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17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（以下、「デジタルCCF対策」という。）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）、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、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・検査の段階にきている。

（４）今回の公開会合では、自律的対応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、事業者のデジタルCCF対策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、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対策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）

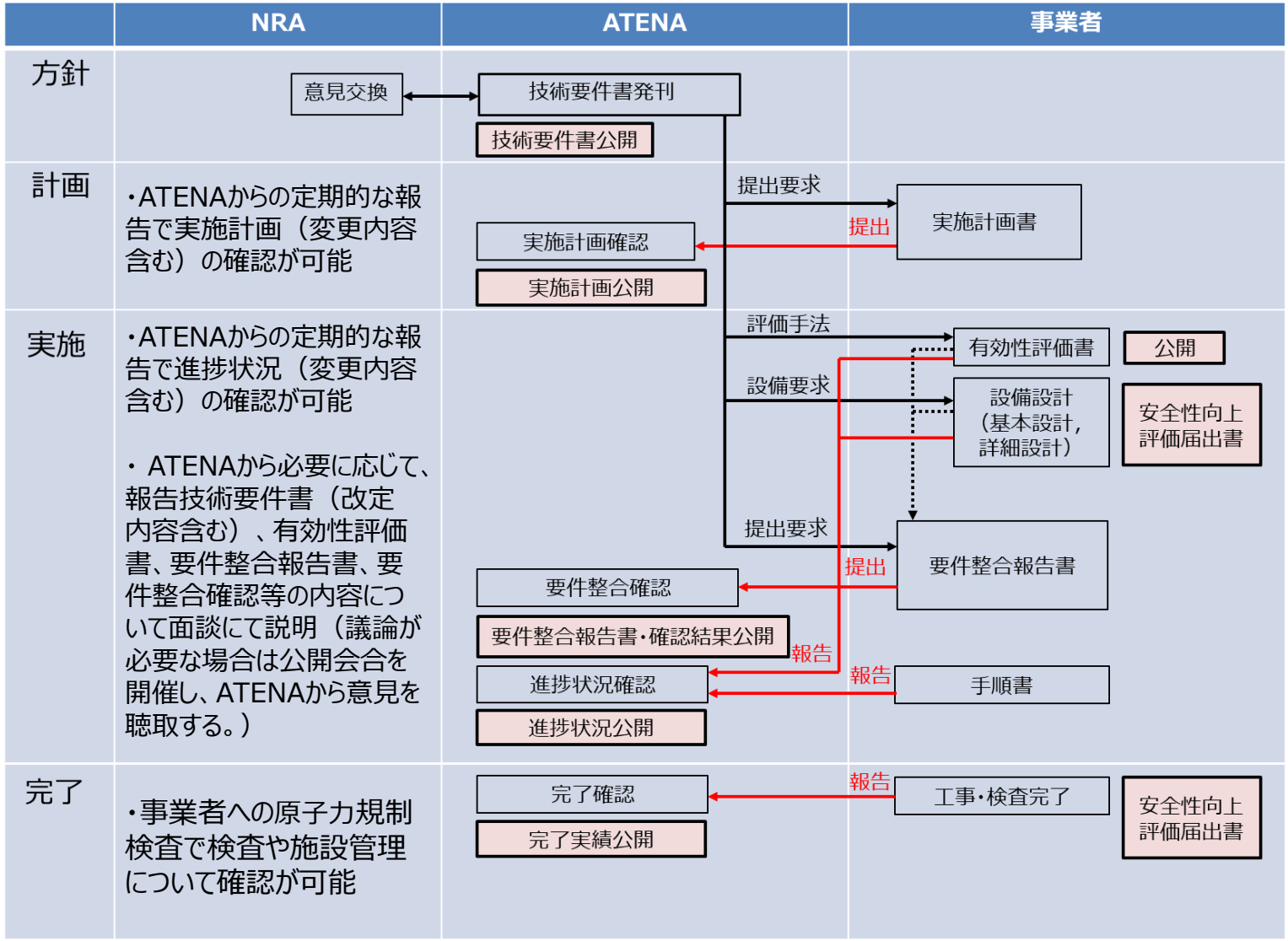


図１基本方針に基づく対応フロー

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. 手順書の整備と教育及び訓練の実施
 5.1 手順書の整備
 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

事業者自主検査で確認する範囲

4．事業者の要件整合報告（1/4）

（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
②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
③要求事項への整合性判定及びその理由
④設計図書名・図書番号と記載場所（ページ・表番号など）
⑤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、要件整合報告書を取りまとめ、承認プロセスと合わせて、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。

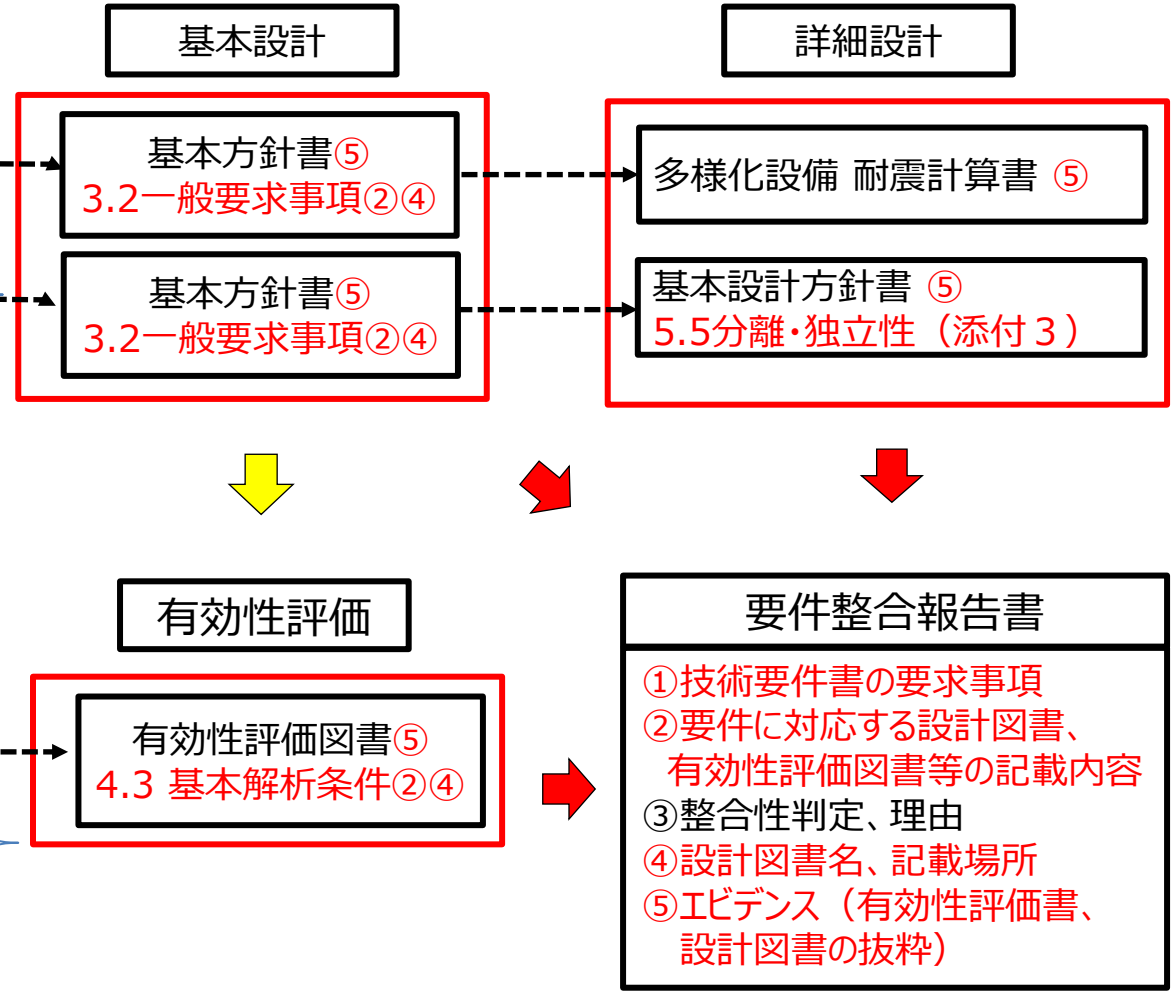
4．事業者の要件整合報告（2/4）

（４）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（例）を添付２に示す。）

ａ．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



4．事業者の要件整合報告（3/4）

（4）技術要件書に対する要件整合報告の概要（つづき）

b．要件整合報告書の具体例（「3.2機能要求」に関する要件整合性確認表）

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			
要求内容	記載内容（概要）	要件整合性		設計図書
		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（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（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（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（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CCF対策基本方針書 ・原子炉制御保護系ファンクショナルダイヤグラム ・補機インターロック線図

4．事業者の要件整合報告（4/4）

（４）技術要件書に対する要件整合報告の概要（つづき）

ｃ．要件整合報告書の具体例（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）

操作器の種類		個数	備考
原子炉トリップ		2	各操作器は 設計基準対象施設と共用
主給水隔離	Aループ	1	
	Bループ	1	
	Cループ	1	
主蒸気ライン隔離	Aループ	1	
	Bループ	1	
	Cループ	1	
安全注入作動		低圧注入/高圧注入　各１	
格納容器隔離動作		各ライン１	
補助給水隔離及び流量調節		各ループ１（合計３）	
主蒸気逃がし弁全開／全閉		3	
加圧器逃がし弁全開／全閉		2	

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．要件整合確認以降の対応方針について

デジタルCCF対策に関して、要件整合確認以降の工事・検査の段階における、事業者及びATENAの対応方針を以下に示す。

（1）事業者自主検査

事業者は、工事完了後に実施する事業者自主検査を、使用前事業者検査と同等の内容及び体制にて実施する。

（具体例）　7．事業者自主検査の対象　13

8．事業者自主検査の内容　16

（2）自律的対応に係る事業者の管理体制等

事業者は、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、保安規定に基づく規定文書及び保安管理体制で管理する。

（具体例）　9．自律的対応に係る事業者の管理体制等　23

（3）デジタルCCF対策工事にあたっての品質保証

・事業者は、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プロセスで管理する。

・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、設計及び工事の計画認可対象の工事と同等のプロセスで管理されていることを確認する。

7．事業者自主検査の対象（1/3）

技術要件書の要求項目に対して、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

多様化設備の仕様等については要件整合報告書で確認する。

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	－

7．事業者自主検査の対象（2/3）

（２）技術要件書「４.有効性評価」の要求項目

有効性評価については、要件整合報告書で確認する。

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
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	－

7．事業者自主検査の対象（3/3）

（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
手順書の整備後の運用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	技術要件書の要求内容	事業者自主検査の対象
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、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。	◯運用に係る検査 ・手順書が規定文書として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。	◯運用に係る検査 ・教育及び訓練の実施に関する内容が、規定文書に定められていることを確認する。

8．事業者自主検査の内容（1/7）

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設備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

（具体例）

（１）PWRの多様化設備の検査対象範囲（例） 17

（２）ABWR※の多様化設備の検査対象範囲（例） 18

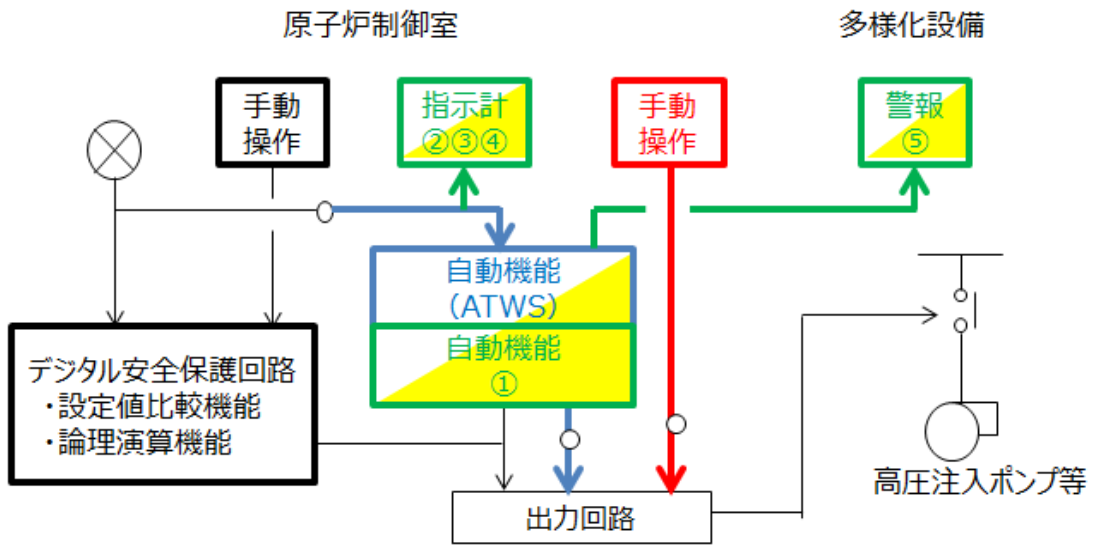
（３）事業者自主検査の具体的な内容 【川内1,2号機の例】 19

※ BWR（ABWRを除く）は、中性子計装・放射線計装・温度計装の設定値比較機能以外はアナログのため既設設備での対応が可能なことから、多様化設備は不要としている。

8．事業者自主検査の内容（2/7）

（１）PWRの多様化設備の検査範囲（例）

設備区分		自動機能	手動操作	指示計	警報
既設流用※	DB設備		・原子炉トリップ ・主給水隔離　・主蒸気隔離 ・補助給水隔離／流量調節 ・高圧／低圧注入系起動 ・格納容器隔離 ・主蒸気逃がし弁全開/全閉 ・加圧器逃がし弁全開/全閉		
	SA設備	・補助給水起動 ・主蒸気隔離			
	自主設備	・原子炉トリップ ・主給水隔離		・１次冷却材圧力 ・加圧器水位 ・主蒸気ライン圧力 ・蒸気発生器水位（狭域） ・格納容器圧力　他	・多様化設備作動 ・加圧器圧力低（原子炉トリップ等） ・加圧器圧力高（原子炉トリップ等） ・蒸気発生器水位低（原子炉トリップ等） ・蒸気発生器水位異常高
新規設置	自主設備	①高圧／低圧注入系起動		②中間領域中性子束 ③燃料取替用水タンク水位 ④格納容器再循環サンプ水位	⑤加圧器圧力異常低 （高圧／低圧注入系作動）



※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。

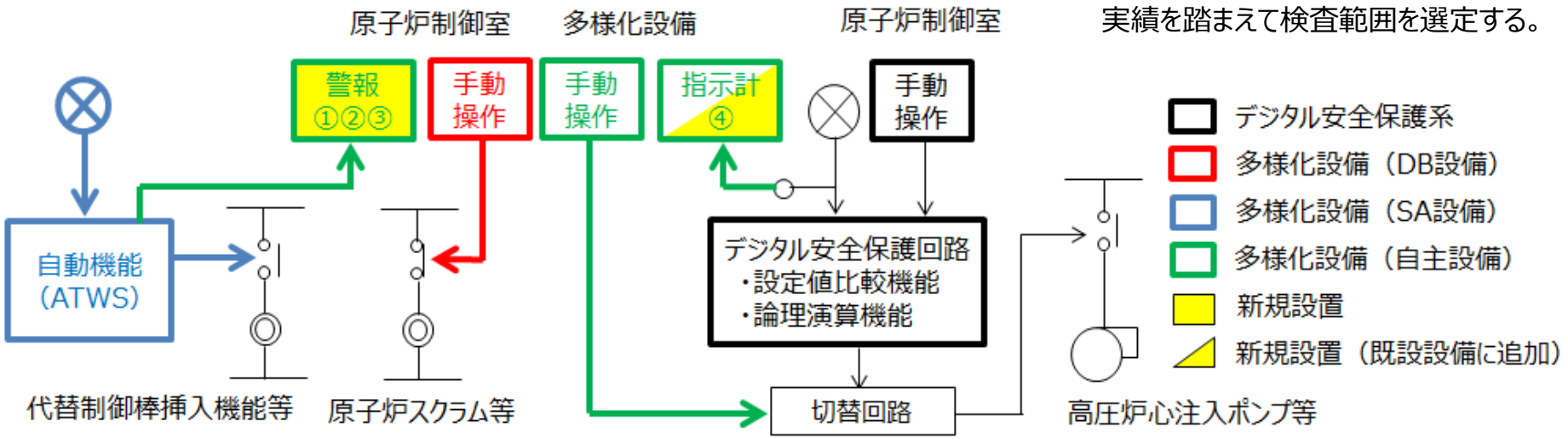
- デジタル安全保護系
- 多様化設備（DB設備）
- 多様化設備（SA設備）
- 多様化設備（自主設備）
- 新規設置（既設設備に追加）

8．事業者自主検査の内容（3/7）

（２）ABWRの多様化設備の検査範囲（例）

設備区分		自動機能	手動操作	指示計	警報
既設流用※	DB設備		・原子炉スクラム ・主蒸気隔離弁閉止		
	SA設備	・代替制御棒挿入機能 ・代替原子炉再循環ポンプトリップ		・原子炉水位 ・原子炉圧力	
	自主設備		・主要な隔離弁閉止 ・高圧炉心注水系起動	・主要な隔離弁の状態 ・高圧炉心注水系系統流量	
新規設置	自主設備			④ドライウェル圧力	①ARI作動 ②原子炉水位低 ③原子炉圧力高

※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。



8．事業者自主検査の内容（4/7）

（３）事業者自主検査の具体的な内容

【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	手順書等を規定文書に定め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

8．事業者自主検査の内容（5/7）

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）） ・自動作動阻止機能	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 ・中間領域中性子束 ・燃料取替用水タンク水位 ・CV再循環サンプ水位	－

8．事業者自主検査の内容（6/7）

⑤ 運用に係る検査

検査項目	確認内容
手順書の整備	◯手順書の内容が、技術要件書の要求内容に整合していること ◯手順書が規定文書として制定されていること 【主な確認項目】 ・デジタル安全保護回路の自動作動が要求されたときに原子炉停止系統及び工学的安全系施設が作動していないことを認知する手段を特定し、ソフトウェアCCF事象を判断する手順を整備する。 ・必要な手順書への移行の方法を明確化する。 ・手順書は、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し、安定状態が維持されるまでに必要な運転操作までを範囲とする。また、運転操作を行う場合の判断条件及び操作場所を記載する。（添付４参照） ・プラント状態を監視するための計器、及びその設置場所を手順書に記載する。

8．事業者自主検査の内容（7/7）

⑤ 運用に係る検査（つづき）

検査項目	確認内容
教育及び訓練の実施	○教育及び訓練の実施に関する内容が、技術要件書の要求内容に整合していること ○教育及び訓練の実施に関する内容が、規定文書に定められていること 【主な確認項目】 ・運転員に対して、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とソフトウェアCCFが重畳した場合に、原子炉停止系統及び工学的安全系施設が作動していないことを認知する手段、それがソフトウェアCCF事象であることの判断等について、的確に対処することができるように教育及び訓練を実施する。 ・運転員に対して、整備された手順書の内容について習熟を図ることができるよう、教育及び訓練を計画・実施する。 ・教育及び訓練の実施対象者 技術要件書に示されている技術要件に従い、ソフトウェアCCF影響緩和対策を実施するプラントの運転員を対象に教育及び訓練を実施する。

9．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、手順書の整備および教育・訓練、故障時の措置ならびに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）多様化設備の故障時の措置

◯保安規定に基づく規定文書の中で管理する。（保修基準）

多様化設備が故障等により機能喪失した場合の代替措置等の対応方針を検討する。

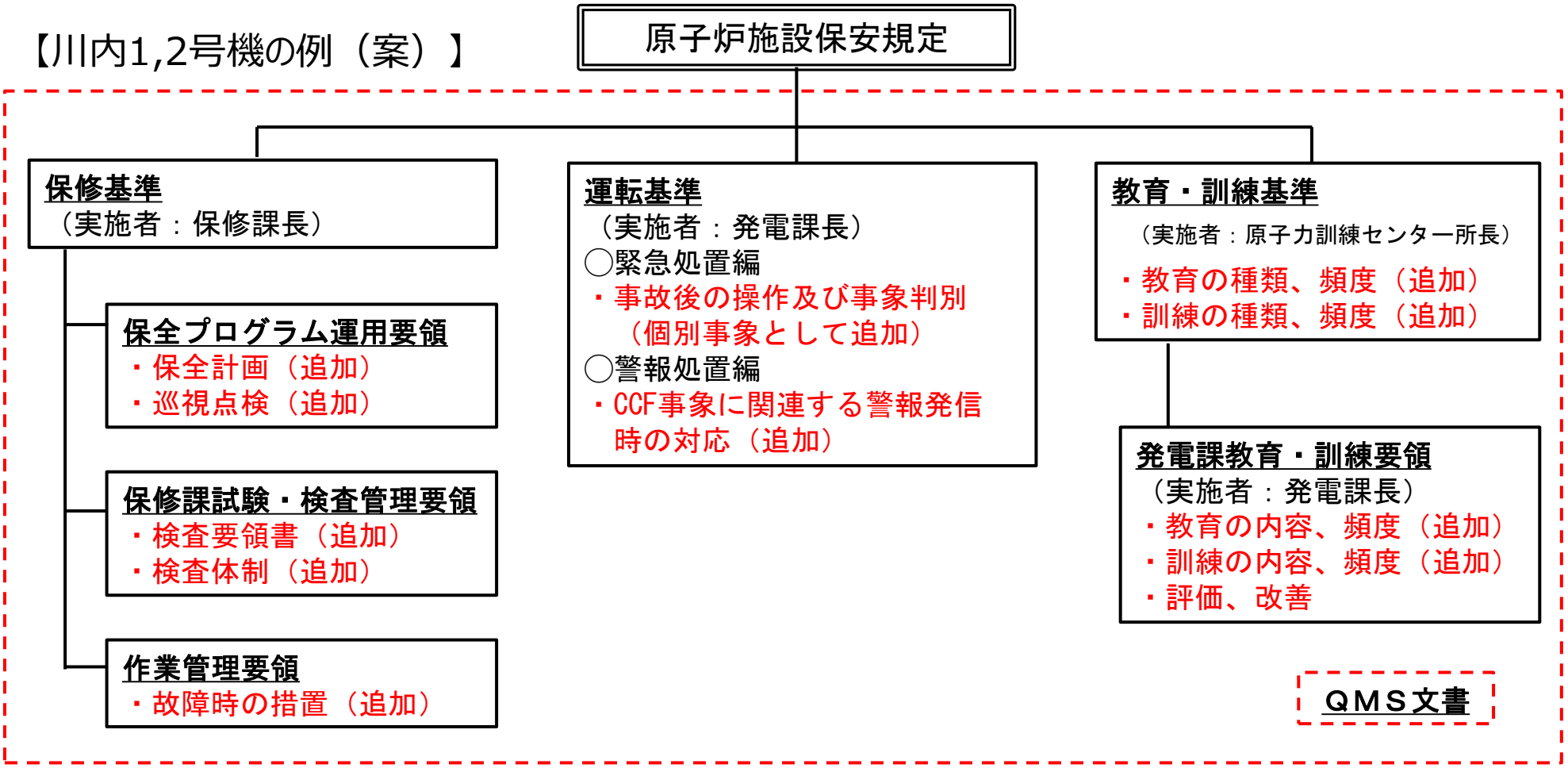
（４）デジタルCCF対策に係る管理体制

◯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。

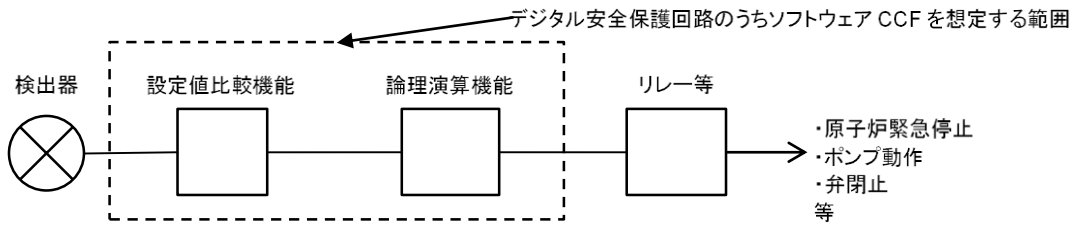
9．自律的対応に係る事業者の管理体制等（2/2）

保全計画、手順書の整備および教育・訓練、故障時の措置ならびに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（案）】



（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。

川内原子力発電所１号機及び２号機
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
に関する要件整合報告書の提出について

別冊資料参照

本要件整合報告書は、2023年1月31日にATENAが事業者から受領したものであり、現在、ATENAが行っている要件整合確認の内容によっては、ATENAの改定指示により内容が変わる可能性がある。

（添付３）悪影響防止について（1/4）

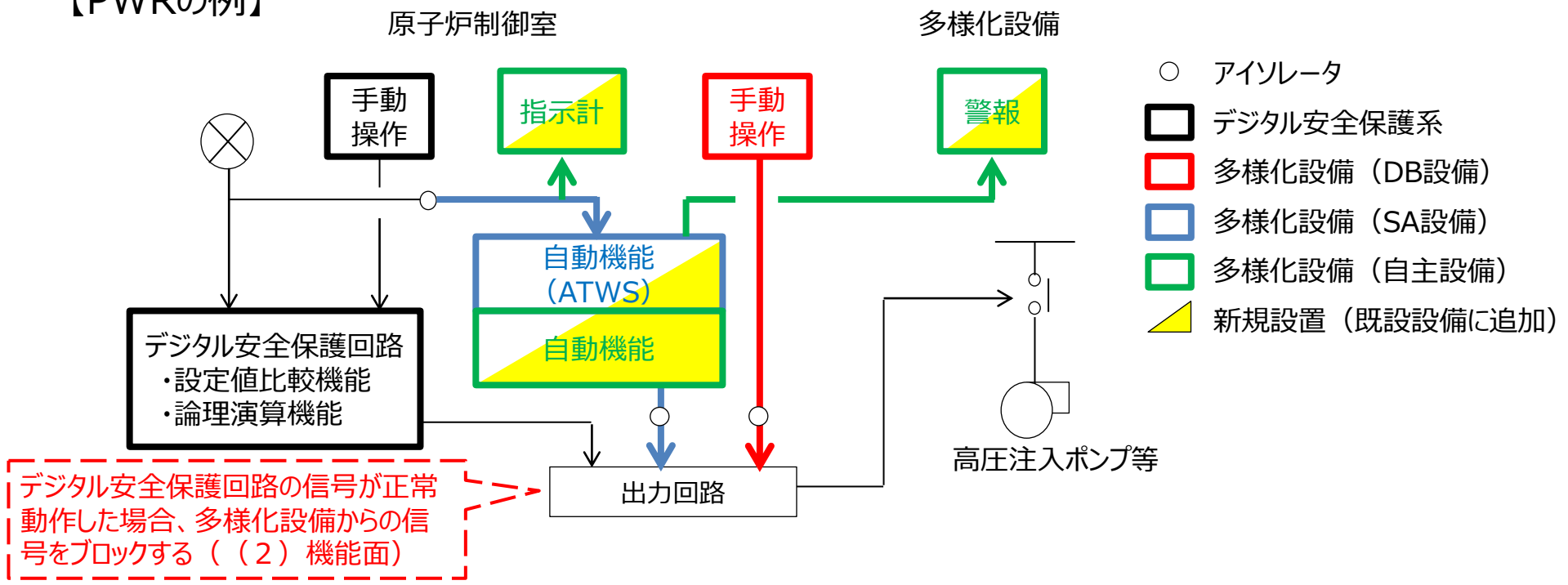
（１）設備面

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。

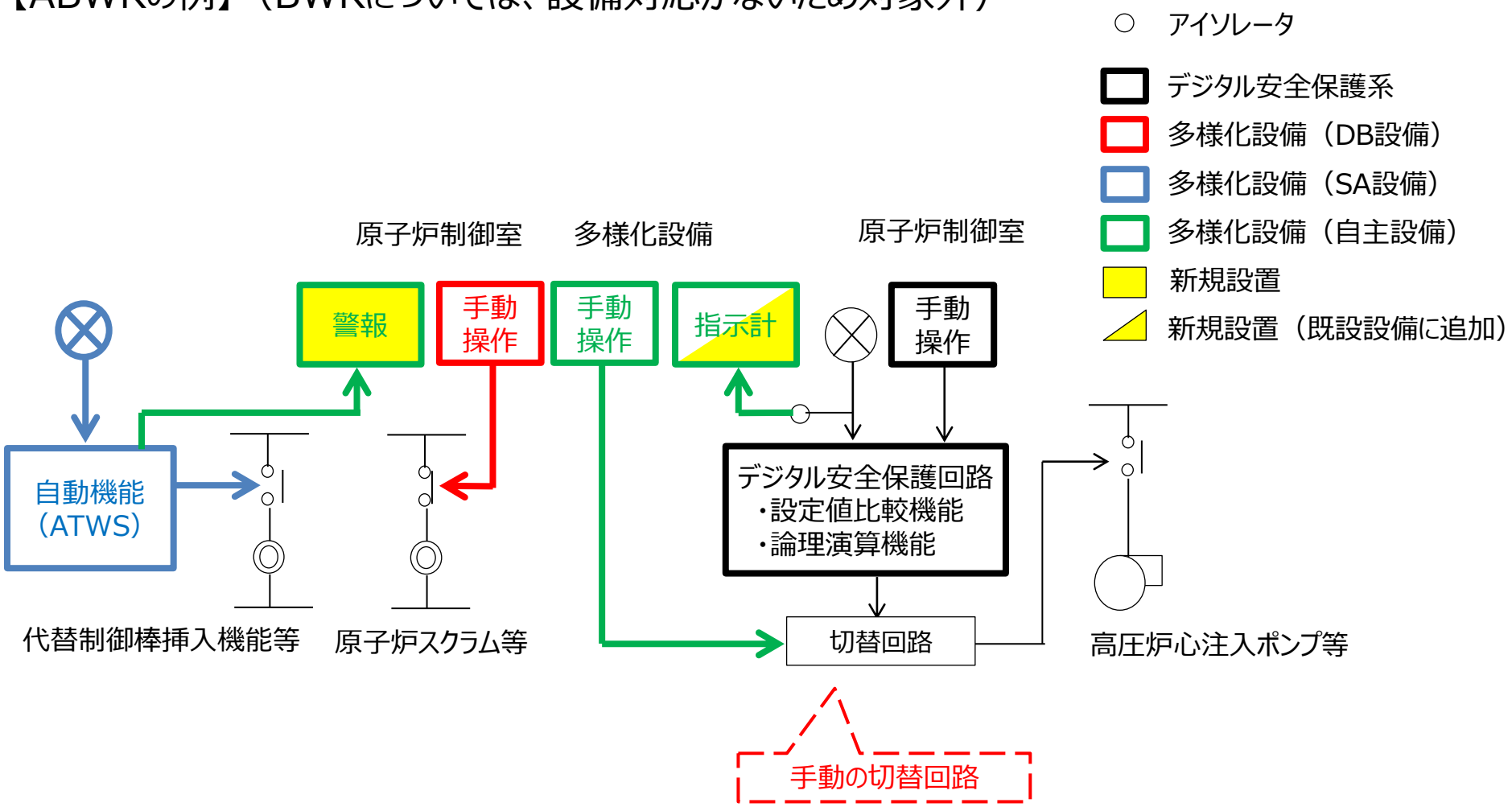
【PWRの例】



（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の場合】

○ 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する設計としている。（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。

○ デジタル安全保護回路の信号と多様化設備の自動作動信号および手動操作信号との出力回路におけるインターフェイスについては、デジタル安全保護回路への悪影響がないよう考慮された回路設計としている。

【ABWRの場合】（BWRについては、設備対応がないため対象外）

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

○ 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。

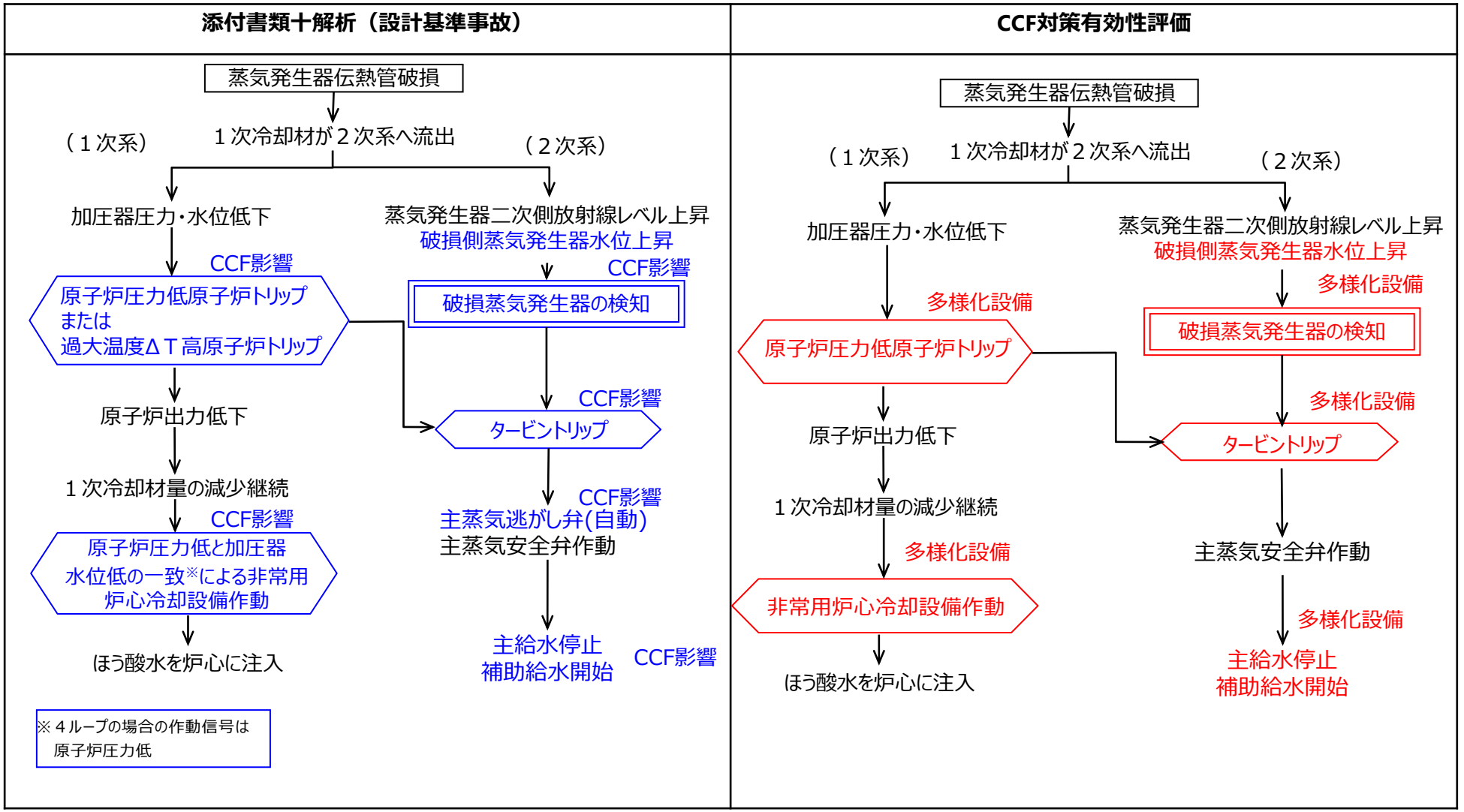
また、技術要件書の要求内容を満足していることを事業者自主検査で確認する。

【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。

（添付4）有効性評価で想定している運転操作等（例）（1/2）

○蒸気発生器伝熱管破損の事象進展（１）



（添付4）有効性評価で想定している運転操作等（例）（2/2）

○蒸気発生器伝熱管破損の事象進展（２）