していることから、より現実的な評価が可能
- ただし、操作の対応時間が十分である場合または判断基準に対して十分な余裕がある場合は、保守的ではあるが従来コードを使用する

解析で期待できるバックアップ設備（次ページ以降参照）

As Isとして期待する機能；
- 外部電源（当該機能による過渡を除く）
- 給水制御（当該機能による過渡及び起因事象により当該機能が喪失する事故を除く）
- CRD注水（パージ水）

運転員操作として期待する機能
- 運転操作に対する制限（10分等）は設けない

その他
- 単一故障：想定せず
- 事象発生前の初期状態：ノミナル条件（水温、出力等）
- 多様性を有する設備（既に設置済の設備）：炉圧高・水位低RPT、ARI（自動作動）
- 現実的な制御棒価値（一本引き抜き：1%Δk、ABWRギャング引き抜き：2.3%Δk）

なお、本資料で示す解析結果は予備評価結果であり、今後の評価の進捗によって変更し得る

無断転載・転載禁止

解析で期待できるバックアップ設備（１／３）

記号説明 ○：アナログ、 ×：デジタルCTL経由

	事象	機器作動	作動方式	監視項目	警報	指示	設置場所
1	スクラム	ARI作動	自動	原子炉水位	×	○（S A）	MCR補助盤（指示計）
				原子炉圧力	×	○（S A）	MCR補助盤（指示計）
				ARI作動の状態	×	—	大型表示盤（簡略表示）
2	隔離	MSIV閉	手動	原子炉水位	×	○（SA）	MCR補助盤（指示計）
				原子炉圧力	×	○（SA）	MCR補助盤（指示計）
				MSIVの状態	–	○（DIV）	主盤（簡略表示）
3	原子炉注水＊	HPCF（C）起動	手動	原子炉水位	×	○（SA）	MCR補助盤（指示計）
				D/W圧力	×	○（NON）	MCR補助盤（指示計）
				系統流量	–	○（DIV）	MCR補助盤（指示計）
				HPCF（C）の状態	–	○（DIV）	MCR補助盤（指示計）

＊ HPCF（B）についてもＲＳＳ室からの手動起動は可能

無断転載・転載禁止

解析で期待できるバックアップ設備（２／３）

記号説明 ○：アナログ、 ×：デジタルCTL経由

	事象	機器作動	作動方式	監視項目	警報	指示	設置場所
4	炉圧制御＊	SRV開	手動	原子炉圧力	×	○（S A）	MCR補助盤（指示計）
				SRV状態表示	–	○（S A）	主盤、大型表示盤（簡略表示）
				原子炉水位	×	○（S A）	MCR補助盤（指示計）
5	S/P冷却	RSW起動	手動	RSW状態表示	–	○	RSS室
		RCW起動	手動	RCW状態表示	–	○	RSS室
				系統流量	–	○	RSS室
		RHR起動（S/Cクーリング モード）	手動	RHR状態表示	–	○	RSS室
				系統流量	–	○	RSS室
				S/P温度	–	○	RSS室
				原子炉水位	–	○	RSS室
				原子炉圧力	–	○	RSS室

＊ ＲＳＳ室でも、ＳＲＶの手動操作、ＳＲＶの状態監視、原子炉圧力の監視、原子炉水位の監視は可能。

無断転載・転載禁止

解析で期待できるバックアップ設備（３／３）

記号説明 ○：アナログ、 ×：デジタルCTL経由

	事象	機器作動	作動方式	監視項目	警報	指示	設置場所
6	原子炉長期冷却	RSW起動	手動	RSW状態表示	–	○	RSS室
		RCW起動	手動	RCW状態表示	–	○	RSS室
				系統流量	–	○	RSS室
		RHR起動（ﾌｨｯﾄﾊﾞｯｸｸｰﾘﾝｸﾞ モード）	手動	RHR状態表示	–	○	RSS室
				系統流量	–	○	RSS室
				原子炉水位	–	○	RSS室
				原子炉圧力	–	○	RSS室

無断転載・転載禁止

CCFを想定した場合の予備評価結果のまとめ

LOCA以外（別添１）：炉心損傷の防止は可能
- 運転中の過渡又は事故事象が発生した場合、ＣＣＦにより自動スクラムはしないもののＡＲＩにより自動CR挿入
- 初期炉心注水として、バックアップ設備（HPCF手動）により注水することとなるが、LOCA以外の事象は炉心損傷までの時間余裕（30分～1時間程度）があることから手動操作により問題なく注水は可能
- 以降の除熱についても、RSS室からの手動起動操作によって対応可能

LOCA（別添２）：事象発生後10分程度でHPCF1台を起動できれば炉心損傷の防止は可能
- LOCAが発生した場合、ＣＣＦにより自動スクラムはしないもののＡＲＩにより自動スクラム
- 原子炉水位は、LOCA以外の事象に比べ早く低下するが、最厳ケースでも14分までにバックアップ設備（HPCF手動）により注水できれば、炉心損傷の防止が可能
- 以降の除熱についても、RSS室からの手動起動操作によって対応可能

RIA（別添３）：ABWRの起動時の異常な引き抜きを除き、エンタルピーは判断基準を満たす
- 炉心設計は、1%ΔKを目安に炉心設計及び操作手順が策定されており、これにより制御棒１本の落下及び引き抜きは低温状態、高温状態ともに判断基準（事故に対するエンタルピー）を満たす
- 一方で、ABWRの起動時における異常な引き抜きは、臨界近傍における制御棒価値を現実的な条件（2.3%Δk）としても、連続での全引き抜きを想定すると最大エンタルピーは判断基準を超えるが、運転員は異常に気づて連続引き抜きを中断することが可能

線量影響（主蒸気管破断、燃料集合体の落下）（参考１）
- 代表サイトにおける現実的評価条件（「値1/10等）においては、概ね判断基準を超えることはない
- サイト条件によっては結果が厳しくなるものの影響は限定的であり、また、更なる現実的条件適用による低減可

- 現行バックアップは概ね有効であり、CCF発生により重大な事態には至ることはない
- ✓ ただし運転員のCCF認知は極めて重要 ⇒ 追加CCF対策の必要性は高い
- ✓ 制御棒の異常な引抜きは、そもそも現実的想定が困難で有り、手順や確認行為により発生防止が図られている ⇒ 追加CCF対策の必要性は低い
- ✓ 線量評価は、炉心損傷防止に重点を置くことで、影響拡大は限定的となる ⇒ 追加CCF対策の必要性は低い

無断転載・転載禁止

LOCA以外の過渡・事故解析のプラント状態

別添1

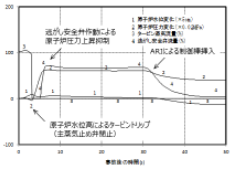
事象	プラント挙動（設計ベース）	CCFによる機器喪失	多様化設備	常用系（on duty）	CCF発生時の対応
冷却材流量の部分喪失	RIP３台トリップ→出力絞下→整定	RPS(ESFAS)/MSIV	RPT(AR起動) HPCF(中操(C)、RSS(B)) RHR(AR(B)/RSS) MSIV(中操)	圧力/給水制御系 外部電源	スクラムせずに整定
外部電源喪失	外電喪失→発電機負荷遮断→スクラム	問上	問上	出力/圧力/給水制御系	ARI(炉圧高)で炉停止 停止後はHPCF/RHRで冷却/除熱(手動)
給水加熱喪失	給水加熱喪失→給水温度低下→中性子束上昇→スクラム(中性子束高)	問上	問上	出力/圧力/制御系 外部電源	問上
冷却材流量制御系の誤操作	再循環流量増加→出力上昇→スクラム(中性子束高)	問上	問上	圧力/給水制御系 外部電源	問上
負荷の喪失	CV急閉→スクラム	問上	問上	出力/給水制御系	問上
主蒸気隔離弁の誤閉止	MSIV誤閉→スクラム	問上(MSIV除く)	問上	出力/圧力/給水制御系 外部電源	問上
給水制御系の故障	給水流量増加→水位上昇→Trトリップ(L8)→スクラム	問上	問上	出力/圧力制御系 外部電源	問上
圧力制御系の故障	最大出力信号発生→CV/BPV全開→炉圧低下→MSV閉→スクラム	問上	問上	出力/給水制御系 外部電源	問上
給水流量の全喪失	給水ポンプトリップ→水位低下→スクラム(L3)	問上	問上	出力/圧力制御系 外部電源	ARI(水位L2)で炉停止 停止後は問上
冷却材流量の喪失	RIP全台トリップ→炉心流量急減→スクラム	問上	問上	圧力/給水制御系 外部電源	ARI(炉圧高)で炉停止 停止後は問上

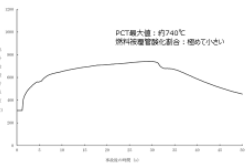
無断転載・転載禁止

LOCA以外の過渡・事故解析の予備評価結果

別添1

冷却材流量の喪失を前提としての評価
- 解析コードは従来コードを使用（保守性排除せず）
- 初期条件は許認可解析と同一（保守性排除せず）
- RPS（炉心流量急減）の不作動を仮定
- 多様化設備のARI（原子炉圧力高信号）による制御棒挿入（約25秒）





- 原子炉圧力＜ 10.34 MPa[gage]（最高使用圧力×1.2）
- PCT＜1200 ℃、ECR＜15%
- 短期挙動の収束後はHPCF/RHRにより原子炉冷却/除熱

無断転載・転載禁止

LOCAの解析条件と評価シナリオ

別添2

- 解析コード：原子炉過渡解析コード（TRACG）
- 初期条件：9×9燃料（A型）炉心 ノミナル出力分布、100%出力／100%炉心流量
- 想定シナリオ：① 給水配管破断 ⇒ 全給水喪失、CRDパージ水による注水継続
  ⇒ RPS（水位低又はD/W圧高）によるスクラム失敗
  ⇒ 多様化設備のARI （水位低L2）による自動制御棒挿入（約25秒）
  ⇒ 多様化設備によるHPCF1台の手動起動
  ⇒ 原子炉水位回復

  ② RHR出口配管破断 ⇒ 給水継続、CRDパージ水による注水継続
  ⇒ RPS（水位低又はD/W圧高）によるスクラム失敗
  ⇒ 多様化設備のARI （水位低L2）による自動制御棒挿入（約25秒）
  ⇒ 復水枯渇による給水停止
  ⇒ 多様化設備によるHPCF1台の手動起動
  ⇒ 原子炉水位回復

・解析では原子炉水位回復までの挙動を評価。水位回復後の長期崩壊熱除去については、RHR S/P水冷却モードが、いずれの配管破断の場合においても破断の影響を受けず、RSSから多様化設備によるRHR(A)(B)の2系統の手動起動が可能であり、HPCFで原子炉水位を維持しながら、S/P水冷却モードにより崩壊熱除去を行うことにより安全な状態に移行する

無断転載・転載禁止

11

破断箇所毎のプラント応答

別添2

事象	プラント挙動（設計ベース）	CCFによる機能喪失	多様化設備	常用系（on duty）	CCF発生時の対応
主蒸気配管破断	配管破断→原子炉スクラム(自動)→MSIVによる原子炉隔離(自動)→ECCSによる炉心冷却(自動)→RHRによる崩壊熱除熱(手動)	RPS/ESFAS/MSIV	RPT/ARI(自動) HPCF(中操)(C)、RSS(B) RHR(A)(B)(RSS) MSIV(中操)	給水制御系（復水枯渇まで給水継続） 外部電源 制御棒駆動系	ARI(水位低)で炉停止停止後はHPCF/RHRで冷却/除熱(手動) MSIVで放射性物質の閉じ込め
給水配管破断	同上	同上	同上	外部電源 制御棒駆動系	同上
RHR出口配管破断	同上	同上	同上	給水制御系（復水枯渇まで給水継続） 外部電源 制御棒駆動系	同上
LPFL配管破断	同上	同上	同上	同上	同上
HPCF配管破断	同上	同上	同上	同上	同上
ドレン配管破断	同上	同上	同上	同上	同上

無断転載・転載禁止

12

LOCA時の操作余裕時間（予備評価結果）

別添2

- HPCF1台の手動起動時間に対する感度解析を実施
- LOCA+CCFの最厳ケースである給水配管破断において、炉心の著しい損傷を防止（ PCT＜1200 ℃、ECR＜15% ） するために、HPCF手動起動に要求される時間余裕は**14分程度**と評価される

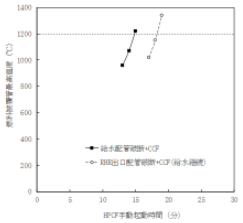


図 TRACGによるLOCA+デジタル安全保護系CCF解析におけるHPCF手動起動時間と燃料被覆管温度の関係

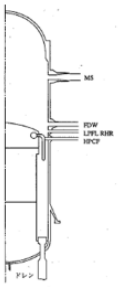
無断転載・転載禁止

13

LOCA破断口位置の考え方

別添2参考

分類	破断位置	配管径 (mm)	有効断面積を与える部所	破断面積
大LOCA	主蒸気配管 (MS)	700	フローリミッタ部×4	ベースの約5倍
	給水配管 (FDW)	550	スパージャノズル部	ベース
	RHR出口配管	350	配管部	ベースと同等
中LOCA	LPFL配管	200	スパージャノズル部	ベースの約1/4
	HPCF配管	200	スパージャノズル部	ベースの約1/6
小LOCA	ドレン配管	65	ベッセルノズル部	ベースの約1/40



・給水配管破断は、破断時に冷却材流出を律速する有効断面積、及び給復水系による注水継続の可否の観点から、運転員操作に要求される時間余裕に対する最厳ケースとなる

・RHR出口配管破断は、給復水系による注水が継続するものの、破断位置が給水の注水位置より低く、効果が限定的であることから、運転員操作に要求される時間余裕を確認

無断転載・転載禁止

14

LOCA＋CCFの予備評価結果（給水配管破断）

別添2参考

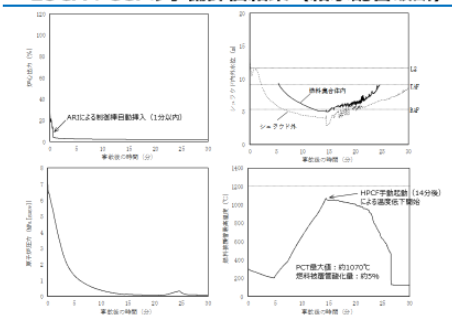


図 TRACGによる給水配管破断＋デジタル安全保護系CCF解析例（14分後HPCF手動起動を想定）

無断転載・転載禁止

15

LOCA＋CCFの予備評価結果（RHR出口配管破断）

別添2参考

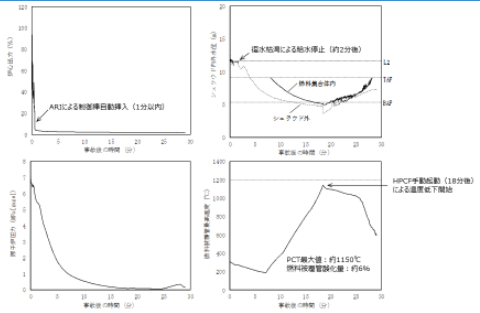


図 TRACGによるRHR出口配管破断（給水継続）＋デジタル安全保護系CCF解析例（18分後HPCF手動起動を想定）

無断転載・転載禁止

16

LOCA時の操作余裕時間（各破断箇所まとめ）

別添2参考

- 主蒸気配管破断は、原子炉減圧及び原子炉冷却材保有水量低下の観点で、最も厳しくなると考えられるが、破断した配管のRPVとの接続が給水スパージャよりも高いところに位置するため、給水継続が冷却材保有水量回復に大きく寄与
- HPCF（C）配管破断の場合、運転員は中央制御室からHPCF（C）を手動起動しても原子炉水位が上昇しないことを確認後、中央制御室からRSSに移動してRSSからHPCF（B）を手動起動する必要がある。このとき炉心の著しい損傷を防止するために運転員操作に要求される時間余裕は40分程度と評価された

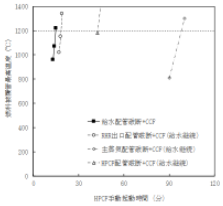


図 TRACGによるLOCA+安全保護系CCF解析におけるHPCF手動起動時間と燃料被覆管温度の関係

無断転載・転載禁止

17

RIA（制御棒過渡・事故）の予備評価結果

別添3

- 解析コード：TRACG（非断熱ドップラ、ボイドフィードバック考慮）
- 評価対象炉心：ABWR 9X9燃料（A型）平衡炉心
- 想定シナリオ：
  （制御棒落下）
  制御棒1本落下（0.95m/s、BWR5相当）⇒出力パルス発生⇒反応度フィードバックによる出力抑制⇒RPSによるスクラム失敗⇒反応度バランスで出力静定
  （制御棒引抜）
  ギャング連続引抜き（3.3cm/s）⇒ペリオド短によるロッドブロック失敗⇒出力パルス発生⇒反応度フィードバックによる出力抑制⇒ RPSによるスクラム失敗⇒反応度バランスで出力静定
- 想定条件（主な変更点）［実炉心で想定される運転条件］
  （制御棒落下）制御棒価値1.3%Δk⇒1.0%Δk、水温20℃⇒60℃
  （制御棒引抜）制御棒価値3.5%Δk⇒2.3%Δk、水温20℃⇒60℃
- 解析結果
  （制御棒落下）最大エンタルピ：約120cal/g（約500kJ/kg）、破損割合：1%程度
  （制御棒引抜）最大エンタルピ：判断基準を満足しない

無断転載・転載禁止

18

起動時引抜きの手順による反応度投入防止について

別添3

- 臨界近傍における操作（別添３参考参照）
  - ✓ 制御棒位置や核計装指示値を操作者及び確認者など複数人で確認しながら、制御棒操作手順に従いペリオドが100秒を超えないよう少しずつ引抜操作を実施する
  - ✓ どのステップで臨界になるか臨界予測により事前に確認されており、比較がなされる
  - ✓ 次のステップへ移行するためには、SRNM指示などのパラメーター変動が特定することの確認が必要
  - ✓ **仮に連続引抜中に異常が起こってもボタンから手を離せば止まる**
- **臨界近傍で、SRNM指示値が変動しない、表示しないなどの異常があるにも関わらず引き抜き続けることは想定し得ない**
- 仮に連続引き抜きが行われるという前提を置いても、1%Δk分を連続引き抜きするのには速い場合でも8sec程度かかるため、それまでに十分に運転員は異常に気づいて連続引き抜きを中断することが可能

➡ **制御棒連続引き抜きの中断に期待することは、LOCAでHPCF手動起動することと同等（人間系によるロッドブロックに相当）**

制御棒連続引き抜きを中断することを仮定した場合の評価

- 想定シナリオ：
（制御棒引抜）
ギャング連続引抜き（3.3cm/s）⇒ペリオド短によるロッドブロック失敗⇒出力パルス発生⇒ RPSによるスクラム失敗⇒連続引抜中にボタンより手を離し引き抜き停止
- 想定条件
（制御棒引抜）制御棒価値3.5%Δk⇒1.0%Δk（8秒以内に操作を停止した場合の反応度として仮定）
水温60℃
- 解析結果
（制御棒引抜）最大エンタルピ：約50cal/g（約200kJ/kg）、破損割合：破損なし

無許可・転載禁止

19

起動時引抜きの手順による反応度投入防止について

別添3（参考）

- 過渡事象「起動時における制御棒の異常な引き抜き」の概要
- 原子炉の起動時に運転員の誤操作等により制御棒が連続的に引き抜かれ、原子炉出力が上昇
- 制御棒引き抜きにより原子炉出力は上昇するが、SRNMペリオド短信号（20 秒）で制御棒引き抜きが阻止され、また、SRNMペリオド短信号（10 秒）で原子炉はスクラムされ、事象は収束
- 投入される反応度は約0.7ドルにとどまり、反応度投入事象には至らないことから、原子炉出力の上昇は緩やかとなり、燃料エンタルピの増加に伴う燃料の破損は生じない
- ここで、制御棒価値ミニマイザに記憶される制御棒引抜シーケンス監視プログラムの設計基準として、臨界近接時におけるギャング引き抜きによる制御棒グループの最大反応度価値を0.035dk以下に制限
- また、起動領域モニタ系は、事象の発生前及び事象の過程中に動作状態にあり、かつ、多重化及びフェイルセイフ設計を採用することから、信頼性の高い設備であることから、そのインタロック機能を考慮。また安全保護系は2out of4方式の構成としているため、単一故障を仮定しても機能を喪失せず信頼性は高い

- 「起動時における制御棒の異常な引き抜き」とデジタルCCF重畳の仮定
- 原子炉の起動時に運転員の誤操作等により制御棒が連続的に引き抜かれた後、ペリオド信号による制御棒引き抜き阻止及びスクラムが作動しないことを仮定
- 1ドルを超える反応度が投入され即発臨界となると、炉出力が急激に上昇かつ断熱的に燃料エンタルピが増大するおそれ

無許可・転載禁止

20

起動時引抜きの手順による反応度投入防止について

別添3（参考）

- 実際の起動手順

制御棒操作手順の作成

- ◆ 以下を満足する制御棒操作手順を作成
- 起動時異常な引抜事象の安全解析入力値に対応する設計目標値：
  制御棒グループ毎の最大反応度価値0.025dk
- 制御棒落下事故の安全解析入力値に対応する設計目標値：
  １本制御棒落下時の最大反応度価値0.010dk
  ※安全解析入力値に対して余裕を見込んだ設計目標値を設定
- **1回の制御棒操作により投入される反応度はペリオド100秒相当程度以下**

制御棒操作手順の遵守

- ◆ 制御棒の操作はあらかじめ定められた**制御棒操作手順に従って実施することが運転上の制限**（保安規定第23条）
  ロッドワースミニマイザ（RWM）で引き抜き手順を逸脱しないことを監視
- 制御棒操作手順に定める位置にないことを確認した場合は、速やかに当該制御棒を制御棒操作手順に定める位置に適合させる
- ◆ 臨界近接の制御棒操作にあたっては、**1回の制御棒操作毎に制御棒位置、SRNM指示、ペリオド、炉水温度、炉圧等を確認し、指示値が静定したあとに次の制御棒操作に移る手順としており、その旨手順書に定められている**

制御棒操作用プッシュボタンの操作

- ◆ また、操作は操作者、確認者、監視員など、**複数人による確認が行われる**
- ◆ 制御棒操作用ハードプッシュボタン「引抜」を離せば制御棒引抜は止まる

無許可・転載禁止

21

保安規定第２３条制御棒の操作

別添3（参考）

第23条　原子炉の状態が運転及び起動において、かつ原子炉熱出力10%相当以下の場合、制御棒の操作は、表23－1で定める事項を運転上の制限とする。

2. 制御棒の操作が前項で定める運転上の制限を満足していることを確認するため、次の各号を実施する。
（1）燃料GMは、原子炉の状態が運転及び起動で、かつ原子炉熱出力10%相当以下の場合における制御棒操作に先立ち、制御棒操作手順を作成し、主任技術者の確認を待て当直長に通知する。
（2）当直長は、原子炉の状態が運転及び起動において、かつ原子炉熱出力10%相当以下の場合は、制御棒価値ミニマイザを使用して、制御棒の操作を行う。
なお、制御棒価値ミニマイザが使用不可能な場合は、制御棒操作手順に従って操作されていることを確認するため、制御棒の操作を行う運転員の他に少なくとも1名の運転員を配置して、制御棒の操作を行う。
さらに、制御棒の操作の都度、制御棒操作手順に定める位置に適合させるように制御棒の操作を行うが、制御棒操作手順に定める位置にないことを確認した場合は、速やかに当該制御棒を制御棒操作手順に定める位置に適合させる。

3. 当直長は、制御棒の操作が第1項で定める運転上の制限を満足していないと判断した場合、表23－2の措置を講じる。

表23－1

項　目	運転上の制限
制御棒の操作	あらかじめ定められた制御棒操作手順に従って実施すること

無許可・転載禁止

22

保安規定第２３条制御棒の操作

別添3（参考）

表23－2

条　件	要求される措置	完了時間
A. 1本以上8本以下の制御棒を制御棒操作手順で定めた位置に適合させることができない場合	A1. 制御棒を制御棒操作手順で定めた位置に適合させる。*1	8時間
B. 条件Aで要求される措置を完了時間内に達成できない場合	B1. 当該制御棒を全挿入する。 及び B2. 当該制御棒駆動機構を除外する。	3時間 4時間
C. 条件Bで要求される措置を完了時間内に達成できない場合	C1. 高温停止にする。	24時間
D. 9本以上の制御棒を制御棒操作手順で定めた位置に適合させることができない場合	D1. 制御棒を制御棒操作手順で定めた位置に適合させる。*2	1時間
E. 条件Dで要求される措置を完了時間内に達成できない場合	E1. 原子炉をスクラムさせる。	速やかに

*1：制御棒操作手順で定めた位置に適合させる操作にあたっては、制御棒操作手順で定めた位置に適合させるための操作を除いて、制御棒の引き抜きを行ってはならない。
*2：制御棒操作手順で定めた位置に適合させる操作にあたっては、制御棒操作手順で定めた位置に適合させるための操作を含めて、制御棒の引き抜きを行ってはならない。

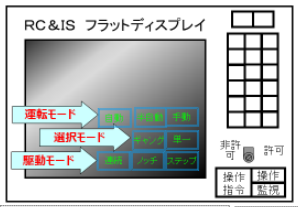
無許可・転載禁止

23

起動時引抜きの操作について

別添3（参考）

- 制御棒操作監視系（RC&IS）による制御棒操作



◆ ギャングモードを用いた通常の引抜手順
1. 選択モード「ギャング」タッチ選択
2. 操作指令ON
3. 運転モード「手動」or「半自動」タッチ選択
4. 操作指令ON
5. 駆動モード「連続」or「ノッチ」or「ステップ」タッチ選択（制御棒操作手順に従う）
6. [手動モードの場合]操作する制御棒を選択（制御棒操作手順に従う）
7. 操作指令ON
8. 制御棒操作用PB「引抜」を押す

◆ 運転モード
- 手動：制御棒の選択及び引抜/挿入操作を全て運転員が行う
- 半自動：予め登録された制御棒引抜シーケンスに基づいて制御棒の選択は自動的に行われるが、引抜/挿入操作は運転員が手動で行う
- 自動：APRに基づいて制御棒の選択及び引抜/挿入操作が自動的に行われる

◆ 選択モード
- 単一：制御棒1本のみを選択し、駆動する
- ギャング：予め定められたギャンググループ単位で制御棒を選択し、駆動する

◆ 駆動モード
- ステップ：1回の操作で1ステップの引抜／挿入を行う
- ノッチ：1回の操作で1ノッチ（4ステップ分）の引抜／挿入を行う
- 連続：連続的に引抜／挿入を行う

無許可・転載禁止

24

線量影響（主蒸気管破断、燃料集合体の落下）

参考1

主蒸気管破断

- 追加放出（燃料破損なし）を想定
- 全量が気相（環境）へ移行と仮定
- 現実的ｆ値 （希ガス漏えい率）：許認可使用値の1/10［近年の平均値の場合更に低減］

		従来許認可のｆ値	現実的ｆ値
有機よう素による内部被ばく	[mSv]	8.99 e-2	8.99 e-3
無機よう素による内部被ばく	[mSv]	2.24 e+1	2.24 e+0
希ガスによる外部被ばく	[mSv]	2.58 e-1	2.58 e-2
合計	[mSv]	2.27 e+1	2.27 e+0

燃料集合体の落下

- 破損本数、プール水によるDF 等は許認可解析と同一［当該保守性は今回排除せず］
- SGTS不作動（地上放出）
- SGTS不作動時の建屋換気率（0.5回/d）［あて換気があるとの保守的仮定］

		従来許認可条件	SGTS不作動
よう素による内部被ばく	[mSv]	1.89 e-4	1.89 e+0
希ガスによる外部被ばく	[mSv]	4.11 e-2	4.11 e-2
合計	[mSv]	4.13 e-2	1.93 e+0

➡
- 代表サイトにおける現実的評価条件（f値1/10等）においては、概ね判断基準を超えることない
- サイト条件によっては結果が厳しくなるものの影響は限定的であり、また、更なる現実的条件適用による低減可
- インベントリを事故解析より引き継ぐが、CCF対策は炉心損傷防止に重点を置くことで、影響拡大は限定的となる

無許可・転載禁止

25

添付資料　2

PWRにおけるデジタル安全保護回路の
ソフトウェアCCFを前提とした影響評価
（予備評価結果）について

1

PWRにおけるデジタル安全保護回路のソフトウェアCCFを前提とした影響評価（予備評価結果）について

関西電力株式会社
三菱重工業株式会社

ディジタル安全保護設備共通要因故障（CCF）のPWRプラントの影響評価と対策

2

- PWRプラントでは、ディジタル更新したディジタル安全保護設備には、共通要因故障（ディジタルCCF）を想定し、CCF対策設備を自主設置している。
- 今般、ディジタルCCFに関する規制化の方針を受け、要求事項のうち、設置(変更)許可申請書 添付書類十で取り扱う運転時の異常な過渡変化及び設計基準事故の全事象に対して、ディジタルCCFの影響評価を実施し、必要な対応をスクリーニングする。

1(1). ディジタルCCF対策評価の想定事象・判断基準・前提条件

3

PWRプラントとして、対象としている事象、判断基準、前提条件を以下に整理する。

項　目		内　容
対象事象	運転時の異常な過渡変化	設置(変更)許可申請書添付書類十で評価対象としている全事象 1. 原子炉起動時における制御棒の異常な引き抜き 2. 出力運転中の制御棒の異常な引き抜き 3. 制御棒の落下及び不整合 4. 原子炉冷却材中のほう素の異常な希釈 5. 原子炉冷却材流量の部分喪失 6. 原子炉冷却材系の停止ループの誤起動 7. 外部電源喪失 8. 主給水流量喪失 9. 蒸気負荷の異常な増加 10. 2次冷却系の異常な減圧 11. 蒸気発生器への過剰給水 12. 負荷の喪失 13. 原子炉冷却材系の異常な減圧 14. 出力運転中の非常用炉心冷却系の誤起動
	設計基準事故	設置(変更)許可申請書添付書類十で評価対象としている全事象 1. 原子炉冷却材喪失 2. 原子炉冷却材流量の喪失 3. 原子炉冷却材ポンプの軸固着 4. 主給水管破断 5. 主蒸気管破断 6. 制御棒飛び出し 7. 蒸気発生器伝熱管破損

1(2). ディジタルCCF対策評価の想定事象・判断基準・前提条件

4

PWRプラントとして、対象としている事象、判断基準、前提条件を以下に整理する。

項　目		内　容
判断基準		設計基準事故に対応した判断基準
前提条件	安全保護回路	ディジタルCCFにより機能喪失
	プラント状態	現実的条件
	単一故障	仮定無し
	外部電源喪失	起因事象(外部電源喪失)以外は仮定無し
	サポート系 (冷却系・空調系等)	起因事象が発生する前の作動状態を維持
	運転操作	CCF対策設備の作動を起点として、中央制御室でのCCF対策盤及び現場での操作に期待する。

1(3). PWRプラントのディジタルCCF対策設備の機能

5

影響評価で想定するCCF対策設備の機能を整理する。

項　目	主要な機能　黒：現行　赤：追加
自動作動系	・原子炉トリップ「原子炉圧力(加圧器圧力)低, 原子炉圧力(加圧器圧力)高, 蒸気発生器水位異常低」 ・タービントリップ ・主給水隔離 ・主蒸気隔離 ・補助給水起動 ・高圧／低圧注入系起動「原子炉圧力(加圧器圧力)異常低」
警報・監視系	・バックアップ設備作動 ・加圧器圧力低（原子炉トリップ等） ・加圧器圧力高（原子炉トリップ等） ・蒸気発生器水位低（原子炉トリップ等） ・蒸気発生器水位異常高 ・加圧器圧力異常低（高圧／低圧注入系作動） ・中間領域中性子束 ・加圧器圧力 ・１次冷却材圧力 ・１次冷却材低温側温度（広域） ・加圧器水位 ・主蒸気ライン圧力 ・蒸気発生器水位（狭域） ・格納容器圧力 ・蒸気発生器２次側放射線 ・対象補機の状態
操作系	・原子炉トリップ／タービントリップ／主給水隔離／主蒸気隔離 ・安全注入（高圧） ・格納容器隔離 ・加圧器逃がし弁 ・補助給水隔離及び流量調節 ・主蒸気逃がし弁

2. 運転時の異常な過渡変化のディジタルCCF影響評価

6

- 「異常な過渡変化」において、原子炉トリップ機能が喪失すると、重大事故等への対処に係る措置の有効性評価の「原子炉停止機能喪失（ATWS）」のシーケンスとなる。
- 有効性評価において、原子炉冷却材圧力バウンダリの健全性確保の観点で厳しくなる「主給水流量喪失時に原子炉トリップ機能が喪失する事故」及び「負荷の喪失時に原子炉トリップ機能が喪失する事故」を重要事故シーケンスとして選定し、原子炉トリップできない状況でも、ＡＴＷＳ緩和設備によって、本２シーケンスが、圧力バウンダリ及び燃料損傷の観点で問題ないことを評価している。
- 「異常な過渡変化」発生時に、安全保護回路のディジタルCCFにより原子炉トリップ機能が喪失した場合でも、現行のCCF対策設備には原子炉トリップ機能を備えており、原子炉トリップできることから、ATWSのシーケンスよりも緩和され、圧力バウンダリ及び燃料損傷の観点で問題ない評価となる。

	添付書類十解析 (安全解析)	ATWS解析 (有効性評価解析)	ディジタルCCF解析
対象事象	「異常な過渡変化」全事象	←	←
緩和手段	原子炉トリップ（自動, 安全保護系） 補助給水（自動, 安全保護系）	主蒸気隔離（自動, ATWS対策設備） 補助給水（自動, ATWS対策設備）	原子炉トリップ（自動, CCF対策設備） 補助給水（自動, CCF対策設備）
評価条件	保守的条件	現実的条件： 減速材温度係数 -13pcm/℃	←
判断基準	異常な過渡変化の判断基準	基準37条の第１の要件（炉心損傷防止）を概ね満足すること	基準第１３条 第２号の要件（設計基準事故）を概ね満足すること

異常な過渡変化に対しては、現行のCCF対策設備で対応可能

3.設計基準事故のディジタルCCF影響評価

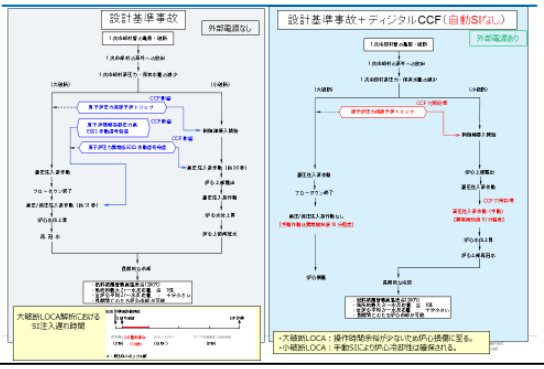
7

事故事象名	影響評価 (補足-1)
原子炉冷却材喪失	現行CCF対策設備の手動による安全注入では大破断LOCAにおいて判断基準は満足できないものの、CCF対策設備により安全注入を自動で作動させることにより、判断基準を概ね満足する。 なお、格納容器に関しても、現場での手動操作により格納容器スプレイを作動させることにより、判断基準を概ね満足する。
原子炉冷却材流量の喪失	現行のCCF対策設備による原子炉トリップ、及び現実的な反応度挿入効果により、判断基準を概ね満足する。
原子炉冷却材ポンプの軸固着	同上
主給水管破断	同上
主蒸気管破断	現行のCCF対策設備による主蒸気隔離、及び現実的な制御棒状態の想定により、判断基準を概ね満足する。
制御棒飛び出し	現行のCCF対策設備による原子炉トリップ、及び現実的な事故想定により、判断基準を概ね満足する。
蒸気発生器伝熱管破損	現行のCCF対策設備による原子炉トリップ、並びに漏洩停止までの必要な手動操作をCCF対策設備等で対応することにより、漏洩量は事故解析と同等であり、判断基準を概ね満足する。

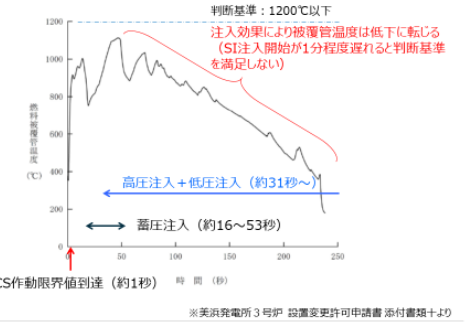
事故に対しては、安全注入機能の自動化により、大中破断LOCA含め対応可能

補足-1 事故のCCF対策評価 「原子炉冷却材喪失」(ECCS性能評価)(1/2)

8



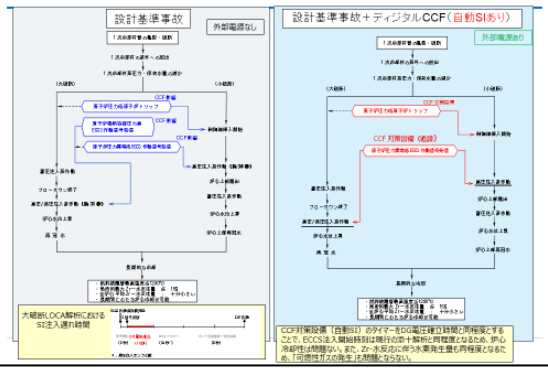
補足-1「原子炉冷却材喪失（ECCS性能評価［大破断］）」の解析例※ 9



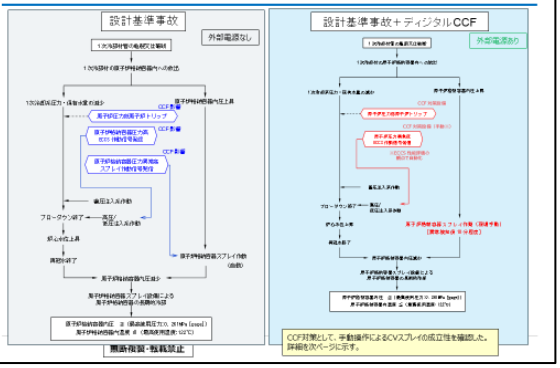
※美浜発電所３号炉 設置変更許可申請書 添付書類十より

無断複製・転載禁止

補足-1 事故のCCF対策評価 「原子炉冷却材喪失」（ECCS性能評価）（2/2） 10



補足-1 事故のCCF対策評価 「原子炉冷却材喪失」（CV健全性評価） 11



無断複製・転載禁止

補足-1「原子炉冷却材喪失（CV健全性評価）」の解析例（1/2） 12

対象プラント：美浜３号機

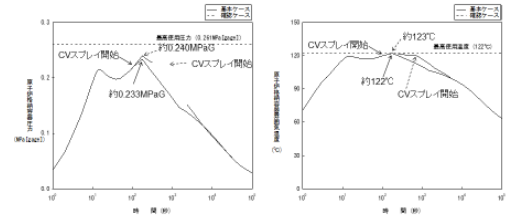
	CVスプレイ開始時間	解析結果		
		最高圧力	最高温度	判定
基本ケース（添十）	108秒	約0.233MPa[gage]	約122℃	最高圧力<0261MPa[gage] 最高温度<122℃
確認ケース	706秒（基本ケース+10分）	約0.240MPa[gage]	約123℃	最高圧力<0261MPa[gage] 最高温度>122℃

（補足）
・手動によるCVスプレイ開始遅れを、添付書類十解析から＋10分と設定した。
・解析には従来許認可コードを使用。
・CCF対策設備では、１系列の高・低圧注入が自動作動する設計であるが、今回、添付書類十解析同様に、保守的に２系列の高・低圧注入を想定した。

（解析結果）
・手動スプレイ操作を仮定した場合、判断基準(最高圧力、最高温度)を概ね満足する結果。
・なお、有効性確認の評価項目であるCV圧力（2Pd(=0.522MPa[gage]））及びCV温度（200℃）に対して十分下回る。

無断複製・転載禁止

補足-1「原子炉冷却材喪失（CV健全性評価）」の解析例（2/2） 13

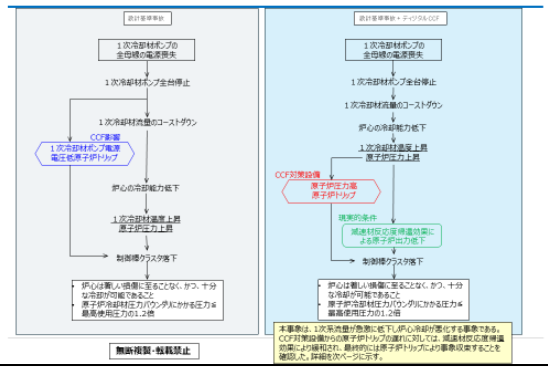


原子炉格納容器圧力　　原子炉格納容器雰囲気温度

CCF対策として手動によるCVスプレイにより、CV内圧及びCV雰囲気温度は添付書類十解析と同等となり、判断基準を概ね満足する。CV壁表面についても同等となることから、熱ばくについても問題とならない。

無断複製・転載禁止

補足-1 事故のCCF対策評価 「原子炉冷却材流量の喪失」 14

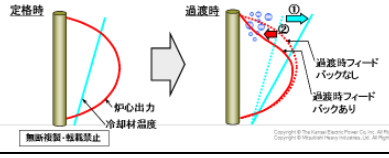


無断複製・転載禁止

補足-1「原子炉冷却材流量の喪失」の解析例（1/2） 15

	添付書類十解析	CCF解析
原子炉トリップ	安全保護系による原子炉トリップ（電源電圧低）	CCF対策設備による原子炉トリップ（原子炉圧力高） ※ 安全保護系による原子炉トリップは不作動 ※ 設定値には計装誤差を考慮し、タイマー＋信号遅れとして12秒を仮定
減速材温度係数	0pcm/℃	-13pcm/℃（ATWS解析と同じ）
局所フィードバック効果(注)	考慮しない	考慮する
その他	－	添付書類十解析と同じ

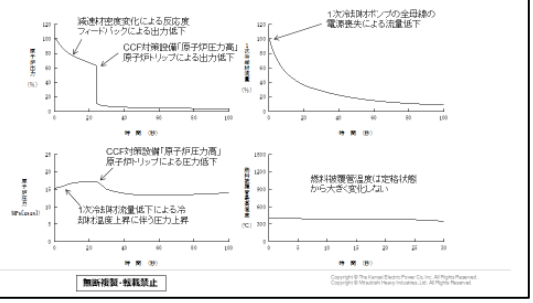
注 SA有効性評価で使用しているSPARKLE-2では、出力上昇や冷却材流量低下などにより、炉心上部の冷却材温度が上昇（①）すると、減速材フィードバック効果により出力分布が抑制される（②）とともに、出力が低下する。



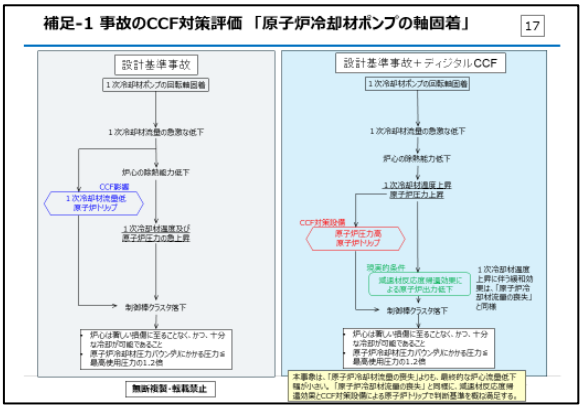
無断複製・転載禁止

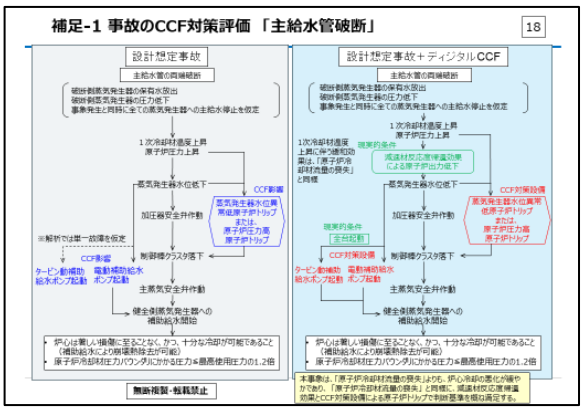
補足-1「原子炉冷却材流量の喪失」の解析例（2/2） 16

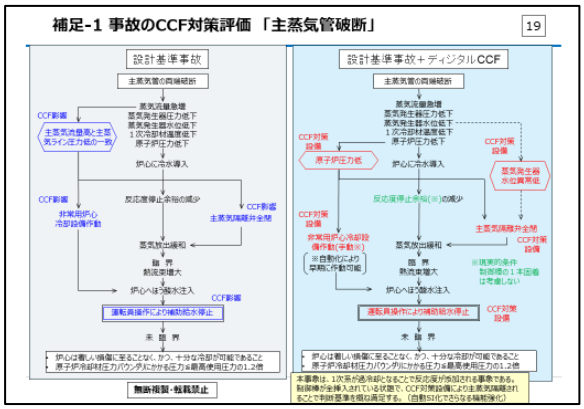
・SPARKLE-2コードを用いた解析例を以下に示す。
・減速材密度変化による反応度フィードバックの効果により出力が低下。燃料被覆管温度は定格状態から大きく変化しない。

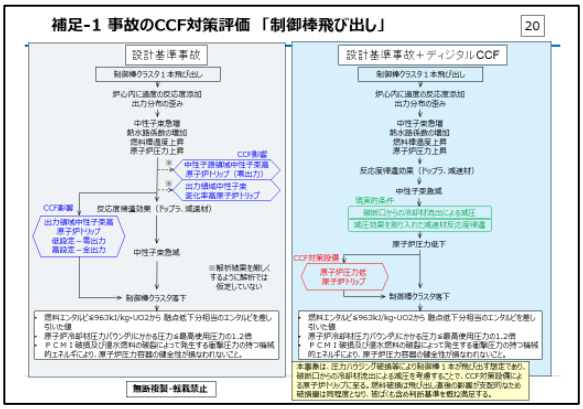


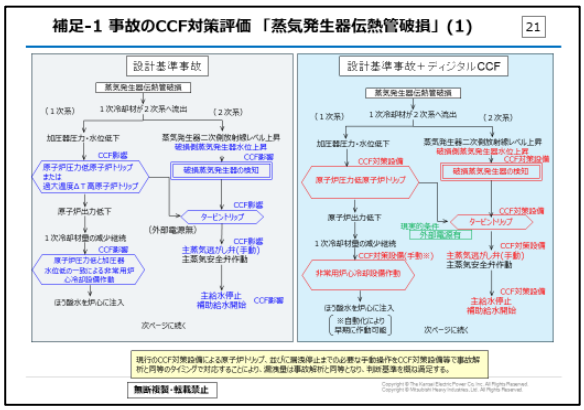
無断複製・転載禁止

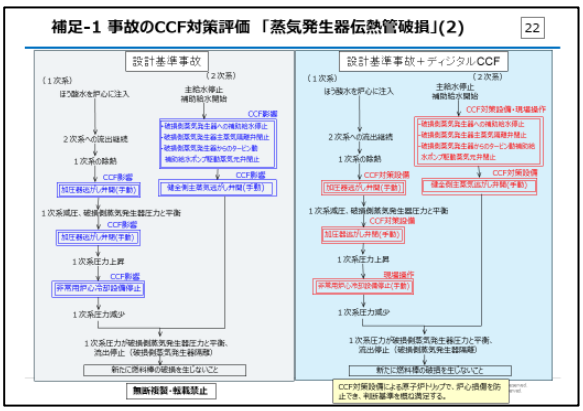












発行者　：原子力エネルギー協議会

問合せ先：contact@atena-j.jp