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

2020 年××月××日
原子力エネルギー協議会

【はじめに】

原子力発電所においては，信頼性向上や保守性の向上を目的として 1980 年代頃から常用系にデジタル計算機が適用され，その良好な運転実績を踏まえ，1990 年代頃から安全保護回路にもデジタル計算機が適用され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，「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）や「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）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が実施されてきた。

これらの活動により，ソフトウェアの共通要因故障（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が，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。

一方，2019 年 10 月 2 日の第 33 回原子力規制委員会において，「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，「検討チーム」と言う。）が設置され，ソフトウェア CCF 緩和対策の規制化に関する議論が進められてきた。原子力エネルギー協議会（以下，「ATENA」という。）では，検討チームにおける議論や国際水準を踏まえ，運転時の異常な過渡変化又は設計基準事故の発生時にソフトウェア 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 緩和対策として炉心損傷防止を重視し，更なる対策を自主的に且つ計画的行うことを 2020 年 1 月の ATENA のステアリング会議※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 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 緩和対策を自主的に整備し，ATENA は事業者の活動状況の確認を行い，対策の確実な実施をフォローしていく。

また，ATENA は，海外動向なども参考にしながら，今後もソフトウェア CCF 緩和対策の技術的検討を継続し，新知見が得られた場合は，必要な対応を進める。

※ ステアリング会議とは，ATENA 会員の責任者クラスが委員として参加する会議体。なお，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。

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（「ATENA 関係者」）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（「本件知的財産権」）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●月●日	初版	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 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，手順書の整備や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など，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ハードウェア信頼性が確保されている。

また，デジタル安全保護回路のソフトウェアについても，品質保証活動や検証及び妥当性確認に加え，1度に1つのタスクのみ実行するシングルタスク処理や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と，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など，十分に高い信頼性が確保されており，ソフトウェアに起因した共通要因故障の発生は十分低く抑えられている（参考資料1）。しかし，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，同一のプラットフォームの使用下において，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の発生時にデジタル安全保護回路のソフトウェア 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。2020 年 1 月 29 日の検討チーム公開会合において，事業者は，自主設置していた多様化設備に，安全系の自動起動や警報を追加することにより，運転時の異常な過渡変化又は設計基準事故 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（参考資料1　第4回検討チーム公開会合）。

本技術要件書に，検討チームでの議論や米国でのソフトウェア CCF 緩和対策要求を参考に，多様化設備への要求事項やその有効性評価手法，ならびに手順書整備と教育の実施要求について記載する。

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 緩和対策を自主的に整備し，ATENA は事業者の活動状況の確認を行い，対策の確実な実施をフォローしていく。（添付資料1）

1.3 適用範囲

デジタル安全保護回路のソフトウェア CCF 緩和対策に適用する。

1.4 用語の定義

- デジタル計算機
  内蔵されたプログラムによって制御され，人手の介入なしにデジタルデータの算術演算や論理計算等の計算を行う装置を言う。

- 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設備を言う。 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または一部を作動させるものを言う。

- 設定値比較機能
  既定の設定信号値と検出した信号値を比較する機能のことを言う。

- 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ロジックで，原子炉停止系統や工学的安全施設の機器を動作させる，また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言う。

- 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言う。 ソフトウェアには，入出力の制御やハードウェアの管理など，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（OS），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やデータ設定などがある。

- ソフトウェア共通要因故障，ソフトウェア CCF（CCF；Common Cause Failure）
  ソフトウェアの不具合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する状態を言う。

- 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，デジタル安全保護回路の代替機能として，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的に，または手動により作動させる設備を言う。

- サポート系
  機器や系統の性能を発揮するのに必要となる電源系，空調系，冷却系などの設備系統を言う。

- 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オペレーティングシステム(OS)やアプリケーションソフトウェアとデータベースとのやり取りを管理するミドルウェアなどをプラットフォームと言う。

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の発生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（設定値比較機能，論理演算機能）とする。図 1 にソフトウェア CCF を想定する範囲の例を示す。

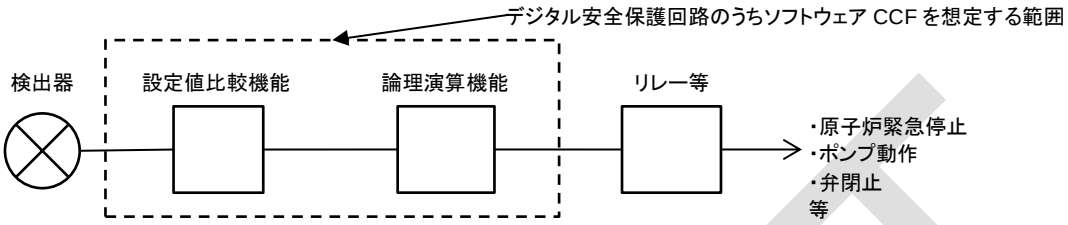


図1：安全保護回路のうちソフトウェア CCF を想定する範囲（例）

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，運転時の異常な過渡変化又は設計基準事故が発生し安全保護回路の自動作動が要求されたときに，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，原子炉停止系統や工学的安全施設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，それ以前に起動し運転中のポンプなどの機器については，ソフトウェアCCFの影響を受けず機器の作動状態に変化は生じないものと想定する。

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。

但し，ソフトウェアに起因する共通要因故障が発生するおそれがない場合，また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多様化設備を用いることなく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良い。

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的に，または手動により作動させることができること。

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，運転員が判断基準を概ね満足した状態で事象を収束させるために必要な時間内に操作を開始できるよう，運転時の異常な過渡変化又は設計基準事故時に安全保護動作の異常の発生認知し，必要な操作の判断を行える機能を設けること。

3.3 多様化設備の範囲

多様化設備の範囲は，3.2 に示す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・警報などの計測制御設備とする（図2）。

ここで，上記の構成要素は，3.5 に示す各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 緩和対策として設けた以外の設備でも多様化設備として資することができるものとする（例　安全保護回路の検出器や操作スイッチ，重大事故等対処設備など）。

なお，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，どの設備を選定したか明確にすること。

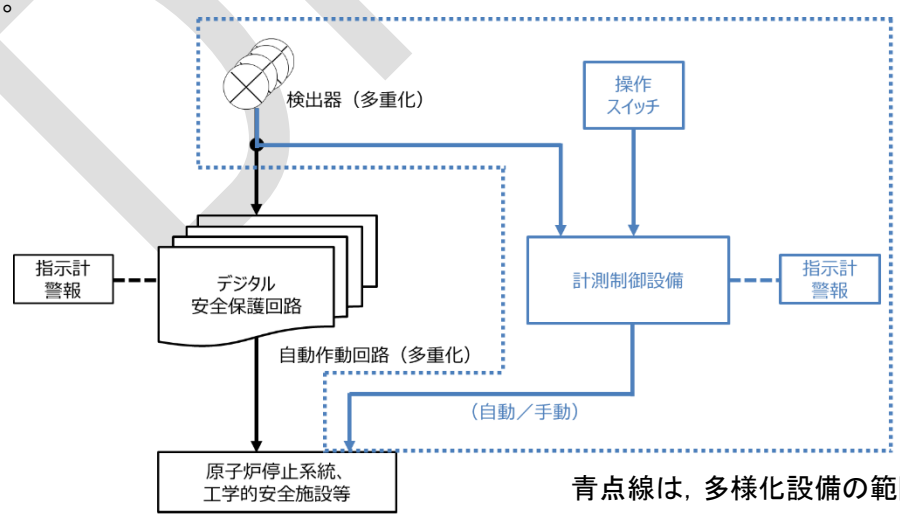


図2　多様化設備の範囲

3.4 設計基本方針

多様化設備は，設計基準事故対処設備や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に鑑み適切と考えられる設計方針を以下に定める。

デジタル安全保護回路は，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（参考資料2 第1回検討チーム公開会合および第3回検討チーム公開会合），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，ソフトウェアに起因する共通要因故障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とみなすことができる。従って，多様化設備の設計においては，単一故障，及び起因事象として溢水・火災などの内部事象又は外部事象により発生する事象を想定しない。

多様化設備は，ソフトウェア CCF 発生時のデジタル安全保護回路を代替する設備としての位置づけであることから，耐環境性，耐震性，供給電源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

多様化設備は，ソフトウェアを用いたデジタル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，アナログ設備など，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無いものを言う。

また，多様化設備に用いられるソフトウェアとデジタル安全保護回路に用いられるソフトウェアとが，そのプログラムに不具合が共通して内在する可能性がないこと，その他ソフトウェア CCF が生ず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される設計とすること。

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喪失に波及しない設計とすること（参考資料３　第３回検討チーム公開会合）。

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），人為による事象及び蒸気タービン，ポンプその他の機器又はまたは配管の損壊に伴う飛散物等に対して，多様化設備が影響を受けても，それが安全機能の喪失に波及し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。
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された設備はこの限りではない。
また，誤操作防止を考慮した設計とすること。（例　盤の配置，計器表示及び警報表示において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）

3.5.12 監視性

多様化設備のうち自動作動系が動作した場合には，その動作原因が原子炉制御室に表示される設計とすること。
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デジタル安全保護回路のソフトウェア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に必要な監視設備を原子炉制御室に設けること。

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」にデジタル安全保護回路のソフトウェアCCF が重畳した場合でも，3 章に示す設備要件を満たす多様化設備等により，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，かつ，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，設置（変更）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」又は「設計基準事故」全事象について解析し評価を行っている。したがって，本有効性評価でも，「運転時の異常な過渡変化」又は「設計基準事故」全事象を対象とすること。

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グルーピング（参考資料1　第4回検討チーム公開会合）してもよい。また，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に期待しない事象について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

有効性評価は，「運転時の異常な過渡変化」及び「設計基準事故」とソフトウェア CCF が重畳する事象に対し，ソフトウェア CCF 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が目的であるため，「運転時の異常な過渡変化」及び「設計基準事故」いずれに対しても判断基準は，設計基準事故（「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」第十三条第二項）において使用される判断基準を準用し，設計基準事故の判断基準が概ね満足されることの確認を行う。なお，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・温度等の条件や，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 に示したとおり，運転中の異常な過渡変化又は設計基準事故とソフトウェア CCF が重畳発生する事象は，設計基準を超える事象と見なすことができるため，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を適用することはせず，重大事故等対策の有効性評価（以下，「SA 評価」という。）のような最適評価を基本的な考え方とする。すなわち，プラント初期条件及び機器の作動状態の想定などについては最適評価条件を考慮し，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。

ただし，ソフトウェア CCF を仮定した場合においても，解析評価結果が判断基準に対して余裕があり，最適評価を適用する必要がないと判断できる場合は，保守的な条件設定のままでもよい。

4.4.1 解析に当たって考慮する範囲

有効性評価を行うに当たっては，異常状態の発生前の状態として，通常運転範囲及び運転期間の全域について考慮し，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

最適解析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状態（出力，圧力，温度，水位，流量，機器の作動状態など）は，設計値等に基づく現実的な運転条件としても良い。 その場合，許認可解析における前提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，炉心状態，機器の容量などは，設計値等に基づく現実的な値を用いる。その場合，許認可解析における前提条件との差異及び根拠を明確にすること。

（BWR の例）
制御棒の異常な引き抜き及び制御棒落下の反応度投入事象において使用する制御棒価値は，現実的な炉心設計を前提とした条件を想定する。

4.4.3 安全機能に対する仮定

ソフトウェア CCF 発生時の安全保護回路，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もしくは手動起動信号で，原子炉停止系統及び工学的安全施設は作動可能（4.5.5 多様化設備に関連する条件参照）。
- 最適評価を行う観点から，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）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の仮定とする。

- 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。
- 事象発生前から機能しており，かつ，事象の過程中も機能し続ける設備は，故障の仮定から除外可能。
- 常用系機能の喪失が，起因となる事象の前提である場合は，当該事象を評価する際にはその機能には期待しない。

4.4.5 多様化設備に関連する条件

（1）機器条件

- 多様化設備の有効性を確認する観点から，多様化設備の単一故障は想定しない。また，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や誤動作が起因となる事象は想定しない。
- ソフトウェア CCF により安全保護回路は機能喪失するが，原子炉停止系統，工学的安全施設等は利用可能であり，多様化設備が代替作動することができる。ただし，想定する起因事象及びCCFが発生した状態においても，多様化設備のサポート系（電源系，冷却系，空調系等）が利用可能であることを確認すること。

（2）操作条件

- 運転員による手動操作は多様化手段の一部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，原子炉制御室において運転員の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，運転訓練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は現実的な想定を前提としてもよい（設計基準事象の評価で想定している運転員操作に対する時間的余裕（いわゆる「10 分ルール」）を考慮する必要はない）。その場合，運転操作開始時間の根拠を明確にすること。
- 原子炉制御室外における現場操作を考慮してよい。その場合においては，運転員による事象の認知から現場操作箇所までの移動時間，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，モデル

（1）最適評価を行う際に必要に応じて，ベストエスティメイトコード[1]を使用しても良い。
（2）現実的な計算モデル（例：崩壊熱モデルにおいて，設計基準事故解析で使用しているGE+3σ式（無限照射）ではなく，ANSI/ANS-5.1-1979 式などを用いる）を使用しても良い。
（3）使用する計算プログラムは，本評価の範囲が適切に評価できることの確認（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確認ができる場合は妥当性確認及び検証は不要である。

[1]想定する事象を現実的に予測できるコード。

5. 手順書整備と教育

5.1 手順書整備

運転時の異常な過渡変化又は設計基準事故が発生し，デジタル安全保護回路に期待される原子炉停止系統や工学的安全系施設が作動していないことが確認された場合，その要因がソフトウェア CCF の重畳発生によることを認知し，原子炉停止系統や工学的安全系機能を動作させたうえ，事象を収束させることができるよう，必要な手順書を適切に整備すること。

5.2 教育及び訓練の実施

運転員には，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にソフトウェア CCF が重畳発生した場合において，的確に対処できるよう，教育および訓練を適切に計画し，計画通りに実施すること。

添付資料 1 対応状況確認プロセス

1．産業界としての基本方針

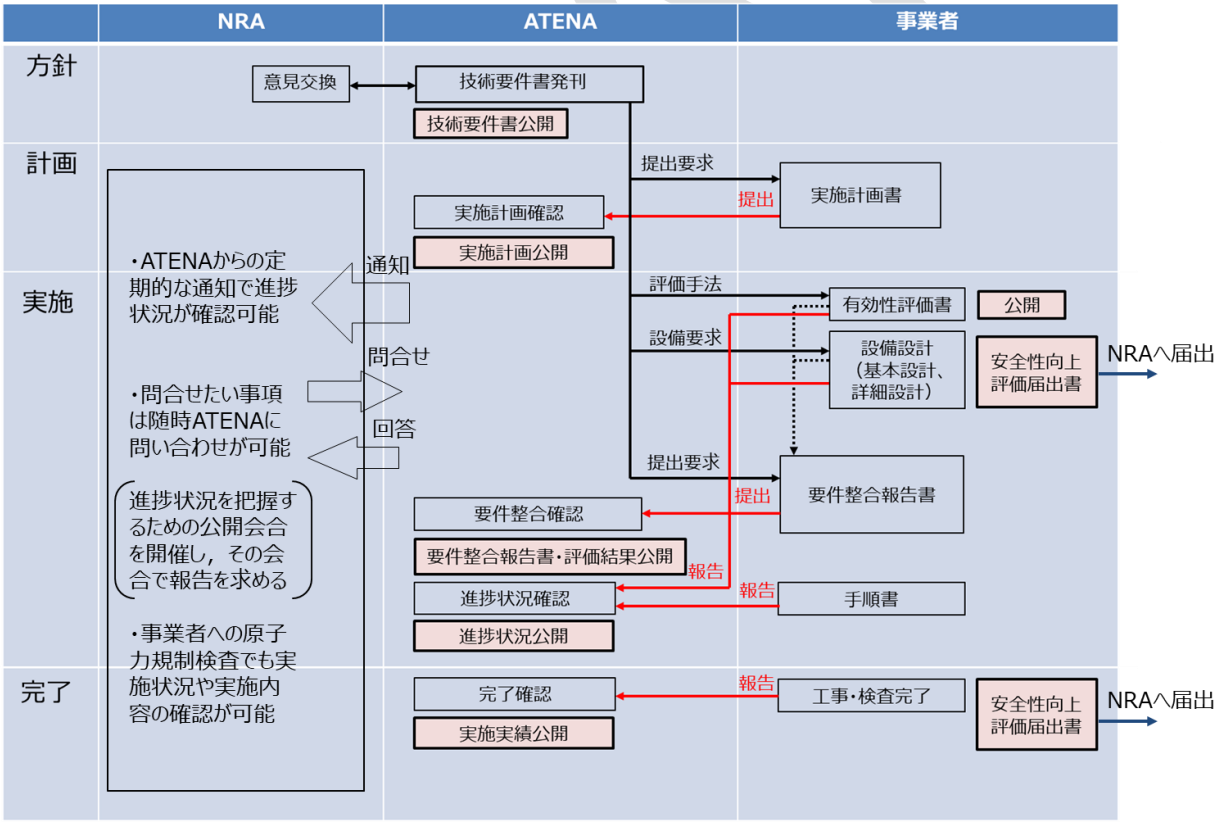
（1）事業者は，ATENA ステアリング会議でコミットした「デジタル安全保護回路のソフトウェア CCF 対策」を，責任を持って自律的かつ計画通りに実施する。

（2）ATENA は，有効性評価手法や設備設計要求を明確にした技術要件書を発刊し，事業者に提示するとともに，事業者に対して以下の対応を求める。
実施計画書の提出
有効性評価書の公開
要件整合報告書の提出
進捗状況の報告（半期に一度）

（3）事業者は，（2）の対応を行うとともに，対策の計画および対策が完了の時点で安全性向上評価届出書を原子力規制委員会（NRA）に提出する。
なお，再稼働前のプラントについては実施計画書の ATENA への提出をもってこれに替えることを検討中。

（4）ATENA は，技術要件書，実施計画，要件整合報告書および ATENA の確認結果，実施実績を HP に公開する。
NRA には，半期に一度進捗状況を報告する。また，NRA から公開情報に関する問合せがあれば回答すると共に，進捗状況を把握するための公開会合が開催される場合には，その場で報告する。

（5）ATENA と事業者は，WG 等を通じて対策実施状況や良好事例等の情報共有を継続して行う。



2. 進捗状況確認の具体的方法

(1)事業者は，対策内容および下記プロセス※の完了予定時期を示した実施計画書を ATENA に提出する。
※「有効性評価」,「基本設計」,「詳細設計」,「要件整合報告」, 「手順書整備」,「工事・検査」

(2)ATENA は，実施計画書を確認後，HP に公開する。

(3)事業者は，半期に一度，それぞれのプロセス※の進捗状況を，ATENA に報告する。
事業者は，計画通りに実施できない場合には，その理由を付して報告し，ATENA は HP で公開する。

(4)ATENA は，半期に一度，確認した状況について NRA に報告する。
また，NRA から公開情報に関する問合せがあれば回答すると共に，進捗状況を把握するための公開会合が開催される場合には，その場で報告する。

3. 要件整合確認の具体的方法

(1)事業者は，許認可や設工認での図書承認プロセスと同等のプロセスの下で要件整合報告書(参考3)を取り纏め，原子力本部長の責任の下，ATENA に提出する。

(2)ATENA は，事業者の要件整合報告書が下記の観点で作成されていることを確認する。
技術要件の各項目について，設計仕様や解析条件等が網羅性をもつ小項目に細分化されていること。
細分化された各項目について，根拠となる設計図書における具体的な記載内容，要件整合判定およびその理由，並びに設計図書名および記載場所が明確に記載されていること。

(3)ATENA は，事業者の要件整合報告書およびその確認結果を HP で公開する。

(4)ATENA は，先行 PWR/BWR 事業者の協力を得て要件整合報告書のひな型を作成し，後続プラントに標準適用できるように共有する。

参考資料1 第4回 検討チーム公開会合資料

後報

参考資料2 第1回 検討チーム公開会合資料

後報

参考資料3 第3回 検討チーム公開会合資料

後報

※ 第2回については，セーフティとセキュリティのインターフェイスに関する非公開の会合のため資料等は原子力規制委員会に掲載されない。

参考資料4 グルーピングの考え方

「4．2　評価すべき事象」におけるグルーピングの考え方（例）

＜BWR のグルーピングの例＞
「原子炉停止」，「炉心冷却」及び「放射能閉じ込め」の各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，原子炉圧力高信号また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または投入事象と，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または投入事象である，制御棒落下と制御棒の異常な引き抜きは，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以降の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。

（放射能閉じ込め）
放射能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），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。
【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，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
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や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，FCS手動起動など）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】