資料3

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

2023年　2月　9日
原子力エネルギー協議会

目 次

1．はじめに

（１）2020年1月29日の公開会合において、産業界としてソフトウェアCCF対策を自律的かつ計画的に取り組む旨表明。 また、2020年10月６日の公開会合において、産業界として対策を自律的に進めていくための基本方針、ATENAの関与（技術要件書発刊、要件整合確認、進捗確認等）、各事業者の対策実施時期等について説明した。

（２）ATENAは、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」（以下技術要件書）を発刊するとともに事業者に対して対策の実施を要求し、半期に一度事業者の対策実施進捗状況を公開、NRAに報告を行っている状況である。

（３）現在、各事業者は予定通り対策を進めており、2023年1月に最早プラントの要件整合報告書がATENAに提出されるとともに、対策設備の工事・検査が完了する段階にきている。

（４）今回の公開会合では、自律的対策における下記概要について産業界の方針をご説明する。

- 事業者の要件整合報告とATENAによる確認について
- 事業者の自主検査について
- 自律的対応に係る事業者の管理体制等について

2．基本方針（1/2）

各事業者とATENAは、以下に示す基本方針に従い、責任を持って自律的かつ計画通りに対策を実施する。（基本方針に基づく対応フローを図１に示す）

（１）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）

（２）ATENAは、各事業者のデジタルCCFに係る安全対策の実施計画を公開するとともに、半期に一度実施状況を公開しNRAへ報告する。

（３）ATENAは、各事業者から提出された要件整合報告書とATENAによる要件整合確認結果を実施状況に合わせて公開するとともにNRAへ報告する。

（４）ATENAは、事業者の対策完了実績を公開しNRAに報告する。

（５）事業者は、設備設計、工事・検査完了の各段階でデジタルCCFに係る安全対策の内容を安全性向上評価届出書に記載してNRAへ届出を行う。

2．基本方針（2/2）

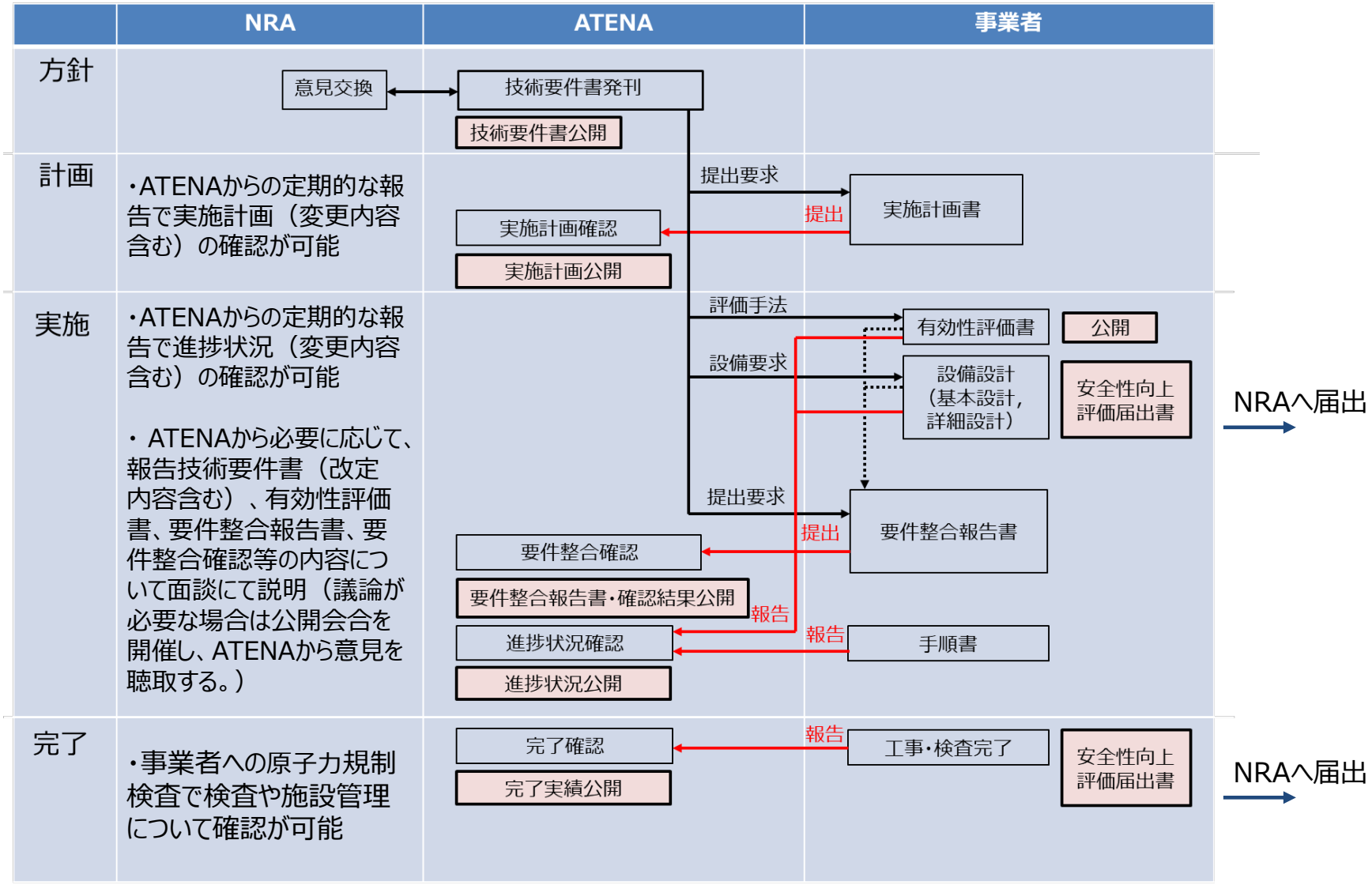


図１基本方針に基づく対応フロー

3．技術要件書の概要（1/2）

（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）技術要件書の概要

- 公開会合を通じてNRAが示した対策水準を具体化した内容としている。
- 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。

3．技術要件書の概要 （2/2）

(3) 技術要件書の目次（各章の要求事項は添付１参照）

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

要件整合報告、確認の対象範囲

4．事業者の要件整合報告（1/2）

（１）目的

事業者は、技術要件書が定める「3．多様化設備要件」及び「4．有効性評価」の各要求内容に対する整合性の確認を行い、確認結果を要件整合報告書に取りまとめ、ATENAに提出する。

（２）要件整合報告書の内容

①技術要件書に記載された要求事項に対応する設計図書及び有効性評価図書の記載内容
②要求事項への整合性判定及びその理由
③設計図書名・図書番号と記載場所（ページ・表番号など）
④記載が確認できるエビデンス(有効性評価書、設計図書の抜粋)

（３）要件整合報告書の品質保証

事業者は、原子炉設置変更許可申請書，および設計及び工事の計画認可申請書での図書承認プロセスと同等のプロセスの下で、要件整合報告書及び承認プロセスを、原子力本部長の責任の下、ATENAに提出する。

【具体的な例】

・許認可申請時と同様に、要件整合報告書の内容について報告書作成箇所以外の箇所または会議体でのレビューを経たうえで、原子力本部長名の文書としてATENAへ提出した。

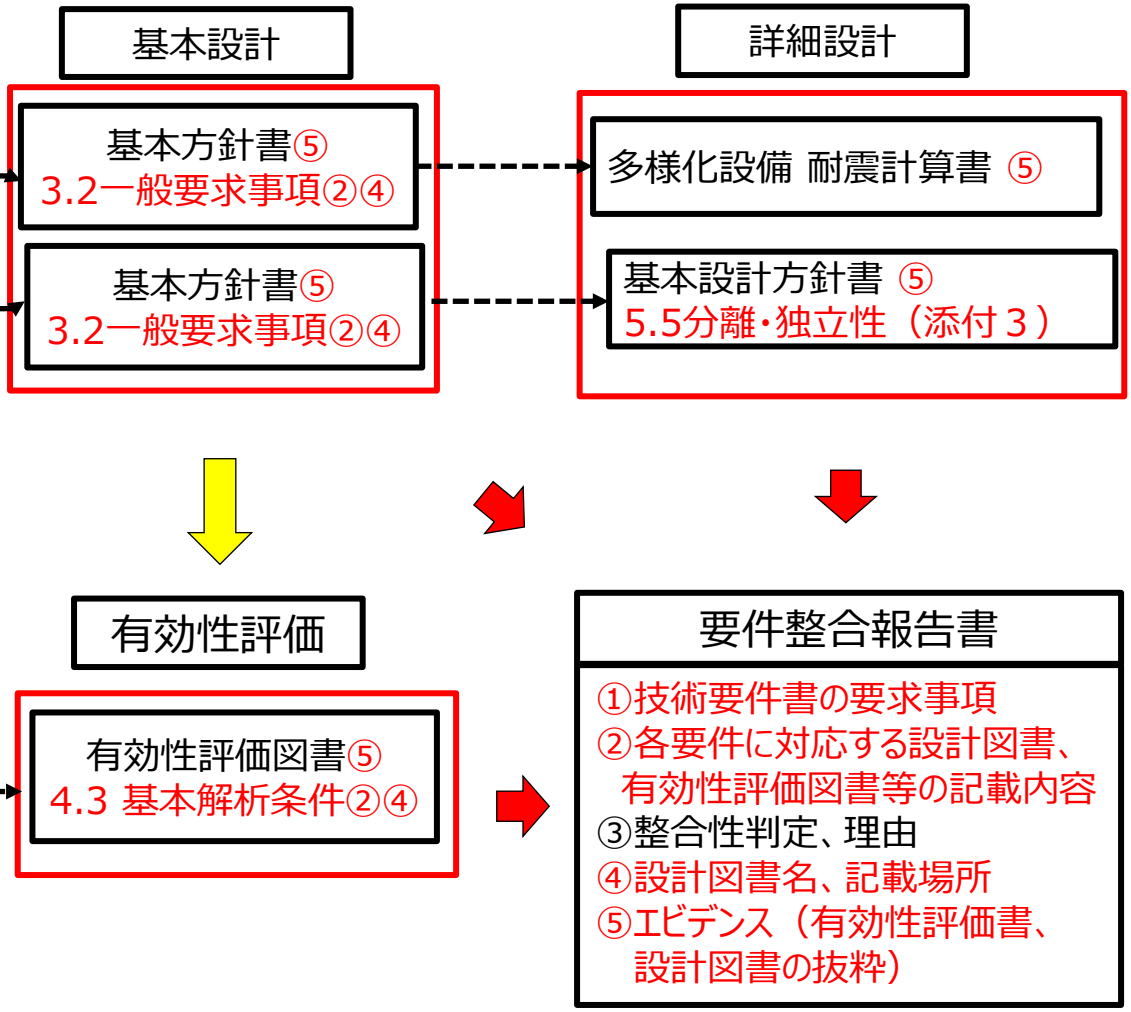
4．事業者の要件整合報告（2/2）

【技術要件書に対する要件整合報告の概要】（要件整合報告書の記載例を添付２に示す。）

技術要件書における要求項目

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
  - 3.5.4　耐震性（例）
    基準地震動Ssに対し機能維持すること①
  - 3.5.8　安全保護回路への波及的影響防止
    多様化設備の故障により安全保護回路の機能を喪失させない設計とすること①

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
  - 4.4.3 安全系機能に対する仮定（例）
    CCFにより安全保護回路の機能喪失を仮定①



5．ATENAの要件整合確認

（1）要件整合報告書の確認

ATENAは、事業者から提出された要件整合報告書及びエビデンス(有効性評価書、設計図書)を下記の要領で確認し、**不十分な点があれば事業者に改定指示を出し**、反映されたことを確認後整合確認書として取りまとめる。

①技術要件書の要求事項が漏れなく摘出されていること。
②記載内容（概要）の欄に、具体的な設備仕様や有効性評価結果が記載され、要求事項への整合性が明確になっていること。また、設計仕様や解析条件等が小項目に細分化されて記載されていること。
③要件整合判定が全て「○」で、かつ、その合理的な理由が記載されていること。
④エビデンスに上記②の欄の内容が具体的に記載されていること。
⑤多様化設備要件と有効性評価の関連する項目が紐づけられていること。

（2）図書承認プロセスの確認

ATENAは、事業者から提出された承認プロセスが、原子炉設置変更許可申請書，および設計及び工事の計画認可申請書での図書承認プロセスと同等のプロセスであることを確認する。

（3）情報公開

ATENAは、事業者の要件整合報告書およびその確認結果を半年ごとの進捗状況の公開にあわせてHPで公開しNRAに報告する。

6．事業者自主検査の対象（1/2）

技術要件書の要求項目に対して、現地工事後の事業者自主検査で確認する対象を以下に示す。

（１）技術要件書「3.多様化設備要件」の要求項目

現地工事後の特性検査と機能及び性能に係る検査を事業者自主検査の対象とする。

技術要件書の要求項目	要件整合報告書で確認	事業者自主検査の対象
3.2　機能要求	自動作動機能（自動原子炉トリップ、自動安全注入作動他）、 手動操作機能、 警報機能、 指示機能	○特性検査 ・設定値確認検査 ・応答時間測定検査 ○機能及び性能に係る検査 ・ロジック検査 ・警報機能検査 ・指示性能検査
3.3　多様化設備の範囲	検出器、操作器、論理回路、指示計、警報、表示灯他の仕様	
3.4　設計基本方針	「3.5　多様化設備への要求事項」で個別に確認	－
3.5　多様化設備への要求事項	耐環境性、耐震性、供給電源、設備の共用、 試験可能性、安全保護回路への波及的影響防止、 火災防護及び溢水防護、外的事象に対する防護、 操作性、監視性	－

6．事業者自主検査の対象（2/2）

（２）技術要件書「４.有効性評価」の要求項目

要件整合報告書で全て確認するため、事業者自主検査の対象はない。

技術要件書の要求項目	要件整合報告書で確認	事業者自主検査の対象
4.2　評価すべき事象	評価対象事象（過渡、事故全事象＋CCF)、グルーピング、解析を省略した事象	－
4.3　判断基準	設計基準事故の判断基準の準用、他の判断基準の適用の有無、判断基準への適合性	－
4.4　解析に当たって考慮すべき事項	最適評価コードの適用、解析の範囲、解析で想定する現実的な条件、安全系機能に対する仮定、常用系機能に対する仮定、多様化設備に関連する条件（機器条件、操作条件）、解析に使用する計算プログラム及びモデル	－

（３）技術要件書「５.手順書の整備と教育及び訓練の実施」の要求項目

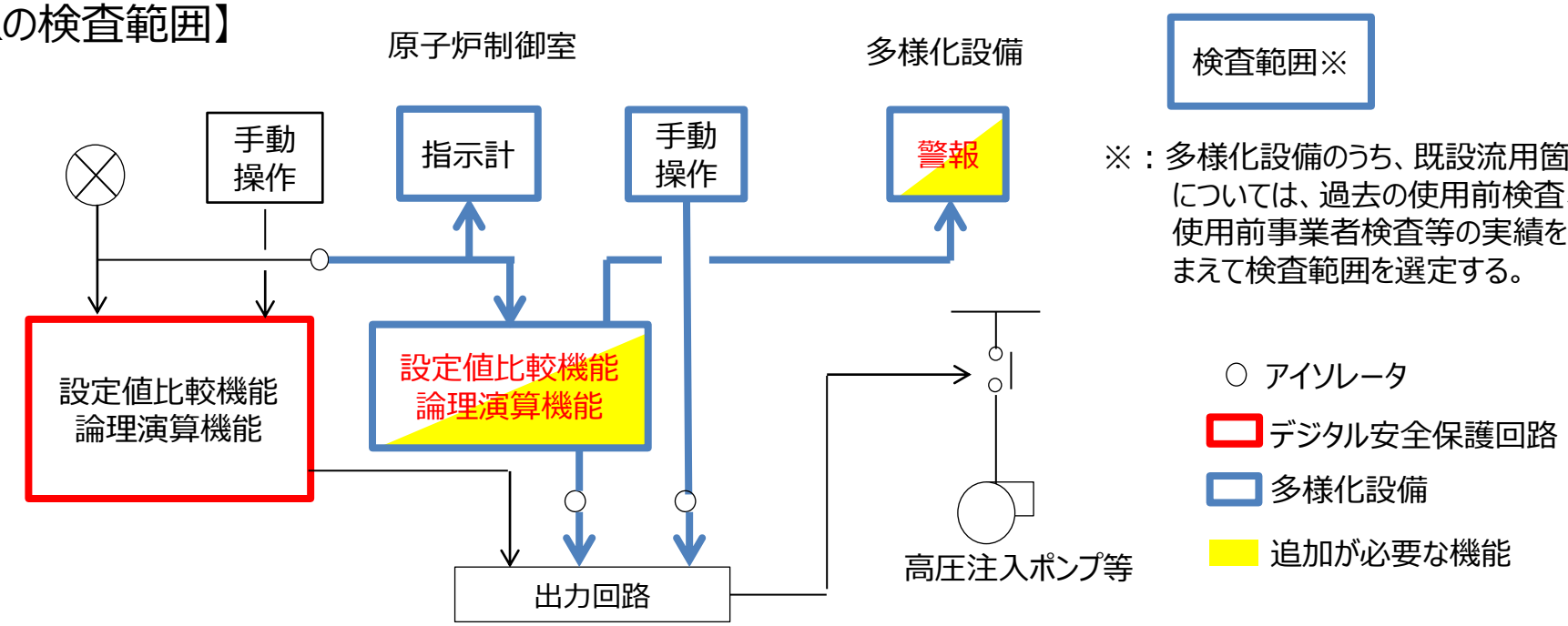
技術要件書の要求項目	要件整合報告書で確認	事業者自主検査の対象
5.1　手順書の整備	－	手順書の整備と確認
5.2　教育及び訓練の実施	－	教育・訓練の内容・頻度

7．事業者自主検査の内容（1/5）

事業者は、以下の範囲について事業者自主検査を実施する。
また、事業者自主検査は、使用前事業者検査と同等の内容及び体制にて実施する。

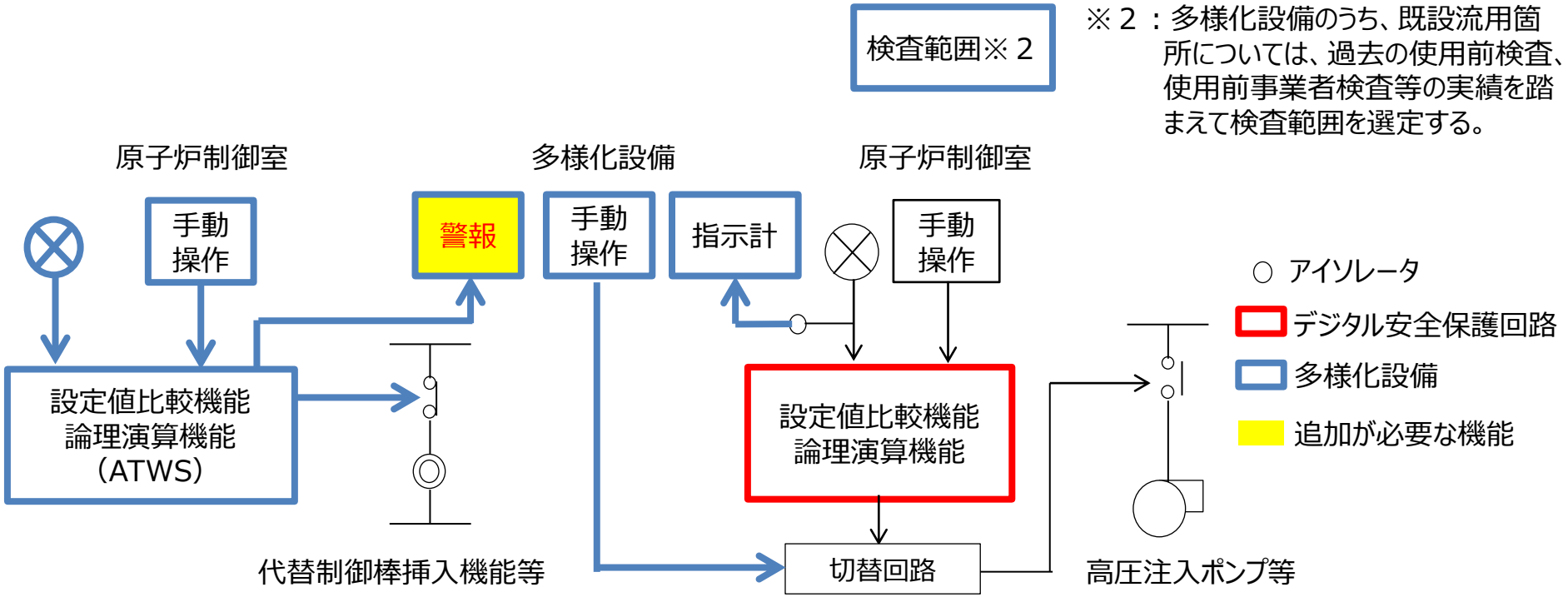
○多様化設備のうち新規設置箇所
○多様化設備のうち既設流用箇所については、過去の使用前検査、使用前事業者検査等の実績を踏まえて検査範囲を選定する。
○手順書の整備と教育及び訓練の実施

【PWRの検査範囲】



7．事業者自主検査の内容（2/5）

【ABWRの検査範囲※１】



※１：BWR（ABWRを除く）については、設備対応がないため、設備の検査範囲は対象なし。

7．事業者自主検査の内容（3/5）

事業者自主検査の具体的な内容を、川内1,2号機の例で示す。

【川内1,2号機の例】

（1）検査内容

○検査項目、検査方法

検査項目	検査方法
特性検査	設定値確認検査、応答時間測定検査
機能及び性能に係る検査	ロジック検査、警報機能検査、指示性能検査
運用に係る検査	手順書等が規定文書に定られていることを確認する

（2）検査体制

○使用前事業者検査と同等の検査担当者の独立性を担保する。

設計・工事箇所：保修課

検査担当箇所　：安全品質保証統括室

7．事業者自主検査の内容（4/5）

（３）特性検査の概要

検査項目	自動機能	手動操作	指示計	警報
設定値確認検査	対象設定値 ・加圧器圧力異常低による高圧／低圧注入系作動	–	–	–
応答時間測定検査	対象応答時間 ・加圧器圧力異常低による高圧／低圧注入系作動	–	–	–

（４）機能及び性能に係る検査の概要

検査項目	自動機能	手動操作	指示計	警報
ロジック検査	対象ロジック ・安全注入（高圧注入系／低圧注入系作動及び格納容器隔離（一部））	対象操作器 ・手動安全注入操作器	–	–
警報機能検査	–	–	–	対象警報 ・加圧器圧力異常低発生
指示性能検査	–	–	対象指示計 ・N35 ・燃料取替用水タンク水位 ・CV再循環サンプ水位	–

7．事業者自主検査の内容（5/5）

（５）運用に係る検査

技術要件書の要求項目	事業者自主検査での確認内容
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とソフトウェアCCFの重畳による事象が発生した場合に、運転員が必要な運転操作を実施し、事象を収束するための手順が、規定文書に定められていることを確認する。
5.2　教育及び訓練の実施	・　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、実施することが規定文書に定められていることを確認する。

8．自律的対応に係る事業者の管理体制等（1/2）

事業者は、自律的対応であるデジタルCCF対策に係る設備の保全計画、手順書の整備、教育・訓練および管理体制について以下のとおり管理する。

【川内1,2号機の例】（他のPWR、ABWR、BWRプラントも同様に管理する。）

（1）多様化設備の保全計画

◯保安規定に基づく規定文書の中で管理する。（保修基準、保全プログラム管理要領）

保全計画：点検頻度、点検方法、検査

検査項目：定期事業者検査と同等の自主検査

検査独立性：定期事業者検査と同等の独立性を担保

（2）デジタルCCF対策に係る手順書の整備および教育・訓練

◯保安規定に基づく規定文書の中で管理する。（運転基準、教育・訓練基準）

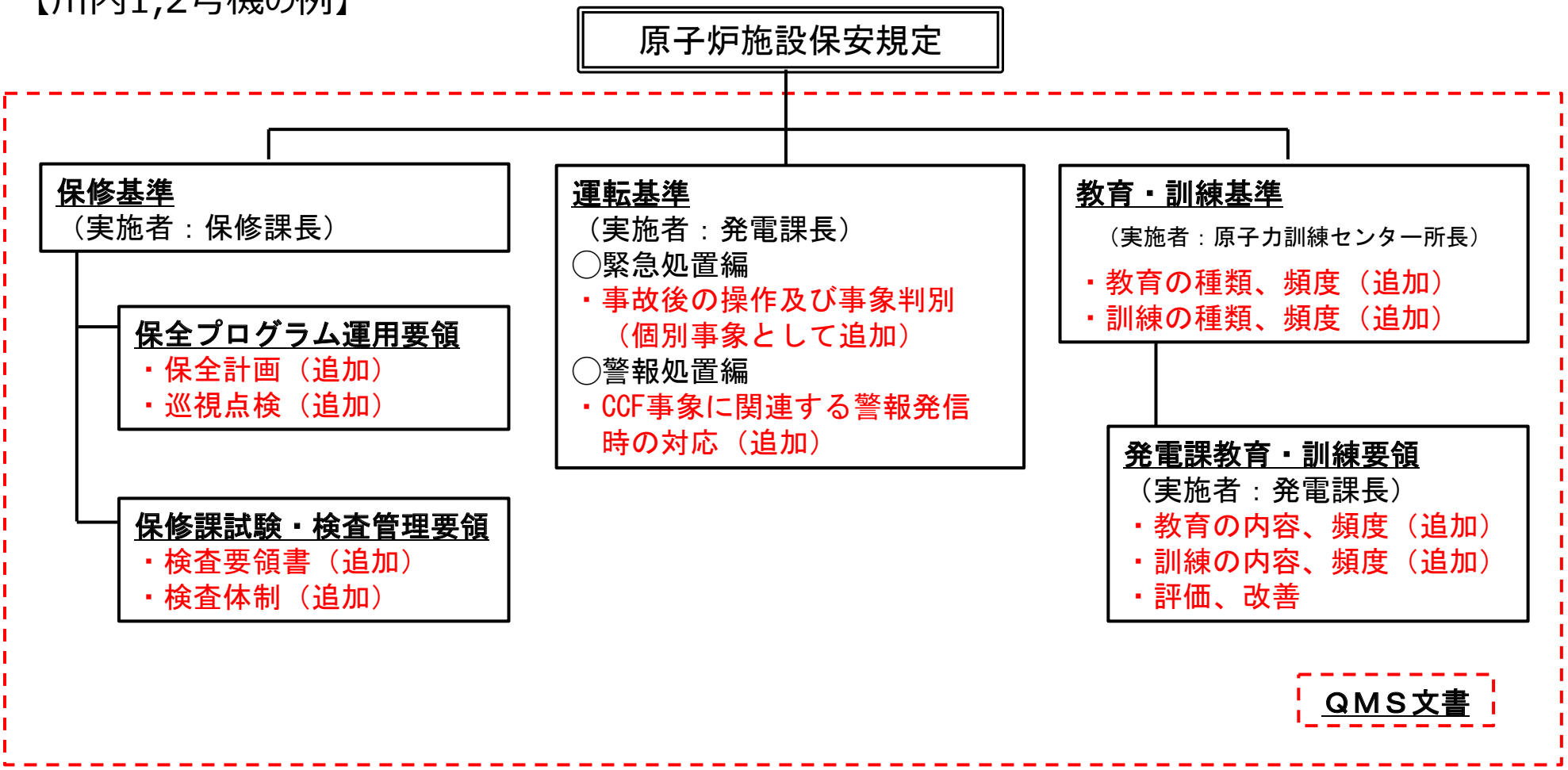
（3）デジタルCCF対策に係る管理体制

◯デジタルCCF対策に係る運転管理、施設管理、教育・訓練については、保安規定に定める保安管理体制のもとで管理する。

8．自律的対応に係る事業者の管理体制等（2/2）

保全計画、手順書の整備、教育・訓練および管理体制に係る文書体系を以下に示す。

【川内1,2号機の例】



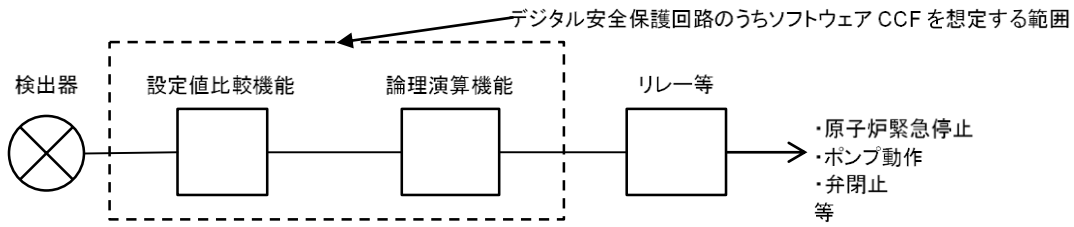
9．事業者の設計管理および検査実施の方法について

（１）ATENAは、事業者に対して、デジタルCCF対策工事にあたっての設計管理及び検査実施の方法について、報告を求める。

（２）事業者は、ATENAに対して、デジタルCCF対策工事にあたっての設計管理及び検査実施の方法について、設計及び工事の計画認可対象の工事と同等の方法で管理することを報告する。

（３）ATENAは、事業者から報告された、デジタルCCF対策工事にあたっての設計管理及び検査実施の方法について、そのプロセスを確認することにより、設計及び工事の計画認可対象の工事と同等の方法であることを確認する。

（添付１）技術要件書の記載内容（１/8）

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。

（添付１）技術要件書の記載内容（2/8）

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。

（添付１）技術要件書の記載内容（3/8）

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。

（添付１）技術要件書の記載内容（4/8）

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。

（添付１）技術要件書の記載内容（5/8）

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。

（添付１）技術要件書の記載内容（6/8）

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。

（添付１）技術要件書の記載内容（7/8）

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。

（添付１）技術要件書の記載内容（8/8）

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。

（添付２）要件整合報告書（例）（1/21）

（判定記号）○：整合有　－：該当なし

表1「3. 多様化設備要件」に関する要件整合性確認表(1/8)

ATENA 技術要件書	ソフトウェア CCF 対策設備設計図書の要件整合性			
	記載内容(概要)	要件整合性		設計図書
要求内容		判定	理由	
3.1 設置要求				
デジタル安全保護回路を設ける場合には，代替機能を有する多様化設備を設置しなければならない。	デジタル安全保護回路の代替機能を有する、多様化設備である共通要因故障対策設備を設置する。	○	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機能をすべて喪失し、かつ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設計基準事故の判断基準を概ね満足することができる設備を共通要因故障対策設備として設けていることを設計図書により確認した。 具体的な代替機能は 3.2 項にて、共通要因故障対策設備の範囲は 3.3 項にて確認した。	・デジタル安全保護系共通要因故障対策基本方針書 3.2 章(39/56) ・多様化設備基本設計方針書(川内 1 号機、川内 2 号機) 2 章
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，他の安全保護回路の安全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。	－	－	－	－

（添付２）要件整合報告書（例）（2/21）

（判定記号）○：整合有　－：該当なし

表1 「3. 多様化設備要件」に関する要件整合性確認表(2/8)

ATENA 技術要件書	ソフトウェア CCF 対策設備設計図書の要件整合性			
	記載内容(概要)	要件整合性		設計図書
要求内容		判定	理由	
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ない。	デジタル安全保護回路が共通要因故障によってその機能をすべて喪失し，かつ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設計基準事故の判断基準を概ね満足することができる設備を共通要因故障対策設備として設ける。 多様化設備である共通要因故障対策設備には，ソフトウェア CCF 対策として，原子炉停止系統及び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るように、以下の機能を設ける。 ・自動作動機能 自動原子炉トリップ 自動安全注入作動　他 (別表1「共通要因故障対策設備が有する自動作動機能一覧表」参照) ・手動操作機能 手動原子炉トリップ他 手動安全注入作動　他 (別表2「共通要因故障対策設備が有する手動作動機能一覧表」参照) ・警報機能 多様化自動作動設備作動警報　他 (別表3「共通要因故障対策設備が有する警報機能一覧表」参照) ・指示機能 蒸気発生器水位(狭域)指示　他 加圧器水位指示　他 (別表4「共通要因故障対策設備が有する指示機能一覧表」参照)	○	デジタル安全保護回路がソフトウェア CCF によってその機能をすべて喪失し，かつ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設計基準事故の判断基準を概ね満足できるように、多様化設備である共通要因故障対策設備には自動作動機能、手動操作機能、警報機能及び指示機能を設けていることを設計図書により確認した。	・デジタル安全保護系共通要因故障対策基本方針書 3.2 章(39/56) ・原子炉制御保護系ファンクナルダイヤグラム(川内 1 号機、川内 2 号機) シート 19 ・補機インターロック線図(川内 1 号機) SHEET NO.0-5、2-10、2-11、2-14-1、2-36、3-3、3-5、4-1、4-6、7-7、7-8、7-10 ・補機インターロック線図(川内 2 号機) SHEET NO.0-5、2-10、2-11、2-14、2-37、3-3、3-5、4-1、4-6、7-7、7-8、7-10 ・多様化設備基本設計方針書(川内 1 号機，川内 2 号機) 6 章
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又は設計基準事故の発生時に安全保護回路の安全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。	多様化設備である共通要因故障対策設備を用いて原子炉停止系統、工学的安全施設等を手動操作する場合に、運転員が必要な時間内に開始できるよう，ソフトウェアCCF 対策として必要なパラメータの監視及び共通要因故障対策設備から作動させた原子炉停止系統及び工学的安全施設等の機器の状態の監視が可能な設計とするとともに、ソフトウェア CCF 時に必要な原子炉停止系統及び工学的安全施設等の手動操作ができる設計とする。また、共通要因故障対策設備が自動作動したことを、吹鳴装置を設け表示灯点灯と共に吹鳴音にて告知する設計とする。	○	多様化設備である共通要因故障対策設備の自動作動機能が動作すると，中央制御室に「多様化自動作動設備作動警報」が発信する。これにより、デジタル安全保護回路がソフトウェア CCF によりすべて機能喪失し，かつ運転時の異常な過渡変化又は設計基準事故が発生したことを検知でき、検知後は、運転員が必要な時間内に手動操作を開始できることを設計図書により確認した。	・デジタル安全保護系共通要因故障対策基本方針書 3.2 章(39/56)

（添付２）要件整合報告書（例）（3/21）

（判定記号）○：整合有　－：該当なし

表1 「3. 多様化設備要件」に関する要件整合性確認表(3/8)

ATENA 技術要件書	ソフトウェア CCF 対策設備設計図書の要件整合性			
	記載内容(概要)	要件整合性		設計図書
要求内容		判定	理由	
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。 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)も多様化設備として用いることができる。 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。	多様化設備である共通要因故障対策設備の範囲は以下の①～⑥である。 ①検出器 蒸気発生器水位(狭域)検出器 加圧器圧力検出器　他 (別表4「共通要因故障対策設備が有する指示機能一覧表」参照) ②操作器 手動原子炉トリップ操作器 手動安全注入操作器　他 (別表2「共通要因故障対策設備が有する手動作動機能一覧表」参照) ③論理回路 多様化自動作動設備 (個別の論理回路については別表1「共通要因故障対策設備が有する自動作動機能一覧表」参照) ④指示計 蒸気発生器水位(狭域)指示 加圧器水位指示　他 (別表4「共通要因故障対策設備が有する指示機能一覧表」参照) ⑤警報 多様化自動作動設備作動警報　他 (別表3「共通要因故障対策設備が有する警報機能一覧表」参照) ⑥表示灯 自動作動及び手動操作による弁・補機動作状態の表示灯 ⑦その他 原子炉保護系計器ラック(炉外核計測装置含むアナログ回路部) 補機制御設備(安全保護系補助リレーラックトレンA及びB、安全保護系シーケンスキャビネットトレンA及びB)	○	多様化設備である共通要因故障対策設備の対象範囲が、設計図書にて明確化されていることを確認した。	・多様化設備基本設計方針書(川内１号機、川内２号機)２章、6.1.1 章、6.1.2 章、6.1.4 章、6.1.5 章、図 6-1

（添付２）要件整合報告書（例）（4/21）

（判定記号）○：整合有　－：該当なし

表1 「3. 多様化設備要件」に関する要件整合性確認表(4/8)

ATENA 技術要件書	ソフトウェア CCF 対策設備設計図書の要件整合性			
	記載内容(概要)	要件整合性		設計図書
要求内容		判定	理由	
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，多様化設備に対しては，設計上，単一故障を考慮しない。 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 との重畳を考慮しない。 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。	本項は基本方針を述べたものであり、具体的には「3.5 多様化設備への要求事項」で、耐環境性、耐震性、供給電源等について個別に記載している。	－	本項は基本方針を述べたものであり、具体的には「3.5 多様化設備への要求事項」で、耐環境性、耐震性、供給電源等について個別に確認した。	－

（添付２）要件整合報告書（例）（5/21）

（判定記号）○：整合有　－：該当なし

表1 「3. 多様化設備要件」に関する要件整合性確認表(5/8)

ATENA 技術要件書	ソフトウェア CCF 対策設備設計図書の要件整合性			
	記載内容(概要)	要件整合性		設計図書
要求内容		判定	理由	
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。	多様化設備である共通要因故障対策設備自体には多重性は不要である。	○	多様化設備である共通要因故障対策設備は、設計想定外の設備であるため、作動機能の維持について構成機器もしくはチャンネルに単一故障もしくは試験または保守のための使用状態からの取り外しを想定する必要はない設計方針としていることを、設計図書により確認した。	・デジタル安全保護系共通要因故障対策基本方針書 3.2 章(39/56) ・多様化設備基本設計方針書(川内 1 号機、川内 2 号機) 5.3 章
3.5.2 多様性				
多様化設備自体には，多様性は要求しない。	多様化設備である共通要因故障対策設備自体には多様性は不要である。	○	多様化設備である共通要因故障対策設備自体には多様性不要とする設計方針としていることを設計図書により確認した。	・デジタル安全保護系共通要因故障対策基本方針書 3.2 章(40/56) ・多様化設備基本設計方針書(川内 1 号機、川内 2 号機) 5.4.1 章、5.18 章
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。	多様化設備である共通要因故障対策設備は、デジタル安全保護回路とは独立、かつ多様性のある別設備で構成し、ソフトウェア CCF の影響で各機能の遂行が阻害されることが無いようにする。	○	多様化設備である共通要因故障対策設備は、デジタル安全保護回路の共通故障要因によって機能が阻害されないように、ハード回路を用いた設計としていることを、設計図書により確認した。また、多様化設備である共通要因故障対策設備は、安全保護設備のソフトウェアの共通故障要因によって作動機能を失わないように、安全保護設備のソフトウェア処理機能を介さずに作動可能な設計としていることを、設計図書により確認した。	・デジタル安全保護系共通要因故障対策基本方針書 3.2 章(40/56) ・多様化設備基本設計方針書(川内 1 号機、川内 2 号機) 5.4.1 章
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。	多様化設備である共通要因故障対策設備は、「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。	○	多様化設備である共通要因故障対策設備は、設置場所における「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 が重畳する環境下で所定の機能が果たせる設計としていること、を設計図書により確認した。	・デジタル安全保護系共通要因故障対策基本方針書 3.2 章(40/56) ・多様化設備基本設計方針書(川内 1 号機、川内 2 号機) 5.11 章

（添付２）要件整合報告書（例）（6/21）

（判定記号）○：整合有　－：該当なし

表1 「3. 多様化設備要件」に関する要件整合性確認表(6/8)

ATENA 技術要件書	ソフトウェア CCF 対策設備設計図書の要件整合性			
	記載内容(概要)	要件整合性		設計図書
要求内容		判定	理由	
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。	多様化設備である共通要因故障対策設備は、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。	○	多様化設備である共通要因故障対策設備は、基準地震動Ssによる地震力に対し機能維持するものとしている。多様化設備である共通要因故障対策設備のうち設計基準対象施設と兼用しておらず、個別の耐震評価が必要な多様化自動作動設備については、基準地震動 Ss による地震力に対し機能維持できることを設計図書(耐震計算書)により確認した。	・デジタル安全保護系共通要因故障対策基本方針書 3.2 章(40/56) ・多様化自動設備(ATWS 緩和設備)の耐震計算書(川内 1 号機、川内 2 号機)
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。	多様化設備である共通要因故障対策設備は、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。	○	多様化設備である共通要因故障対策設備は、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していることを設計図書により確認した。	・デジタル安全保護系共通要因故障対策基本方針書 3.2 章(40/56) ・多様化設備基本設計方針書(川内 1 号機、川内 2 号機) 5.16 章
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。	多様化設備である共通要因故障対策設備は、二以上の発電用原子炉施設において共用及び相互接続しない設計とする。	○	多様化設備である共通要因故障対策設備は、二以上の発電用原子炉施設にて共用及び相互接続しないものとしていることを設計図書により確認した。	・デジタル安全保護系共通要因故障対策基本方針書 3.2 章(40/56) ・多様化設備基本設計方針書(川内 1 号機、川内 2 号機) 5.19 章
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。	多様化設備である共通要因故障対策設備は、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。	○	多様化設備である共通要因故障対策設備は、定検時において、模擬信号あるいは実動作によって設定値・ロジックなどの機能が確認できる設計としていることを設計図書により確認した。	・デジタル安全保護系共通要因故障対策基本方針書 3.2 章(40/56) ・多様化設備基本設計方針書(川内 1 号機、川内 2 号機) 5.6 章
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を喪失させない設計とすること。	多様化設備である共通要因故障対策設備は、共通要因故障対策設備の故障影響により安全保護系の安全機能が喪失しない設計とする。	○	安全保護回路と共通要因故障対策設備が部分的に設備を共用する場合には、共通要因故障対策設備の影響により安全保護機能を失わないように、安全保護回路は共通要因故障対策設備から電気的・機能的に分離した設計であることを設計図書により確認した。	・デジタル安全保護系共通要因故障対策基本方針書 3.2 章(40/56) ・多様化設備基本設計方針書(川内 1 号機、川内 2 号機) 5.5 章

（添付２）要件整合報告書（例）（7/21）

（判定記号）○：整合有　－：該当なし

表1 「3. 多様化設備要件」に関する要件整合性確認表(7/8)

ATENA 技術要件書	ソフトウェア CCF 対策設備設計図書の要件整合性			
	記載内容(概要)	要件整合性		設計図書
要求内容		判定	理由	
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。	多様化設備である共通要因故障対策設備は、火災・溢水の影響を受けたとしても、安全保護系の安全機能が喪失しない設計とする。	○	・仮に、多様化設備である共通要因故障対策設備が火災・溢水の影響を受けて機能喪失したとしても、多重性を有した安全保護回路の安全機能を喪失させない設計であることを、設計図書により確認した。 ・多様化設備である共通要因故障対策設備は、実用上可能な限り不燃性または難燃性材料を設備構成品に使用し、内部火災等への耐性を可能な限り有する設計であることを、設計図書により確認した。	・デジタル安全保護系共通要因故障対策基本方針書 3.2 章(40/56) ・多様化設備基本設計方針書(川内 1 号機、川内 2 号機) 5.14 章
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を喪失させない設計とすること。	多様化設備である共通要因故障対策設備は、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、その他の機器又は配管の損壊に伴う飛散物等に対して、共通要因故障対策設備が影響を受けない設計とする、又は、共通要因故障対策設備が影響を受けても安全機能が喪失しない設計とする。	○	発電所で考慮する自然現象及び外部人為事象等に対して、共通要因故障対策設備の受ける影響評価を行った結果、これらの事象に対して多様化設備である共通要因故障対策設備が影響を受けない、または影響を受けたとしても、安全保護系の機能を喪失しないことを確認した。 各事象に対する共通要因故障対策設備への影響評価を別表5「共通要因故障対策設備の自然現象、外部人為事象等に対する影響評価整理表」に示す。	・デジタル安全保護系共通要因故障対策基本方針書 3.2 章(40/56) ・多様化設備基本設計方針書(川内 1 号機、川内 2 号機) 5.12 章
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。	多様化設備である共通要因故障対策設備のうち手動操作器は、中央制御室に設置する。また、操作器は誤操作防止を考慮した設計とする。	○	誤操作防止が図られたハード操作器及び表示を 3.3 項の操作スイッチ及び表示として中央制御室に設置する設計としていることを設計図書により確認した。	・デジタル安全保護系共通要因故障対策基本方針書 3.2 章(40/56) ・多様化設備基本設計方針書(川内 1 号機、川内 2 号機)5.15.1 章、6.1.2 章
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。	－	－	－	－

（添付２）要件整合報告書（例）（8/21）

（判定記号）○：整合有　－：該当なし

表1 「3. 多様化設備要件」に関する要件整合性確認表(8/ 8)

ATENA 技術要件書	ソフトウェア CCF 対策設備設計図書の要件整合性			
	記載内容(概要)	要件整合性		設計図書
要求内容		判定	理由	
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。	多様化設備である共通要因故障対策設備のうち、事象発生の検知や、事象の判定及び対応操作の判断に必要な警報機能や監視機能は、中央制御室に設置する。	○	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 が重畳した事象を認知できる警報として、3.2 項、3.3 項及び別表3「共通要因故障対策設備が有する警報機能一覧表」で示した多様化自動作動設備作動警報を中央制御室に告知する設計としていることを、設計図書により確認した。 事象の判定及び対応操作に必要な監視設備として、3.2 項、3.3 項及び別表4「共通要因故障対策設備が有する指示機能一覧表」で示した指示計を中央制御室に設置する設計としていることを、設計図書により確認した。	・デジタル安全保護系共通要因故障対策基本方針書 3.2 章(40/56) ・多様化設備基本設計方針書(川内 1 号機、川内 2 号機) 5.15.1 章、6.1.4 章、6.1.5 章
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。	多様化設備である共通要因故障対策設備の論理回路（多様化自動作動設備）が自動作動した場合には、中央制御室の原子炉補助盤裏面の多様化自動作動設備表示パネルに警報が出力・表示される設計とする。	○	多様化自動作動設備が自動で作動した場合には、3.2 項、3.3 項及び別表3「共通要因故障対策設備が有する警報機能一覧表」で示したとおり、各警報が中央制御室に表示される設計としていることを、設計図書により確認した。	・多様化設備基本設計方針書(川内 1 号機、川内 2 号機) 5.15.1 章、6.1.4 章、6.1.5 章

（添付２）要件整合報告書（例）（9/21）

（判定記号）○：整合有　－：該当なし

表２「4. 有効性評価」に関する要件整合性確認表(1/ 13)

ATENA 技術要件書	ソフトウェア CCF 対策有効性評価図書の要件整合性			
		要件整合性		
要求内容	記載内容（概要）	判定	理由	有効性評価図書
4.2 評価すべき事象				
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に評価	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ため、「運転時の異常な過渡変化」及び「設計基準事故」の全事象を有効性評価の対象とする。	○	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ている。	3.2 事象選定の基本的考え（P.8）
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を確認し，その妥当性を示すこと。	－	○	評価すべき事象において、グルーピングは考慮していない。	3.3 有効性評価事象（P.9）
以下に該当する場合は解析を省略できる。 ・判断基準に対して影響の程度が軽微である事象	以下の事象は判定基準に対して影響が軽微であるため、解析を省略する。 ・運転時の異常な過渡変化 ・蒸気発生器伝熱管破損 ・可燃性ガスの発生 ・被ばく評価全般 「運転時の異常な過渡変化」にソフトウェア CCF が重畳した場合、多様化設備の作動により原子炉トリップに至るため、原子炉停止機能喪失	○	対象事象は判定基準に対して影響が軽微であることを示している。	3.3.1 運転時の異常な過渡変化（P.9） 3.3.2 設計基準事故（P.10） 4.4 運転時の異常な過渡変化（P.22, P.30） 4.5.7 蒸気発生器伝熱管破損（P181, P.189）

（添付２）要件整合報告書（例）（10/21）

（判定記号）○：整合有　－：該当なし

表２「4. 有効性評価」に関する要件整合性確認表(2/ 13)

ATENA 技術要件書	ソフトウェア CCF 対策有効性評価図書の要件整合性			
		要件整合性		
要求内容	記載内容（概要）	判定	理由	有効性評価図書
	（ATWS） の有効性評価（原子炉トリップしない仮定）よりも事象進展が緩和される。したがって、この場合、判断基準に照らし合わせて影響の程度が軽微であり、解析を省略する。 蒸気発生器伝熱管破損について、ソフトウェア CCF の重畳を考慮した場合における運転操作や操作時間が添付書類十解析と同等であり、判断基準に照らし合わせて影響の程度が軽微であるため解析を省略する。また、当該事象に関する定性的な検討について述べている。 「可燃性ガスの発生」及び「環境への放射性物質の異常な放出」に分類される事象の被ばく評価については、判断基準に照らし合わせて影響の程度が軽微であるため解析を省略する。また、これら評価への影響について述べている。			4.6.2.3 可燃性ガスの発生（P.217） 4.6.3 被ばく評価への影響（P.228～P.233）

（添付２）要件整合報告書（例）（11/21）

（判定記号）○：整合有　－：該当なし

表２「4. 有効性評価」に関する要件整合性確認表(3/ 13)

ATENA 技術要件書	ソフトウェア CCF 対策有効性評価図書の要件整合性			
		要件整合性		
要求内容	記載内容（概要）	判定	理由	有効性評価図書
・グルーピングしたグループ内の代表事象に包絡される事象	－	○	評価すべき事象において、グルーピングは考慮していない	3.2 事象選定の基本的考え（P.9）
・デジタル安全保護回路の動作を期待しない事象	下記事象については、デジタル安全保護回路の動作を期待していないプラントでは、解析を省略する。 ・燃料集合体落下 ・放射性気体廃棄物処理施設の破損	○	デジタル安全保護回路の動作を期待していない事象については解析を省略している。	4.6.3.1 放射性気体廃棄物処理施設の破損（P.229） 4.6.3.3 燃料集合体の落下（P.231）

（添付２）要件整合報告書（例）（12/21）

（判定記号）○：整合有　－：該当なし

表２「4. 有効性評価」に関する要件整合性確認表(4/ 13)

ATENA 技術要件書	ソフトウェア CCF 対策有効性評価図書の要件整合性			
		要件整合性		
要求内容	記載内容(概要)	判定	理由	有効性評価図書
4.3 判断基準				
全事象に対して判断基準は設計基準事故において使用される判断基準を準用し，その判断基準を概ね満足することの確認を行う。	全事象に対する判断基準として設計基準事故において使用される判断基準を準用する。 また、解析等により判断基準を概ね満足することを確認している。	○	設計基準事故において使用される判断基準を準用し、その判断基準を概ね満足することの確認を行うこととしている。	4.1 判断基準(P.11) 4.4 運転時の異常な過渡変化 4.5 設計基準事故
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。	原子炉格納容器の最高使用圧力/温度を上回る場合の判断基準として、既許認可で確認された原子炉格納容器の限界圧力(最高使用圧力の 2 倍)／限界温度(200℃)を設定している。	○	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/限界温度を判断基準として設定している。	4.1 判断基準(P.11)

（添付２）要件整合報告書（例）（13/21）

（判定記号）○：整合有　－：該当なし

表２「4. 有効性評価」に関する要件整合性確認表(5/ 13)

ATENA 技術要件書	ソフトウェア CCF 対策有効性評価図書の要件整合性			
		要件整合性		
要求内容	記載内容(概要)	判定	理由	有効性評価図書
4.4 解析に当たって考慮すべき事項				
最適評価コードにより，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。	「原子炉冷却材喪失」以外の事象については，最適評価コードを適用する。	○	最適評価コードの適用を示している。	4.2 解析に使用する計算プログラム (P.12)
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，保守的評価を採用してもよい。	解析対象とする「原子炉冷却材喪失」については，現行措置及び追加措置の多様化設備により，設置変更許可申請書 添付書類十解析（設計基準事故）と同様の過渡応答になると考えられ，最適評価を適用する必要はないと判断されるため，添付書類十解析と同じ保守的評価を適用する。	○	保守的な評価コードの適用を示すとともに，その理由を記載している。	4.2 解析に使用する計算プログラム (P.12)

（添付２）要件整合報告書（例）（14/21）

（判定記号）○：整合有　－：該当なし

表２「4. 有効性評価」に関する要件整合性確認表(6/ 13)

ATENA 技術要件書	ソフトウェア CCF 対策有効性評価図書の要件整合性			
		要件整合性		
要求内容	記載内容(概要)	判定	理由	有効性評価図書
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。	設置変更許可申請書 添付書類十解析(設計基準事故)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」の要求に従い、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、判断基準に照らして最も厳しくなる初期状態(解析条件)を選定している。ソフトウェア CCF 対策の有効性評価についても、この方針に従い解析条件を設定している。	○	添付書類十解析と同様に、全ての運転範囲及び運転期間を包絡する解析条件を設定している。	4.3 基本解析条件 (P.14)
解析は，想定した事象が，判断基準をほぼ満足しながら，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。	添付書類十解析と同様、事象発生から安定状態へ移行できると合理的に判断できる時点までの解析結果(グラフ)を示している。	○	事象発生から、注水等によりプラント状態が安定状態へ移行できると判断でき、かつ主要パラメータの傾向が事象収束の方向にあると判断できる時点まで解析を実施している。	4.4 運転時の異常な過渡変化 (各グラフ) 4.5 設計基準事故 (各グラフ)

（添付２）要件整合報告書（例）（15/21）

（判定記号）○：整合有　－：該当なし

表２「4. 有効性評価」に関する要件整合性確認表(7/ 13)

ATENA 技術要件書	ソフトウェア CCF 対策有効性評価図書の要件整合性			
		要件整合性		
要求内容	記載内容(概要)	判定	理由	有効性評価図書
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こと。その場合には，安全設計の妥当性確認に用いる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。	プラント初期条件及び設定根拠を、解析条件として示している。また、添付書類十解析と異なる条件を用いたものは、差異及び根拠を示している。	○	プラント初期条件及び設定根拠が示されている。	4.3 基本解析条件 (P.14) 4.4 運転時の異常な過渡変化 (各主要解析条件表) 4.5 設計基準事故 (各主要解析条件表) 添付 1-1, 添付 1-2
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こと。その場合には，安全設計の妥当性確認に用いる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。	事象発生による外乱の程度、炉心状態、機器容量等の解析条件及び設定根拠を示している。また、添付書類十解析と異なる条件を用いたものは、差異及び根拠を示している。	○	解析条件及び根拠が示されている。	4.3 基本解析条件 (P.14) 4.4 運転時の異常な過渡変化 (各主要解析条件表) 4.5 設計基準事故 (各主要解析条件表) 添付 1-1, 添付 1-2
作動設定点等については計装上の誤差は考慮しなくともよい。	自動起動を期待する多様化設備の作動設定点として保護限界値を設定し、解析条件としている。	○	多様化設備の作動設定点として、計装上の誤差を考慮して保守的に保護限界値を設定している。	4.3 基本解析条件 (P.16,P.17)

（添付２）要件整合報告書（例）（16/21）

（判定記号）○：整合有　－：該当なし

表２「4. 有効性評価」に関する要件整合性確認表(8/ 13)

ATENA 技術要件書	ソフトウェア CCF 対策有効性評価図書の要件整合性			
		要件整合性		
要求内容	記載内容(概要)	判定	理由	有効性評価図書
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こと。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。	－	○	誤操作が起因の一つとなる「運転時の異常な過渡変化」の評価では，「主給水流量喪失」を代表として有効性評価を実施している。「主給水流量喪失」はポンプ等の故障が起因事象であることから、現実的な操作の条件を設定する必要はない。	4.4 運転時の異常な過渡変化 (P.18)
4.4.3 安全系機能に対する仮定				
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。	各事象においてデジタル安全保護回路の機能喪失に伴い、本設の原子炉停止系統及び工学的安全施設が動作しないことを解析条件としている。	○	ソフトウェア CCF による機能喪失を解析条件に反映している。	4.3 基本解析条件(P.14) 4.4 運転時の異常な過渡変化 (各主要解析条件表) 4.5 設計基準事故 (各主要解析条件表)
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。	「原子炉格納容器健全性評価」において，デジタル安全保護回路の機能喪失に伴い自動起動しない格納容器スプレイ設備について、手動起動操作を解析条件としている。	○	ソフトウェア CCF による機能喪失への対応操作として、手動起動を解析条件として反映している。	4.3 基本解析条件(P.14) 4.5.8 原子炉格納容器健全性評価(P.196) 添付 1-3 運転員操作条件

（添付２）要件整合報告書（例）（17/21）

（判定記号）○：整合有　－：該当なし

表２「4. 有効性評価」に関する要件整合性確認表(9/ 13)

ATENA 技術要件書	ソフトウェア CCF 対策有効性評価図書の要件整合性			
		要件整合性		
要求内容	記載内容(概要)	判定	理由	有効性評価図書
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。	各事象において、起因事象による影響を受けない、安全機能を有する機器の単一故障は仮定していない。	○	起因事象の影響を受けない安全機能を有する機器の単一故障を解析条件としていない。	4.3 基本解析条件(P.14) 4.4 運転時の異常な過渡変化 (各主要解析条件表) 4.5 設計基準事故 (各主要解析条件表)
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。	起因事象との従属性がなく、かつソフトウェア CCF の影響を受けない安全機能のサポート系（電源系、冷却系、空調系等）の作動状態を想定する。また、これらのサポート系を利用した原子炉停止系統及び工学的安全施設の作動を仮定する。	○	必要な安全機能に対するサポート系について、起因事象及びソフトウェア CCF の影響を受けないことを確認している。	4.3 基本解析条件(P.14) 添付２ 多様化設備が作動させる設備に対するサポート系の有効性
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。	起因事象が外部電源喪失である事象以外では、外部電源喪失は仮定していない。	○	起因事象が外部電源喪失である事象以外は、外部電源喪失を解析条件としていない。	4.3 基本解析条件 (P.14)

（添付２）要件整合報告書（例）（18/21）

（判定記号）○：整合有　－：該当なし

表２「4. 有効性評価」に関する要件整合性確認表(10/ 13)

ATENA 技術要件書	ソフトウェア CCF 対策有効性評価図書の要件整合性			
		要件整合性		
要求内容	記載内容（概要）	判定	理由	有効性評価図書
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。	事象発生前から機能している常用系設備は、機能喪失は仮定していない。	○	起因事象の影響を受けない常用系設備の機能喪失を解析条件としていない。	4.3 基本解析条件 (P.14)
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。	常用系機能の喪失が前提となる事象では、当該常用系の機能には期待していない。	○	常用系である各種制御系等の故障を起因とする事象では、事象発生後、その機能には期待していない。	4.3 基本解析条件 (P.15)
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。	－ （多様化設備の動作のクレジットを取ることの理由である。）	○	多重性が要求されない多様化設備の単一故障を想定していない。	－
・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。	－ （同上）	○	多様化設備が代替作動させる設備の故障及び誤動作が起因となる事象は想定していない。	－

（添付２）要件整合報告書（例）（19/21）

（判定記号）○：整合有　－：該当なし

表２「4. 有効性評価」に関する要件整合性確認表(11/ 13)

ATENA 技術要件書	ソフトウェア CCF 対策有効性評価図書の要件整合性			
		要件整合性		
要求内容	記載内容(概要)	判定	理由	有効性評価図書
・多様化設備が作動させる原子炉停止系統，工学的安全施設等は，そのサポート系（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。	多様化設備が作動させる原子炉停止系統、工学的安全施設等は、そのサポート系が使用できない場合には利用できないものとする。	○	多様化設備が作動させる設備は、そのサポート系が起因事象及びソフトウェア CCF の影響を受けず利用可能であることを確認している。	4.3 基本解析条件(P.14) 添付 2 多様化設備が作動させる設備に対するサポート系の有効性
(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。	有効性評価で期待している手動操作は、ハード対策（追加措置）完了までに整備される操作手順書に従い操作が適切に行われること、及び運転操作訓練が適切に行われることを前提としている。	○	解析上の運転員の手動操作の成立性が、運転員操作手順書、教育訓練により裏付けられることを示している。	4.3 基本解析条件(P.15) 添付 1-3 運転員操作条件

（添付２）要件整合報告書（例）（20/21）

（判定記号）○：整合有　－：該当なし

表２「4. 有効性評価」に関する要件整合性確認表(12/ 13)

ATENA 技術要件書	ソフトウェア CCF 対策有効性評価図書の要件整合性			
		要件整合性		
要求内容	記載内容(概要)	判定	理由	有効性評価図書
・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。	－	○	中央制御室での原子炉停止系統及び工学的安全施設の手動操作はない。	－
・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もよい。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。	有効性評価で期待している中央制御室以外での現場操作は、現場への移動時間，現場での操作時間の各所要時間に基づき、解析条件として設定している。	○	移動や操作に係る所要時間を計測し、根拠を明確にした上で、中央制御室以外での現場操作の成立性を確認している。	4.3 基本解析条件(P.15) 添付 1-3 運転員操作条件

（添付２）要件整合報告書（例）（21/21）

（判定記号）○：整合有　－：該当なし

表２「4. 有効性評価」に関する要件整合性確認表(13/ 13)

ATENA 技術要件書	ソフトウェア CCF 対策有効性評価図書の要件整合性			
		要件整合性		
要求内容	記載内容(概要)	判定	理由	有効性評価図書
4.4.6 解析に使用する計算プログラム及びモデル				
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。	有効性評価に用いた計算プログラム及びモデルについて詳述した他の資料を引用している。(「原子炉冷却材喪失」は設置変更許可申請書 添付書類十(設計基準事故)解析で用いているコードを使用，「原子炉冷却材喪失」以外の事象は SPARKLE-2 コードを使用)	○	解析で用いた計算プログラム及びモデルは，引用した他の資料から確認できる。	4.2 解析に使用する計算プログラム(P.12,13) 6. 参考文献(P.240)
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行わ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行われている場合には，妥当性確認及び検証は不要である。	有効性評価に用いた計算プログラム及びモデルの適用妥当性については，設置変更許可申請書 添付書類十解析(設計基準事故，重大事故等対策の有効性評価)での使用実績を記載するとともに，詳述した他の資料を引用している。	○	解析で用いた計算プログラム及びモデルの妥当性や許認可使用実績は，引用した他の資料から確認できる。	4.2 解析に使用する計算プログラム(P.12) 6. 参考文献(P.240)

（添付３）悪影響防止について（1/4）

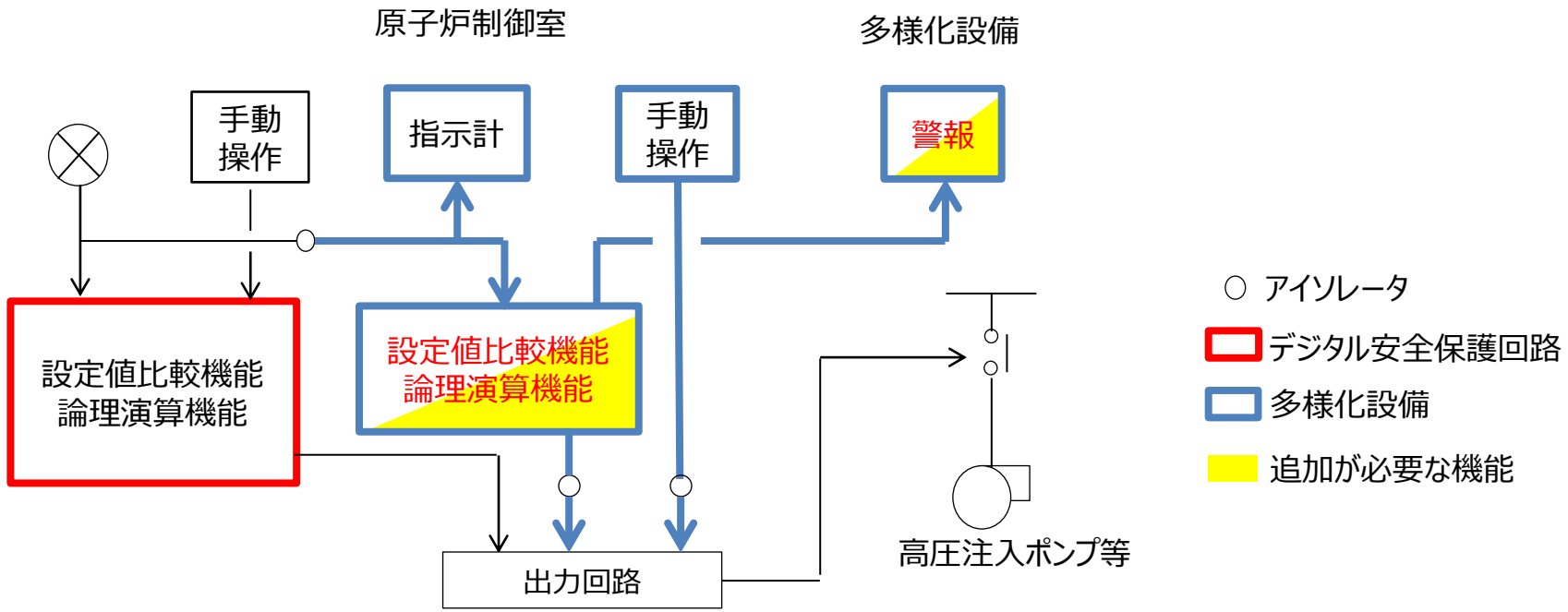
（１）設備面

多様化設備から安全系への悪影響防止のため、電気的分離と物理的分離を行っている。

◯電気的分離：多様化設備とデジタル安全保護回路の電気的分離を図る観点から、信号の取り合い部分にはアイソレータ（絶縁回路）を設置している。

◯物理的分離：多様化設備とデジタル安全保護回路の物理的分離を図る観点から、多様化設備は安全系と独立して設置している。

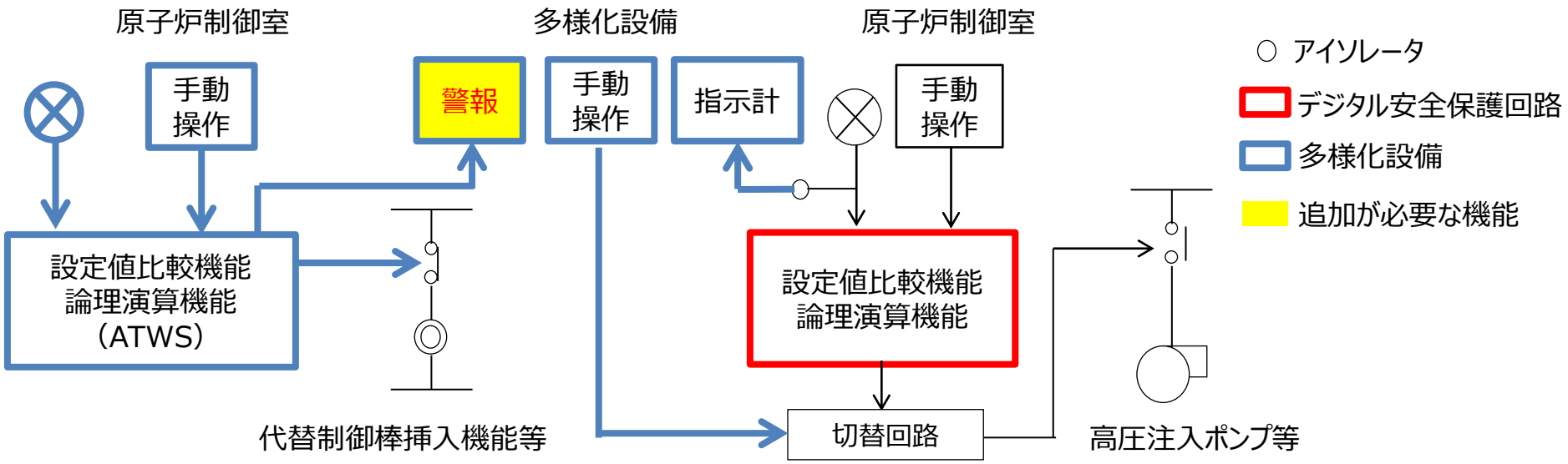
【PWRの例】



（添付３）悪影響防止について（2/4）

（１）設備面（つづき）

【ABWRの例】（BWRについては、設備対応がないため対象外）



（添付３）悪影響防止について（3/4）

（２）機能面

【PWRの例】

デジタル安全保護系が正常に動作した場合に、多様化設備が不必要に自動作動することのないよう、デジタル安全保護系が正常に作動したことを確認できる信号によって、多様化設備の作動をブロックできる設計としている。（自動作動阻止機能）

①原子炉トリップしゃ断器が正常に動作した場合は、多様化設備による原子炉トリップ、主蒸気隔離、タービントリップ、主給水隔離を自動的にブロックする。

②安全注入が正常に作動した場合には、多様化設備による安全注入を自動的にブロックする。

③プラント起動停止時などに多様化設備の不要な作動を防止するために、多様化設備の手動ブロック操作器により多様化設備からの信号をバイパス可能とする。

【ABWRの例】（BWRについては、設備対応がないため対象外）

①自動作動する代替制御棒挿入機能（ARI)と代替冷却材再循環ポンプ・トリップ機能（RPT)は、自主設置設備ではなくSA設備であるATWS設備を使用する。

②高圧炉心注水ポンプは手動起動のため、自動作動する安全保護系に影響を与えることはない。

（添付３）悪影響防止について（４/4）

（３）運転操作面

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の重畳による事象として、**独立した手順書**を整備することで、確実な事象判別、誤操作防止を図る。

また、技術要件書の要求内容を満足していることを事業者自主検査で確認する。

【技術要件書の要求内容】

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。