ATENA20-ME〇〇

2020.9.17　ドラフト
ATENA 会内レビュー中

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てきた。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，ソフトウェアの信頼性を確保する取り組みとして，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)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(Common Cause Failure)」という。）が発生し，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，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 9 月に，第 29 回原子力規制委員会臨時会議で，発電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，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，産業界として更なる対策（従来の多様化設備に加え、安全系の自動作動機能や警報の追加、及び手順書の整備）を自主的に且つ計画的行うことを ATENA のステアリング会議で決定した。

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 対策を行うにあたり，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示すことにより，事業者が合理的且つ早期に対応できることを意図して整備したものである。

各事業者は，本書に示した技術要件に従い対策を整備する。ATENA は事業者の実施状況と対策の適合性確認を行い，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 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。

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。

改訂来歴

改訂番号	日付	内容	改訂箇所
初版	2020. .	発刊初版	

目次

1. 序文

1.1 目的

本技術要件書の目的は，事業者がデジタル安全保護回路のソフトウェア CCF 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仕様及びその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，適切なソフトウェア検証等により信頼性の高い設計がなされているものの，特定のできないエラーが発生する不確かさを有する。また，同一のプラットフォームの使用等により，潜在的なソフトウェア CCF の可能性を完全に排除することはできず，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潜在的可能性を有する。このため，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することとなるが，これによりデジタル安全保護回路のソフトウェア CCF に対する脆弱性に対して適切に対処可能であることを示す必要がある。

本技術要件書に，検討チームでの議論を基に，多様化設備への要求事項と有効性評価手法を記載する。

1.3 適用範囲

デジタル安全保護回路のソフトウェア CCF 対策としての多様化設備に適用する。

1.4 用語の定義

- 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安全保護機能（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等の機器を動作させる，または警報発生やランプ点灯等させるための信号処理を行う機能のことを言う。

- ソフトウェア
  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）及び設計上の要求機能を、コンピュータ上で直接的に実現するアプリケーションソフトウェアを指す。

- ソフトウェア共通要因故障，ソフトウェア CCF（CCF；Common Cause Failure）
  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，

ソフトウェアの潜在的な不具合による共通要因故障により安全保護機能の一部又は全てが喪失する状態を言う。

- 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，重大事故等対処設備等を自動的に，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。

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

ソフトウェアにCCFの発生を想定する設備の範囲は，デジタル技術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。

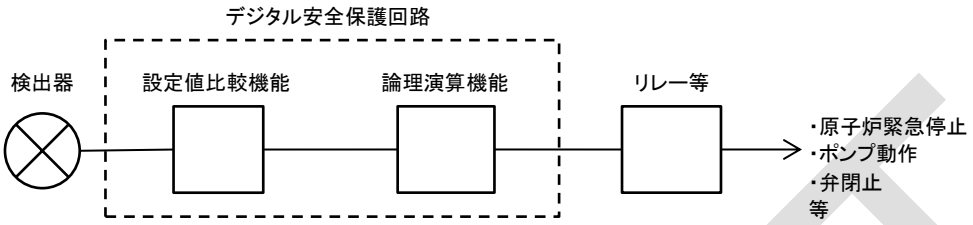


図1：安全保護回路のうちソフトウェア CCF を想定する範囲（例）

2.2 ソフトウェアCCFの故障モード想定

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，2.1 に示す範囲でソフトウェア CCF が発生し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によって安全保護機能が作動できなくなった場合においても，それ以前に起動していたポンプなどの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，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，重大事故等対処設備等を自動的に，または手動により作動させることができること。

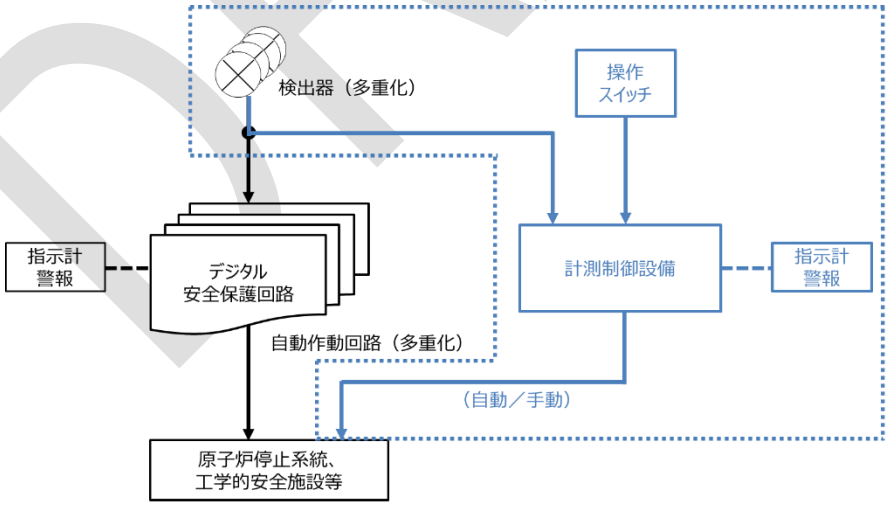
工学的安全施設等を手動により作動させる場合には，運転員が必要な時間内に操作を開始できるよう，安全保護動作の異常の発生及び設計基準事故の事象の発生を認知できる機能を設けること。

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。

ここで，上記の構成要素は，3.5 に示す各要件を満足する限り，既設設備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，重要事故対処設備など）。

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，どの既設設備を選定したか明確にすること。



青点線は，多様化設備の範囲を示す

3.4 設計基本方針

多様化設備は，デジタル安全保護回路の代替機能であることから、設計基準事故対処設備や重大事故等対処設備の重要度分類には該当しないことから，代替機能として適切と考えられる設計基本方針を以下に定めるものとする。

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，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，多様化設備には，単一故障を想定した設計を行う必要はなく，多重性は要求しない。また，溢水・火災あるいは外的影響は，ソフトウェア CCF の要因とはならないことから，重畳発生することを設計で考慮する必要はない。

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作動できる設計とする。

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，デジタル安全保護回路のソフトウェア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，そのプログラムに潜在的な不具合が共通して存在する可能性がないこと，その他ソフトウェアに起因する共通要因故障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と共用し，または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

火災或いは溢水により運転時の異常な過渡変化が発生する場合においては，多様化設備が，火災・溢水の影響を受けたとしても，設計基準事故対処設備の安全機能喪失に波及しない設計とすること（参考資料●参照）。

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

多様化設備の操作は，原子炉制御室から行える設計とすること。
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。

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 が重畳する事象が発生した場合において，事象の判定及び対応操作に必要となる警報及び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，デジタル安全保護回路のソフトウェア CCF の発生を前提としたうえで，3 章に示す設備要件を満たす多様化設備等により，想定した事象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，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。

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，設計時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，重大事故事項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。

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，異常状態，すなわち「運転時の異常な過渡変化」又は「設計基準事故」（以下，「設計基準事象」という。）について解析し評価を行っている。したがって，本有効性評価では，これら評価の対象としている全事象を対象とする。

4.3 事象想定

前項で述べたとおり，設計基準事象を対象とし，有効性評価の目的に照らして解析すべき事象を適切に選定する。評価に際しては，ソフトウェア CCF の影響を確認する観点から，類似する事象はグルーピングしてもよい。また，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，故障モードの包絡性）を確認し，その妥当性を示すこと。

4.4 判断基準

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する。なお，原子炉格納容器の限界圧力・温度等，設備の健全性が別途確認されている条件，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。

ソフトウェア CCF の発生を仮定した前提で実施する本評価は設計基準事象を超えるものであるが，ソフトウェア CCF 対策により，事象進展を設計基準事故対処設備が担う深層防護のレベルに留めることができる能力を確認することが目的であるため，設計基準事故の判断基準を基本とする。その上で，4.5 章で示す最適評価により，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もってソフトウェア CCF 対策として講じた措置が妥当であることの確認を行う。

4.5 解析に当たって考慮すべき事項

多様化設備の有効性を評価するに当たり，現実的な条件を設定することが適切である。これは，過度に保守的な条件を設定した場合，ソフトウェア CCF の影響を受けない設備や多様化設備の効果など現実的なプラント応答等を確認することが困難になるためである。このため，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。

4.5.1 解析に当たって考慮する範囲

解析結果は，想定した事象が，判断基準を概ね満足しながら支障なく収束できることを，その事象が包絡している全事象について確認できるものでなくてはならない。そのためには，少なくとも事象が収束し原子炉が支障なく安定状態に移行できることが，合理的に推定できなければならない。

4.5.2 解析で想定する現実的な条件等

解析を行うにあたっては，設計時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，SA 評価のような最適評価を基本的な考え方とする。ただし，ソフトウェア CCF を仮定した場合においても，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この限りではない。

・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，プラントの運転条件等を前提とした条件としても良い。 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。

・事象発生によって生じる外乱，炉心状態，機器の容量などは現実的な条件を想定する。

(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。

4.5.3 安全機能に対する仮定

安全機能(安全保護系及び工学的安全施設の機能)は以下の仮定による。

・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場合を想定する。

・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とする（4.5.5 多様化設備に関連する条件参照）。
・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。

4.5.4 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による。

・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 on-duty の設備は，駆動源が維持される限りその作動状態を継続するものとする。
・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。

4.5.5 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，工学的安全施設及び重大事故等対処設備の故障や誤動作が起因となることは想定しない。
・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，工学的安全施設及び重大事故等対処設備は利用可能であり，多様化設備として供用できる。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）が利用可能なことの確認が必要である。
（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）。
・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する。

4.5.6 解析に使用する計算プログラム，モデル及びパラメータ

a. 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。
b. 現実的な計算モデル（例：崩壊熱モデル，ベストエスティメイトコードにおける計算モデルの保守性に係る不確かさを考慮しない等）を使用しても良い。
c. 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この限りではない。

[1]想定する事象を現実的に予測できるコード。

5. 手順整備と教育

5.1 手順整備

運転時の異常な過渡変化又は設計基準事故が発生し，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，炉心の著しい損傷を防止するため，必要な手順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，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 が重畳発生した場合において，事象の種類及び事象の進展に応じて的確に対処するため，教育及び訓練を継続的に実施すること。

添付資料