2020.9.25ドラフト
公開会合資料

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の
自律的対応について

2020年10月6日
原子力エネルギー協議会

目 次

1．はじめに（1/2）

（1）1月29日の公開会合で，産業界としてソフトCCF対策を自律的かつ計画的に取り組む旨表明。また，産業界が自律的に取り組む場合，ATENAの関与として下記を示した。

①技術要件書を作成し事業者へ提示する

②事業者に実施計画の提出を要求し、進捗フォローを行う

（2）7月8日の原子力規制委員会で，当面の対応として以下が決まった。

①対策水準の内容を，事業者が自らの自主的取り組みでどのように実現されるのか公開の会合で提案を受ける

②必要に応じて，進捗の状況を公開の会合の場で把握し，その結果を原子力規制委員会に報告する

1．はじめに（2/2）

今回の会合では以下の事項について説明・提案する。

1．ソフトウェアCCF対策を自律的に進めていくための産業界の基本方針

2．事業者の対策実施に対するATENAの関与

3．各事業者の対策実施予定時期

4．技術要件書の概要と原子力規制委員会で示された対策水準との対応
（対策設備の要求事項と有効性評価手法を纏めた技術要件書が，原子力規制委員会で示された対策水準と整合が取れていることの認識共有を図りたい）

2．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。

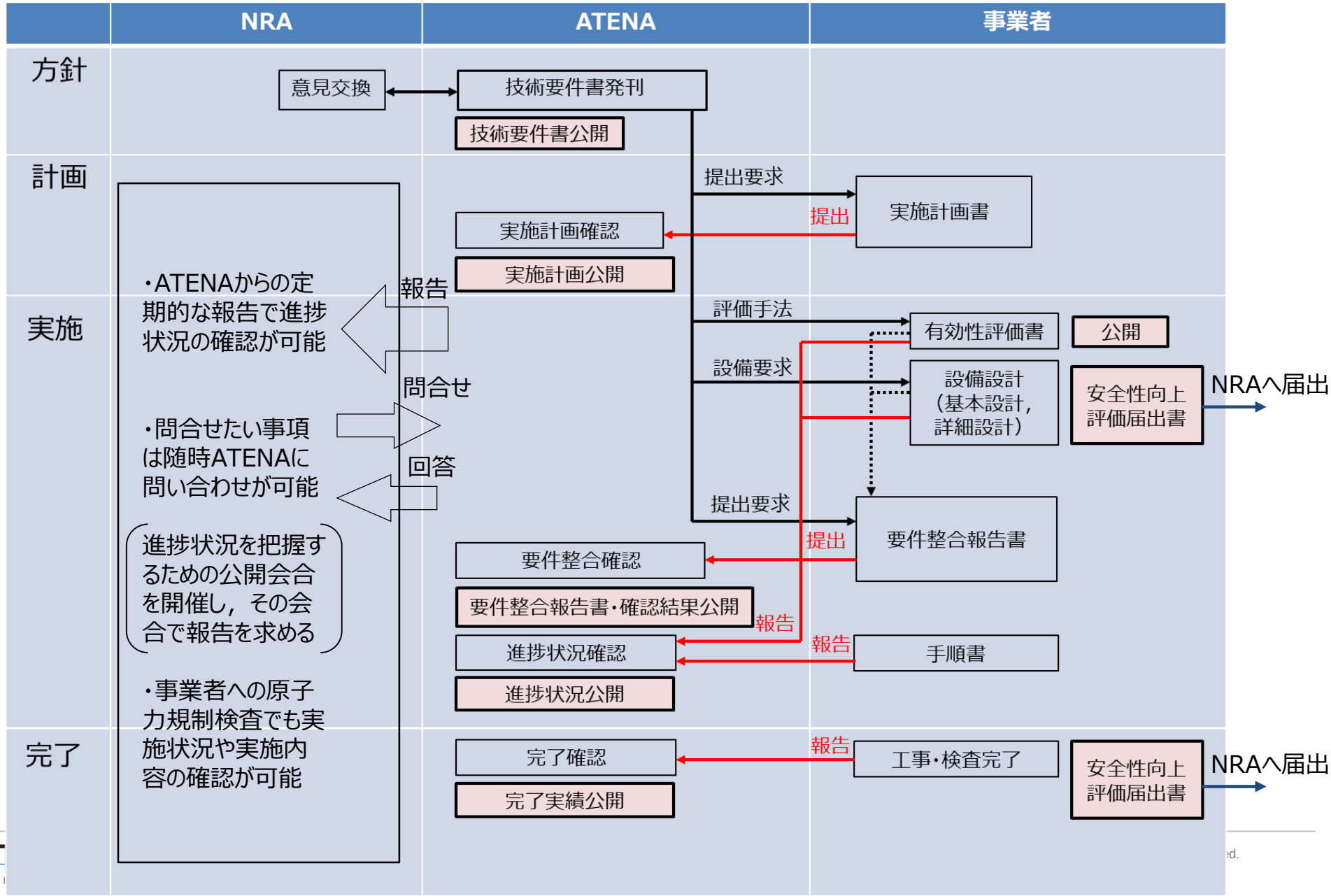
① 実施計画書の提出
② 有効性評価書の公開
③ 要件整合報告書の提出
④ 進捗状況の報告（半期に一度）

（3）事業者は，（2）の対応を行うとともに，対策の計画および完了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。

（4）ATENAは，技術要件書，実施計画，要件整合報告書およびATENAによる確認結果，進捗状況、完了実績をHPに公開する。
ATENAは、NRAに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等を通し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。

3．基本方針に基づく対応フロー



４．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。

（2）ATENAは，実施計画書を確認後，HPに公開する。（参考１）

（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，確認した進捗状況についてNRAに報告する。（参考2）
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。

※「有効性評価」，「基本設計」，「詳細設計」，「要件整合報告」，「工事・検査」

（参考１）対策実施計画の予実績管理（例）

ソフトウェアCCF緩和対策に関する事業者の対策実施計画予定・実績

事業者	主要な対策		完了時期					備考
			有効性評価	基本設計	詳細設計	要件整合報告	工事・検査	
A電力 ○○発電所 1号機	・自動機能追加 ・警報機能追加	予定	2022年3月	2022年11月	2023年6月	2023年6月	2024年11月	
		実績	2022年3月					
B電力 ○□発電所 2号機	・自動機能追加 ・警報機能追加	予定	2021年4月	2021年12月	2022年7月	2022年7月	2023年12月	
		実績	2021年4月	2022年1月※ ※○○の理由により、予定より完了が遅れた。	2022年7月	2022年7月		
X電力 ○△発電所 3号機	・警報機能追加	予定	2022年3月	2022年11月				
		実績	2022年3月					

新規制基準適合性に係る工事計画認可が下り、再稼働時期の見通しが立った際に報告をする。

（参考２）NRAへ報告内容（例）

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有要因故障対策
に関する原子力事業者の対策実施状況について

2022年4月～ 2022年9月の期間，事業者の進捗は以下のとおりです。

１．A電力　○○発電所　1号機
・「有効性評価」が2022年4月に完了しました。

２．B電力　○□発電所　2号機
・「詳細設計」が2022年7月に完了しました。
・ATENAへの「要件整合報告」が2022年7月に完了し，ATENAは要件整合報告書および
その確認結果をＨＰで公開しました。

5．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３）要件整合報告書（例）

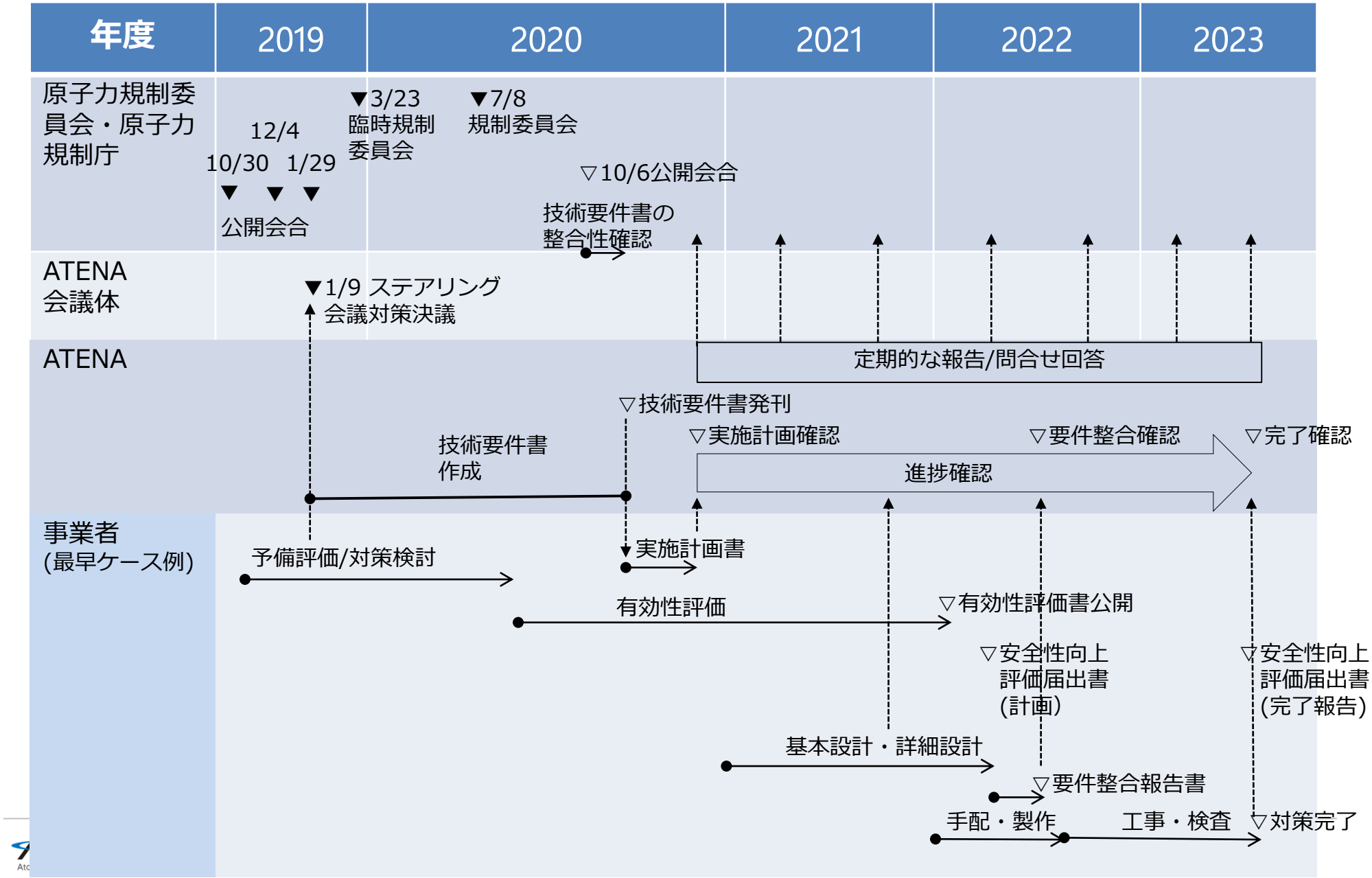
要件整合報告書は全項目に対して記載するが，ここでは例として一項目を抽出

例：「LOCA＋ソフトウェアCCF」事象の解析条件(ABWR)

技術要件書		設計図書における要件整合			
項目	要求内容	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		設計図書名および記載場所
			判定	理由	
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（ノミナル条件）としてよい。	・100%出力/100%炉心流量	○	定格出力，定格炉心流量を初期条件としている。	・有効性評価書A.B節 xページ
		・9×9燃料A型炉心ノミナル出力布	○	ノミナル出力分布を初期条件としている。	・有効性評価書A.B節 ｘページ
		・原子炉圧力 7.17MPa(abs)	○	定格原子炉圧力を初期条件としている。	・有効性評価書A.B節 ｙページ
		・原子炉水位　NWL	○	通常原子炉水位を初期条件としている。	・有効性評価書A.B節 yページ
		・100%給水流量/100%主蒸気流量	○	定格給水流量，定格主蒸気流量を初期条件としている。	・有効性評価書A.B節 yページ
		・給水温度 216℃	○	定格出力での給水温度を初期条件としている。	・有効性評価書A.B節 yページ

判定凡例：○　→　適合している

6. ソフトウェアCCF対策に関する対応スケジュール



7．ソフトウェアCCF対策実施予定時期について（1/3）

実施予定時期の考え方

- 再稼働済み，もしくは2023年度までに再稼働するプラントは，2023年度以降の最初の定期事業者検査時
- 2023年度以降に再稼働するプラントは再稼働時期までに実施

対象プラント

- デジタル安全保護回路導入済プラント
  （部分デジタル化のプラントも含む）

対策　（現状の自主設備に追加となる対策）

対象	対策
BWR（ABWR）／PWR共通	・事象発生時の手順書整備
ABWR	・警報機能追加
PWR	・SI自動起動機能追加 ・警報機能追加

7．ソフトウェアCCF対策実施予定時期について（2/3）

PWR	実施予定時期 ［定検回数］，（新規制基準許可状況）
泊１号	新規制基準適合性に係る工事完了までに実施（許可申請済）※
泊２号	新規制基準適合性に係る工事完了までに実施（許可申請済）※
泊３号	新規制基準適合性に係る工事完了までに実施（許可申請済）※
美浜３号	2023年度［第27回定検］（許可済）
大飯３号	2023年度［第20回定検］（許可済）
大飯４号	2023年度［第19回定検］（許可済）
高浜１号	2024年度［第29回定検］（許可済）
高浜２号	2024年度［第29回定検］（許可済）

PWR	実施予定時期 ［定検回数］，（新規制基準許可状況）
高浜３号	2023年度［第26回定検］（許可済）
高浜４号	2023年度［第25回定検］（許可済）
伊方３号	2023年度以降に実施する最初の定検にて実施（許可済）
玄海３号	2023年度［第17回定検］（許可済）
玄海４号	2023年度［第15回定検］（許可済）
川内１号	2023年度［第27回定検］（許可済）
川内２号	2023年度［第26回定検］（許可済）
敦賀２号	新規制基準適合性に係る工事完了までに実施（許可申請済）※

※　新規制基準適合性に係る工事計画認可が下り，当該工事完了時期の見通しが立った際に報告を受ける。

7．ソフトウェアCCF対策実施予定時期について（3/3）

BWR	実施予定時期 （新規制基準許可状況）
東通１号	新規制基準適合性に係る工事完了までに実施（許可申請済）※1
女川２号	新規制基準適合性に係る工事完了までに実施（許可済）※1
柏崎刈羽６号	2023年度以降に実施する最初の定検にて実施（許可済）
柏崎刈羽７号	2023年度以降に実施する最初の定検にて実施（許可済）
浜岡３号	新規制基準適合性に係る工事完了までに実施（許可申請済）※1
浜岡４号	新規制基準適合性に係る工事完了までに実施（許可申請済）※1

BWR	実施予定時期 （新規制基準許可状況）
志賀２号	新規制基準適合性に係る工事完了までに実施（許可申請済）※1
島根２号	2023年度以降に実施する最初の定検にて実施（許可申請済）
島根３号	建設中に実施（許可申請済）
東海第二	新規制基準適合性に係る工事完了までに実施（許可済）※1
大間	建設中に実施（許可申請済）

※１　新規制基準適合性に係る工事計画認可が下り，当該工事完了時期の見通しが立った際に報告を受ける。

※２　新規制基準適合性審査を未申請の下記プラントについては，新規制基準適合性審査の申請・許可後，工事計画認可が下り，当該工事完了時期の見通しが立った際に報告を受ける。

・女川3号，柏崎刈羽１～５号，浜岡5号，志賀1号

8．技術要件書（案）の概要（1/10）

（１）目的

本技術要件書の目的は，事業者が自律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。

（２）技術要件書（案）の概要

- NRAが示した対策水準を具体化した内容とする。
- 多様化設備要求については，多様性・多重性・耐震性などの主要な項目について要求事項を記載する。
- 有効性評価手法については，評価すべき事項・判断基準・解析に当たって考慮すべき事項など共通的な条件について要求事項を記載する。
- 手順書の整備や教育訓練の実施について要求する。

8．技術要件書（案）の概要 （2/10）

(3) 技術要件書（案）の目次

1．序文
- 1.1 目的
- 1.2 概要
- 1.3 適用範囲
- 1.4 用語の定義

→ 技術要件書作成の経緯・位置づけを記載

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
- 2.2 ソフトウェアCCFの故障モード想定

→ CCFの定義を記載

3．多様化設備要件
- 3.1 設置要求
- 3.2 機能要求
- 3.3 多様化設備の範囲
- 3.4 設計基本方針
- 3.5 多様化設備への要求事項

→ 設備要求を記載

4．有効性評価
- 4.1 有効性評価の目的
- 4.2 評価すべき事象
- 4.3 判断基準
- 4.4 解析に当たって考慮すべき事項

→ 有効性評価手法への要求を記載

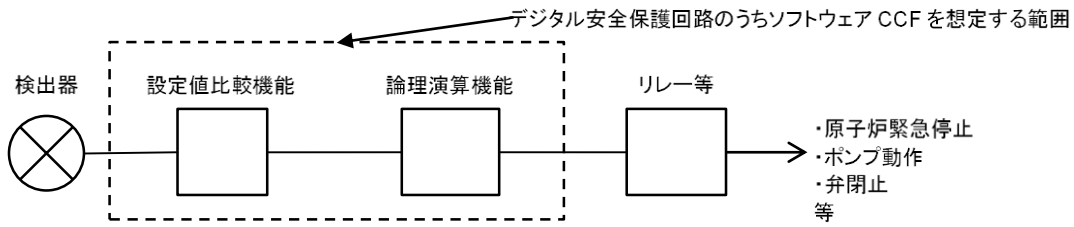
5．手順書整備と教育
- 5.1 手順書整備
- 5.2 教育及び訓練の実施

→ 手順整備と教育訓練の要求を記載

添付資料

参考資料

8．技術要件書（案）の概要（3/10）

1．序文	概要
1.1 目的	本技術要件書の目的は，事業者が自律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	（省略）
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	（省略）
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。 
2.2 ソフトウェアＣＣＦの故障モード想定	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。

8．技術要件書（案）の概要（4/10）

3.多様化設備要件	概要
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，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。
3.4　設計基本方針	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，単一故障や溢水・火災あるいは外的影響とソフトウェアCCFの重畳を想定した設計を行う必要はない。
3.5.1　多重性	多様化設備には，多重性は要求しない。

8．技術要件書（案）の概要（5/10）

3.多様化設備要件（続き）	概要
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。
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	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。

8．技術要件書（案）の概要（6/10）

3.多様化設備要件（続き）	概要
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。
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。

8．技術要件書（案）の概要（7/10）

４.有効性評価	概要
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，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	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こと。
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」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を確認する。

8．技術要件書（案）の概要（8/10）

４.有効性評価（続き）	概要
4.4　解析に当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。
4.4.1　解析に当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	・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。 ・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ても良い。
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。 ・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。

8．技術要件書（案）の概要（9/10）

４.有効性評価（続き）	概要
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。 ・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。 ・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は多様化手段の一部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は現実的な想定を前提としても良い。 ・原子炉制御室外における現場操作を考慮して良い。
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）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を使用しても良い。 （２）現実的な計算モデルを使用しても良い。 （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がなされたものであること。

8．技術要件書（案）の概要（10/10）

5. 手順書整備と教育	概要
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。

9. NRA対策水準とATENA技術要件書（案）の対応（1/6）

出典：令和2年度　原子力規制委員会　第15回会議
議題4「発電用原子炉施設のデジタル安全保護回路に係る共通要因故障対策の今後の対応について」資料より引用

NRA対策水準	ATENA技術要件書（案）
①安全保護回路とは異なる動作原理の機構により，原子炉停止系統及び工学的安全施設を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ものとすること。 ➢ 「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故障によってデジタル安全保護回路の安全保護機能と同時にその代替作動機能を喪失するおそれがない系統，機器その他の機構をいう。	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 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。 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。 3.5.4　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。

9. NRA対策水準とATENA技術要件書（案）の対応（2/6）

NRA対策水準	ATENA技術要件書（案）
②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，安全保護回路の安全保護機能が喪失したときにおいても，発電用原子炉施設の安全性が損なわれることを防止することができるものとすること。 ➢ 「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，安全保護回路の安全保護機能が喪失したとき」とは，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において，デジタル安全保護回路がソフトウェアに起因する共通要因故障によってその異常な状態を検知することできないとき又は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ことができないときをいう。	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，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 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こと。 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」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を確認する。 2.2 ソフトウェアＣＣＦの故障モード想定 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。

9. NRA対策水準とATENA技術要件書（案）の対応（3/6）

NRA対策水準	ATENA技術要件書（案）
➢ 「発電用原子炉施設の安全性が損なわれることを防止することができる」とは，最適評価により設計基準事故時の要件を概ね満足すること又は炉心の著しい損傷を防止することができることをいう。	4.4 解析に当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。 4.4.1 解析に当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 ・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。 ・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。 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。 ・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。

9. NRA対策水準とATENA技術要件書（案）の対応（4/6）

NRA対策水準	ATENA技術要件書（案）
➢ 「発電用原子炉施設の安全性が損なわれることを防止することができる」とは，最適評価により設計基準事故時の要件を概ね満足すること又は炉心の著しい損傷を防止することができることをいう。 （続き）	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。 ・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。 ・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は多様化手段の一部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は現実的な想定を前提としても ・原子炉制御室外における現場操作を考慮してよい。 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）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を使用しても良い。 （２）現実的な計算モデルを使用しても良い。 （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がなされたものであること。

9. NRA対策水準とATENA技術要件書（案）の対応（5/6）

NRA対策水準	ATENA技術要件書（案）
③共通要因によって安全保護回路の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，適切な措置を講じたものとすること。 ➢ 「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と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。	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 運転時の異常な過渡変化多様化設備が，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。 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。

9. NRA対策水準とATENA技術要件書（案）の対応（6/6）

NRA対策水準	ATENA技術要件書（案）
④外部電源が利用できない場合においてもその代替作動機能が損なわれるおそれがないものとするほか，重要安全施設と同等の信頼性を確保したものとする。	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。 3.5.11　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。 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。