資料２－１

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の変更箇所について

2021年3月26日
原子力エネルギー協議会

目 次

1．はじめに

（１） 技術要件書の発刊

2020年12月24日に「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」を発刊。

（２） 変更の概要

令和２年10月の公開会合で本技術要件書のドラフト版を提示し、その後下記の変更を加え最終版とした。

- 本文については、主に表現の適正化を行った。
- 各節ごとに解説(具体例、要求した理由、要求しなかった項目とその理由など)を追加。
- ６章に対策例を、添付書類１に多様化設備例を追加。
- ７章に参考文献を追加。

（３） 今後の改定について

- 有効性評価・設備詳細設計などの進捗に伴い、例示箇所等の更新を行う。
- 海外動向を注視し、新知見が得られた場合に反映の要否を検討し、必要に応じて改定を行う。

2．技術要件書の目次

技術要件書作成の経緯・位置づけを記載

CCFの定義を記載

設備要求を記載

有効性評価手法への要求を記載

手順書整備と教育訓練の要求を記載

予備評価に基づく多様化設備例を記載

（注）変更箇所を朱記

3．技術要件書変更内容の概要（1/14）

2．ソフトウェアCCFについて	概要(表現適正化を除く変更箇所を朱記)	解説
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。	・（例１）中性子計装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を記載。 ・（例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を記載。
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。	・「誤作動信号が出力される場合を故障モードとして想定しない」理由を記載。 ・「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」理由を記載。 ・「機器の作動状態の変化は想定しない」理由を記載。

3. 技術要件書変更内容の概要（2/14）

3.多様化設備要件	概要(表現適正化を除く変更箇所を朱記)	解説
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，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よい。	・「ソフトウェアCCFが発生するおそれがない場合」を解説。 ・「ソフトウェア自身が多様性を有している」を解説。 ・「多様化設備を設けなくてもよい」を解説。また、BWRで中性子計装にデジタル技術を適用した例を記載。

3. 技術要件書変更内容の概要（3/14）

3.多様化設備要件	概要(表現適正化を除く変更箇所を朱記)	解説
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，又は手動で作動できなければならない。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又は設計基準事故時に安全保護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。	・「設計基準事故の判断基準を概ね満足できる」を解説。 ・「必要な時間内」を解説。

3. 技術要件書変更内容の概要（4/14）

3.多様化設備要件	概要(表現適正化を除く変更箇所を朱記)	解説
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。	・「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」理由を記載。
3.4 設計基本方針	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、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，多様化設備には，単一故障や溢水・火災あるいは外的影響（地震を除く）とソフトウェアCCFの重畳を考慮しない。	・「デジタル安全保護回路が十分に高い信頼度でソフトウェア設計がなされている」理由を記載。 ・「多様化設備が，重要度分類には該当しない」理由を記載。
3.5.1 多重性	多様化設備には，多重性は要求しない。	・「多様化設備に多重性は要求しない」理由を記載。

3．技術要件書変更内容の概要（5/14）

3.多様化設備要件	概要(表現適正化を除く変更箇所を朱記)	解説
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。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。	・「多様化設備そのものには多様性は要求しない」理由を記載。 ・「多様化設備にソフトウェアを適用することができる」を解説。 但し、多様化設備に適用するデジタル技術の要件は今後検討すると記載。
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。	・「多様化設備に基準地震動Ss機能維持を要求する」理由を記載。
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。	・「多様化設備に外部電源によらずとも機能を発揮できることを要求する」理由を記載。

ATENA Atomic Energy Association

3．技術要件書変更内容の概要（6/14）

3.多様化設備要件	概要(表現適正化を除く変更箇所を朱記)	解説
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。	・多様化設備に，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ことを要求する理由を記載。
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。	・多様化設備に，運転中の試験を必ずしも要求しないことの理由を記載。 ・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	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を喪失させない設計とすること。	・多様化設備により安全保護機能を喪失させない具体例を記載。
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を喪失させない設計とすること。	・火災・溢水に対する多様化設備と安全保護回路の設計要求を解説。 ・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理由を記載。

3．技術要件書変更内容の概要（7/14）

3.多様化設備要件	概要(表現適正化を除く変更箇所を朱記)	解説
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。	・「想定される自然現象（地震を除く）」を解説。 ・「人為による事象」を解説。 ・「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」を解説。
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。	・「多様化設備の誤操作防止を考慮した設計」例を記載。 ・「切替スイッチを設ける場合」の例を記載。 ・「指示計及び警報」に対する考慮事項を記載。 ・「原子炉制御室以外に設置する場合」の条件を記載。
3.5.12　監視性	多様化設備が自動で作動した場合には，その作動原因が原子炉制御室に表示される設計とすること。	・「警報及び監視設備」を解説。 ・「警報及び監視設備」に対する留意事項を記載。

3．技術要件書変更内容の概要（8/14）

４.有効性評価	概要(表現適正化を除く変更箇所を朱記)	解説
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，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。	・有効性評価の目的を解説。 ・「概ね満足する」を解説。 ・「解析等により確認する」を解説。
4.2 評価すべき事象	本有効性評価では，運転時の異常な過渡変化又は設計基準事故全事象を対象とする。	・「有効性評価が対象とする全事象」を記載。
4.3 判断基準	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（「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」第十三条第一項第二号）において使用される判断基準を準用し，その判断基準が概ね満足されることを確認する。	・「設置許可基準に記載されている具体的な判断基準」を記載。

3．技術要件書変更内容の概要（9/14）

４.有効性評価	概要(表現適正化を除く変更箇所を朱記)	解説
4.4　解析にあたって考慮すべき事項	安全設計の妥当性確認に用いる安全解析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。	—
4.4.1　解析にあたって考慮する範囲	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。	・「通常運転範囲」を解説。 ・「運転期間」を解説。 ・「燃料交換等による長期的な変動」を解説。 ・「合理的に推定できる時点」を解説。 ・解析点及び解析範囲が、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理由を記載。
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。 ・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。 ・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。	・「設計値等に基づく現実的な運転条件とすることの」解説を記載。 ・設計値に基づく現実的な値の具体例を記載。 ・現実的な操作条件の例として、ABWRの制御棒誤引き抜きにおける操作を記載。

3．技術要件書変更内容の概要（10/14）

４.有効性評価	概要(表現適正化を除く変更箇所を朱記)	解説
4.4.3　安全機能に対する仮定	・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または運転員が事象の発生を認知した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。 ・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。	・安全機能のサポート系の取り扱いについて理由を記載。

3．技術要件書変更内容の概要（11/14）

4.有効性評価	概要(表現適正化を除く変更箇所を朱記)	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する。 ・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。	・「外部電源は利用可能」とする理由を記載。 ・「故障の仮定から除外できる設備」の解説と例。 ・「常用系設備が復旧し，利用可能となることは想定しない」を解説。
4.4.5 多様化設備に関連する条件	（１）機器条件 ・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。 ・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。 （２）操作条件 ・運転員による手動操作をCCF対策として期待することができる。 ・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良い。 ・原子炉制御室外における現場操作を考慮して良い。	・「多様化設備の単一故障を想定しない」理由及び例を記載。 ・「現実的な時間での運転操作を設定してもよい」理由を記載。

3．技術要件書変更内容の概要（12/14）

4.有効性評価	概要(表現適正化を除く変更箇所を朱記)	解説
4.4.6 解析に使用する計算プログラム，モデル及びパラメータ	（１）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，適用範囲において妥当性確認および検証がなされたものであること。許認可での使用実績により確認済みの場合は、妥当性確認及び検証は不要である。	・「評価に用いる計算プログラム」の例を記載。 ・「ベストエスティメイトコード」の例を記載。 ・「評価に用いる計算モデル」の例を記載。

3．技術要件書変更内容の概要（13/14）

5．手順書の整備と教育及び訓練の実施	概要(表現適正化を除く変更箇所を朱記)	解説
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，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を認知した場合，その要因がソフトウェアCCFの重畳発生によることを判断し，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。	・「手順書の整備」を解説。
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にソフトウェアCCFが重畳発生した場合において，整備された手順書に従い，的確に対処できる力量を付与させるための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。	・「教育及び訓練の実施目的」を解説。 ・「教育及び訓練の計画・実施」を解説。

3．技術要件書変更内容の概要（14/14）

	概要(表現適正化を除く変更箇所を朱記)	解説
6. 対策例	事業者が実施した予備評価結果に基づく多様化設備による対策例を記載。	—
7. 参考文献	本技術要件書を作成するにあたり 参考とした文献を記載。	—