

デジタル安全保護系のソフトウェア共通要因故障対策の状況、 原子力規制検査の方針及び今後の対応

令和5年5月17日
原子力規制庁

1. 趣旨

本議題は、発電用原子炉施設におけるデジタル安全保護系のソフトウェア共通要因故障（以下「デジタルCCF」という。）対策の事業者の自律的対応状況及び今後の原子力規制検査の方針について報告するとともに、原子力規制委員会と原子力エネルギー協議会（以下「ATENA」という。）との意見交換の実施について、了承を諮るものである。

2. 経緯

令和2年1月29日の第4回発電用原子炉施設におけるデジタル安全保護系の共通要因故障対策等に関する検討チーム（以下「検討チーム」という。）において、ATENAから、デジタルCCF対策については、ATENAのガバナンスの下で事業者が対策を進めていくことが表明され、同年3月23日の第73回原子力規制委員会において、検討チームの検討結果を踏まえ、デジタルCCF対策として満足すべき水準（以下「対策水準」という。）が了承された。

同年10月6日の第5回検討チームでは、ATENAから対策水準の実現を自律的に進めていくための産業界の基本方針として、ATENAが対策水準に係る技術要件書¹を策定し、事業者に対応の実施を求めること、その際、事業者を実施計画書、有効性評価書、技術要件に整合していることの報告の提出及び進捗状況の報告を求めること、提出された文書及びATENAによる確認結果並びに対策の進捗と完了実績について、ATENAがホームページで公開することが示され、また、各事業者の対策実施予定時期についても示された。

これを受け、同年10月21日の第33回原子力規制委員会において、各事業者の対策について、原子力規制庁は、ATENAから半期に1度書面で報告を受けること、日常検査の中で事業者の取組について監視することとされた。

今般、九州電力株式会社川内原子力発電所1号機（以下「川内原子力発電所1号機」という。）において、デジタルCCFの対策工事に着手することとなったことから、ATENAから、川内原子力発電所1号機を例として、工事に係る事業者の自律的対応について説明したい旨、申し出があった。このため、本年2

¹ ATENA 20-ME05 (Rev.0) 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

月17日の第6回及び3月20日の第7回検討チームにおいて、ATENAから説明を受けた（参考1～3参照）。概要を以下に示す（事業者意見聴取の結果については、別紙参照）。

3. 事業者の自律的対応の状況

以下のとおり、ATENA及び事業者が実施する活動の内容を把握することができた。

(1) 技術要件に整合していることの報告の確認

当初、ATENAは、事業者に対し技術要件書²との整合について報告書の提出を求めるとしていたが、技術要件のうち追加設備の運用に関するものは対象外との説明があった。意見交換の結果、ATENA及び事業者が実施する活動から得られた改善事項を今後の活動に取り込む観点から、ATENAは、追加設備の運用についても事業者に報告を求め、その確認を行う旨、説明があった。

(2) 自主検査への立ち会い確認

当初、ATENAは、事業者が追加設備の自主検査を使用前事業者検査と同等の内容及び体制で実施したか報告を受けるが立ち会いはしないとしていたが、意見交換の結果、ATENAは、デジタル安全保護系への波及的影響の防止の観点から各事業者の自主検査に立ち会う旨、説明があった。

(3) 追加設備の運用管理に関する規定の整備の確認

当初、ATENAは、事業者が保全計画や手順書を保安規定に基づく文書として管理するとしたことについて、ATENAとしての関与には言及しなかった。意見交換の結果、ATENAは、事業者が保安規定に基づく文書及び体制で管理するよう規定されているかを確認する旨、説明があった。

(4) 事業者の実施時期とATENAの確認時期との前後関係

当初、ATENAは、上記(1)～(3)のホールドポイントについては言及しなかった。意見交換の結果、ATENAは、事業者が実施する追加設備及び有効性評価に関する技術要件に整合していることの報告の確認を追加設備の工事の開始までに、運用に関する技術要件に整合していることの報告の確認及び工事・検査完了確認を運用開始までに実施する旨、説明があった。

(5) 自律的取組の改善

当初、ATENAは、ATENA及び事業者が実施する活動から得られた改善事項を今後の活動に取り込む活動について言及しなかった。意見交換の結果、ATENA及び事業者が実施する活動から得られた改善事項は定期的に抽出し、今後の活動に取り込む活動を行う旨、説明があった。

² デジタルCCF対策のための追加設備、有効性評価、及び運用に関する要件から構成される

4. 原子力規制検査の方針

デジタルCCF対策に係る追加設備を対象とする原子力規制検査は、事業者の保安活動の監視の一環として以下のとおり実施する。

- (1) 日常検査において、事業者が行う自主検査等の不適合、追加設備の不具合・トラブル等について、コンディション・レポートが、適切に報告、処置されているか品質マネジメントシステムの観点から監視することを基本とする。
- (2) 必要に応じて、事業者が行う設計管理、運用管理（手順書の整備、教育訓練等）、自主検査（据付確認検査、特性検査、機能及び性能に係る検査等）等についても日常検査を行う。

なお、川内原子力発電所1号機について、追加設備に関する原子力規制検査を実施したところ、現時点において指摘事項は確認されていない。

5. 原子力規制委員会とATENAとの意見交換（原子力規制委員会了承事項）

上記3. で述べたように、ATENA及び事業者が実施する活動の内容を把握することができたものの、ATENAとのやりとりにおいて、当方から指摘を行わないとATENAによる活動の改善が十分に見られなかった。また、ATENAは、川内原子力発電所1号機における対策工事の着工時期を直前まで把握しておらず、また、東京電力HD株式会社柏崎刈羽原子力発電所7号機についても既に着工されていたことを把握していなかった。

これらのことから、ATENAの組織的な取組や事業者との連携については、引き続き確認が必要な状況と考える。このため、改めて、事業者の自律的対応に対するATENAの関与についてのトップマネジメントの姿勢や考え方について、原子力規制委員会とATENAとの意見交換会において確認していただきたい。

別紙	事業者意見聴取の結果
参考1	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（第6回検討チーム 資料6-1）
参考2	川内原子力発電所1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対策に係る工事への対応について（第7回検討チーム 資料7-1）
参考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（第7回検討チーム 資料7-2-1）

事業者意見聴取の結果

1. 第6回検討チーム

1-1. 事業者等からの説明の概要（参考1）

（1）基本方針及び事業者の要件整合報告

ATENAは、既設の多様化設備に追加したデジタルCCF対策に係る追加設備に係る有効性評価手法や設備設計要求を具体的に記載した技術要件書を発刊しており、事業者の対策工事の実施にあたっては、実施計画書の提出、有効性評価書の公開、技術要件に整合していることの報告（以下「要件整合報告」という。）の提出及び進捗状況の報告を求めている。また、ATENAは、提出を受けた実施計画、要件整合報告確認の結果及び事業者の対策完了実績を半年ごとに公表し、原子力規制委員会に報告する。

技術要件書には、対策水準を達成するための具体的な要求として、主要な設備要求、有効性評価手法、手順書の整備及び教育訓練の実施が規定されている。

事業者は、技術要件書が定める多様化設備及び有効性評価要求に対する設計図書及び有効性評価書の整合性を確認し、確認結果を要件整合報告に取りまとめ、エビデンスとともにATENAに提出する。その際、事業者内において原子炉設置変更許可申請書及び設計及び工事の計画認可申請書と同等のプロセスにて取りまとめ、品質保証を行う。

（2）ATENAの要件整合確認

ATENAは、事業者から提出された要件整合報告及びエビデンスについて、技術要件への対応や有効性評価結果が具体的に記載されているかを確認し、必要に応じ事業者へ改訂指示を行う。要件整合判定が「○」になっていることを確認後、その結果を要件整合確認書として取りまとめる。併せて、要件整合報告が原子炉設置変更許可申請書及び設計及び工事の計画認可申請書と同等のプロセスにて作成されていることを確認する。また、要件整合報告及びその確認結果について、半年ごとの進捗状況公開に合わせて公開するとともに原子力規制委員会へ報告する。

（3）要件整合確認以降の対応方針

要件整合確認以降の工事・検査の段階においては、設計管理及び検査実施の方法は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し、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。また、設備の保全計画、手順書の整備、教育・訓練及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。

（4）事業者自主検査

事業者は、使用前事業者検査と同等の内容及び体制にて、以下を対象に事業者自主検査として特性検査、機能及び性能に係る検査及び手順書の整備後の運用に係る検査を実施する。

- ・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であって、過去の使用前検査、使用前事業者検査の実績を踏まえ、検査対象と選定した箇所
- ・手順書の整備と教育及び訓練の実施

また、事業者自主検査にあたっては、使用前事業者検査と同等の検査担当者の独立性を確保する。

(5) 自律的対応に係る事業者の管理体制等

事業者は、多様化設備の保全計画、手順書の整備、教育・訓練、故障時の措置及び管理体制について、保安規定に基づく規定文書として保修基準、運転基準及び教育・訓練基準を定め、管理する。

1-2. 主な質疑応答

(1) 技術要件書及び要件整合報告

NRA：ATENAが技術要件書を策定するにあたり、どのようなプロセスを執ったのか。また、外部有識者への意見聴取は行っているか。（遠山技術基盤課長）

ATENA：ATENAのWGにおける他部門の部長によるレビュー、ATENAの役員による確認の後、各事業者の本部長が出席するATENAのステアリング会議での承認を受けて策定しているが、ATENA、事業者及びメーカー以外の、第三者による確認は受けていない。（谷川部長 ATENA 技術班）

NRA：事業者から提出された要件整合報告について、ATENAで整合確認をしたということだが、具体的にはどの程度の詳細さで、確認したのか。（遠山技術基盤課長）

ATENA：設計図書にどのように記載されているかを確認している。（谷川部長 ATENA 技術班）

NRA：技術要件書の波及的影響の防止の要求に、追加設備が既設の安全保護系の機能を阻害しないこととあるが、この点はどのように確認したのか。例えば、追加設備側から既設のデジタル安全保護系に対して、自動ブロック信号を出さない設計としているかを確認したのか。（遠山技術基盤課長）

ATENA：波及的影響の防止という意味では、具体的にどのような手段でそれが達成されているかがポイントになると認識している。現状の要件整合報告での記載、説明及び設計図書でそれが確認できているかを今後、確認していくこととなる。（谷川部長 ATENA 技術班）

NRA：デジタル安全保護系が機能喪失した時の判断について、デジタルCCFがどんな形で発生するのかというのはいろいろなケースがあり得ると思うが、どう認識しているのか。（杉山原子力規制委員）

ATENA：明確な事象として把握できていないのが正直な認識。国内に限らず、

明確にするのは難しいと考えている。今回の対策としては、異常が起きたときにハードウェアで検知し、対処するように設備対応している。
(遠藤 ATENA デジタルCCF-WG委員)

NRA:技術要件に誤操作防止として手順書の整備、教育訓練の実施とあるが、要件整合確認の対象範囲に含まれていない。ATENAとしては確認する必要はないと判断したのか。(今瀬原子力規制専門職 技術基盤課)

ATENA:手順書の整備と教育訓練の実施については、ATENAの技術要件書に要求や注意事項を記載している。その要求の達成については、事業者自身が確認をするものと考えている。(谷川部長 ATENA 技術班)

NRA:PDCAは、手順書の整備や教育訓練を通して出てくるものもある。技術要件書に反映できるものが拾えなくなることを危惧しており、そのようなことのないよう、仕組みをつくってもらいたい。(森下審議官)

ATENA:ATENAも含めた産業界としてPDCAに抜けがないように、ATENAで一度検討したい。(谷川部長 ATENA 技術班)

NRA:要件整合報告の品質保証について、事業者はATENAへ承認プロセスと合わせて提出するとあるが、これから提出されて確認するということか。
(菊川管理官補佐 実用炉監視部門)

ATENA:元々は承認プロセスについて要求していたが、要件整合報告と合わせて、承認プロセスも提出し直してもらおうことを考えている。(谷川部長 ATENA 技術班)

NRA:川内原子力発電所における対策工事は運用開始の予定時期が迫っているが、これから要件整合報告を確認するというスケジュールとなっている。また、手順書や運用規定についてATENAがどう関わるかは、これから検討するとしている。このような現状をどう考えているのか。(菊川管理官補佐 実用炉監視部門)

ATENA:事業者のスケジュールをきちんと押さえた上で、PDCAを含め管理すべきであった。スケジュール的に厳しい状況ではあるが、事業者のスケジュールどおり対応していきたい。(谷川部長 ATENA 技術班)

(2) 追加設備の工事の実施

NRA:原子力規制検査であれば、実施時期について申請で把握できる。事業者からATENAへスケジュールを提出するルールはないのか。なければ、ルール作りから検討してもらいたい。(森下審議官)

ATENA:半年に一度、各プロセスの時期を報告してもらっている。工事、検査の時期については年度単位で報告を受けていて、今回は時期の把握が不十分になった。今後は年月単位での報告を受けるとともに、スケジュールを変更した際は直ちに報告するよう求めていく。(谷川部長 ATENA 技術班)

(3) ATENAによる事業者の管理

NRA：事業者が自主による対応を進めていく上で、ATENAのデュープロセスがしっかりしていることが重要であり、スケジュールありきで説明されている現状に非常に強い懸念を覚える。発電所側の事情はあるかと思うが、事業者の工事が終わってからATENAの確認内容が公開されていくのでは、デュープロセスがまともに機能しているとはいえない。全体を見直し、改めて説明してもらい必要がある。要件整合確認についてもATENAが確認をしたことが示されることが第一と考える。（大島原子力規制部長）

ATENA：検査や工事に関してATENAがどのように関わっていくかの検討が不足していたことが最大の要因と考えている。そこを十分検討した上で、デュープロセスを事業者とも共有し、機能させていきたい。（谷川部長 ATENA 技術班）

NRA：事業者が工事、検査を完了した際、ATENAが完了確認するとあるが、何を確認するのか、完了確認に係るATENA側の体制や力量をどう整理しているのか。また、ATENAが完了確認しないと事業者は運用できないプロセスになっているのか。（村上課長補佐 検査監督総括課）

ATENA：完了確認については、工事、検査が完了したという報告を受け、それを公開するものと考えていたが、ATENAが何を確認するのか、その確認はどのレベルかを考え直して、このプロセス自体を見直したい。（谷川部長 ATENA 技術班）

NRA：多様化設備の運用にあたって、保安規定に相当するような運用規定について、ATENAは確認したのか。また、故障時の措置については、対応方針を検討するとあるが、運用を開始しようという段階で検討しているのか。（菊川管理官補佐 実用炉監視部門）

ATENA：デジタルCCFという事象自体、非常に特定しづらく、現在事業者と技術的な相談をしており、検討する。（谷川部長 ATENA 技術班）

NRA：事業者が実施する部分については、通常の許認可の流れに沿って、使用前事業者検査と同等に実施されると考えている。一方で、ATENAがどういう位置づけで本件について関わっていくのかというのは、もう少し整理が必要。検討の上、また説明してもらいたい。（大島原子力規制部長）

（4）変更管理

NRA：技術要件書や要件整合報告に変更が生じた場合、また、工事が完了した後の変更があった場合に、自主検査として再検査をするのかの判断やプロセスはどうなるのか。（村上課長補佐 検査監督総括課）

ATENA：ATENAは確認内容について審査する立場ではないが、そのような場合どうするかは検討したい。（谷川部長 ATENA 技術班）

（5）デジタル安全保護回路への波及的影響防止

NRA：デジタル安全保護回路への波及的影響防止は、確実に実施されている

ことが一番大事と考えている。アイソレータを設置する場合の健全性や信頼性の確認など、現場等で確認することはあるのか（村上課長補佐 検査監督総括課）

ATENA：必要なものについては事業者自主検査の特性検査やロジック検査において確認したいと考えているが、必要十分か、というのは、検討したい。（谷川部長 ATENA 技術班）

NRA：追加設備が規制要求されている設備に絶対に影響を与えない、というのは、追加設備を規制要求とは切り離して管理できるという担保になる。波及的影響の防止について、ATENAがどう確認するのかをしっかりと検討してもらいたい。（森下審議官）

NRA：追加設備は、定格熱出力一定運転のときに機能させるとあるが、故障した場合でも、原子炉の運転は継続するのか。（菊川管理官補佐 実用炉監視部門）

ATENA：現時点では運転を継続するという方向で検討している。（谷川部長 ATENA 技術班）

（6）ATENAにおける要員の力量と独立性

NRA：事業者自主検査は、使用前事業者検査と同等の考え方で実施をするとして、独立した検査員が検査を実施する体制を組むのだと思うが、ATENAの要件整合確認等についても、力量や独立性を担保するのか。波及的影響の防止は、これまでの使用前事業者検査においても基本設計方針の検査として実施されており、使用前事業者検査と同等に実施するのであれば、外す理由はないと考えている。（上田企画調査官 専門検査部門）

ATENA：ATENAでの整合確認でも、チームを組んで確認しており、力量では問題無いと考えている。一方で、ATENAの組織設計上、第三者性が担保できていない状況である。（谷川部長 ATENA 技術班）

NRA：第三者性にもグレードはあると思うが、直接設計に携わったものが担当するようなことがないのは最低限かと思うので、配慮してもらいたい。（上田企画調査官 専門検査部門）

NRA：デジタルCCF対策に限らず、自主による対応を進めていく上で、第三者性について、ATENAの考え方を整理しておくべきと思う。（森下審議官）

ATENA：追加設備に対して、ATENAがどういった立ち位置で事業者の取組を確認するのか、検討していかなければいけないと思っている。（酒井 ATENA デジタルCCF-WG委員）

2. 第7回検討チーム

2-1. 事業者からの説明の概要

(1) 川内原子力発電所1号機（参考2）

(a) 工事への対応

- デジタルCCF対策については、従来から自主対策として「多様化自動作動設備」を設置。
- 自動作動機能（高圧／低圧注入系起動）、指示計（格納容器再循環サンプ広域水位 他）及び警報（加圧器圧力異常低（高圧／低圧注入系作動））を新規設置するための工事を実施。
- 2023年3月末から4月上旬にかけてデジタルCCF対策工事に係る自主検査を実施し、4月中旬にはデジタル CCF 対策に係る追加設備の使用を開始する計画。

(b) デジタル安全保護系への波及的影響防止

- 設備面では、多様化設備からデジタル安全保護系への悪影響防止のため、電气的分離と物理的分離を実施。
- 機能面では、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。
- 運転操作面では、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の重畳による事象として、独立した手順書を整備。

(c) 多様化設備の運用開始後の管理体制等

- 多様化設備の保全計画、手順書の整備及び教育・訓練、多様化設備の故障時の措置、管理体制については、保安規定に基づく規定文書の中で管理。

(2) ATENA（参考3）

(a) 事業者に対する追加対応の要求

- ①追加設備の運用に関する要件整合報告の提出
- ②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し、検査記録を提出。
- ③運用開始後の管理体制として、保安規定に基づく規定文書及び保安管理体制で管理し、管理文書を提出。
- ④品質保証体制として、設計管理は設工認対象の工事と同等のプロセスで管理し、管理記録を提出。

(b) 安全保護回路への波及的影響防止への対応

設計上考慮している多様化設備と安全保護回路の電氣的・物理的分離の重要性に鑑み、事業者自主検査にATENA又は第三者機関が現場で同席。

(c) プロセスの管理

- ① 工事開始前までに、事業者が実施する追加設備及び有効性評価に関する要件整合確認を実施する。
- ② 追加設備の運用開始前までに、運用に関する要件整合確認、保安規定に基づく規定文書・保安管理体制による管理体制の確認及び工事・検査完了確認を実施する。

(d) 継続的改善

- 設計段階や設計段階以降の事業者の現場での活動で得られた気づきを、デジタルCCF-WGで定期的に抽出し、改善事項として技術要件書への反映等を実施。

(e) 力量と独立性

要件整合確認や工事・検査完了確認を行う要員は、以下とする。

- 業務経歴を基に力量を確認し、確認要員リストに登録して管理。
- 確認要員リストの中から、当該工事の設備設計等に直接関わっていない者を選定。

2-2. 主な質疑応答

(1) 事業者検査・運用に関するもの

NRA：独立した手順書を整備する、ソフトウェアCCFの重畳によることを判断した上で運転操作を実施とあるが、CCFの原因を判定するのは難しいのではないか。（今瀬原子力規制専門職 技術基盤課）

ATENA：CCFが発生したかを直接的に確認するのではなく、デジタル安全保護系の動作が想定したものになっていたかを確認することで、CCFに相当するような事態に陥っていることを確認するという手順になっている。（内海 ATENA デジタルCCF-WG委員）

NRA：要件書の段階から議論されてきた課題は反映済みと思うが、運転手順に関するところは、今後も検討してほしい。手順書を作成し、訓練等の段階になって課題が出てきたときには、手順書だけでなく設備にフィードバックすることも含めて検討いただくと、PDCA活動としてはよいと思う。（今瀬原子力規制専門職 技術基盤課）

ATENA：運用管理については、PDCAをしっかりと回して、必要な改善等は実施していく。（岡原 ATENA デジタルCCF-WG委員）

NRA：多様化設備が作動した後に、既設設備が正常に復帰した場合の設計はど

うなっているのか。既設も多様化設備も両方とも動いている場合も、お互いに悪影響を及ぼさずに作動するという確認をしているのか。（菊川管理官補佐 実用炉監視部門）

ATENA:デジタル安全保護系は作動可能な部分があれば、作動する。デジタル安全保護系が作動していない時には、多様化設備のほうが動く設計になっている。デジタル安全保護系が作動している時に、多様化設備が停止信号を出すというような機能はそもそも持っていないので、波及的な影響はないと考える。（内海 ATENA デジタルCCF-WG委員）

(2) ATENAの関与に関するもの

NRA: ATENAは工事や使用を中止する権限を有しないが、事業者はホールドポイントを経て、使用を開始するとあるが、例えば、ATENAが検査で指摘をしても、工事や使用を中止する権限はないので事業者が先に進めるということにならないようどのように担保しようとしているのか（森下審議官）

ATENA:例えば、検査においてATENAが指摘をしたら、自主検査としては不合格になるので、不合格の状態で前に進むことはないと考えている。各事業者のCNOのコミット事項であると考えていただきたい。（谷川部長 ATENA 技術班）

NRA: 手順書の中に、立会者から異論があった場合には先に進めないということが、チェック項目として入ると理解したが、ATENAにおいて対応されると思っているのか。（森下審議官）

ATENA: そのように運用したい。（谷川部長 ATENA 技術班）

NRA: 九州電力はしっかりと要件確認をしたことが資料に示されているが、ATENAのほうで、何をコメントしたのかが、第三者には分からない。ATENAが実施していることがブラックボックスになっている。ATENAが何をどのように確認したかを、情報発信し、透明性を確保していくということが大事ではないか。（森下審議官）

ATENA: 公開する方向で検討していきたい。（谷川部長 ATENA 技術班）

NRA: 要件整合報告をATENAにおいて検討したものをざっとみたが、個別の項目に適合しているというチェック結果は書かれているが、ATENAからコメントして、事業者が対応したというような往復のプロセスがあったかどうか、分からない。（杉山委員）

ATENA: ATENAから改定指示を出し、どのような理由で改定を要求したのか、それに対する九州電力の回答、ATENAが最終的に合意したかをコメントシートの形で記録として残している。プロセスが見えるような形で公開するか検討する。（谷川部長 ATENA 技術班）

NRA: 前回の議論の中で、ATENAがどういう立ち位置で本件に関わっていくのかということが、幾つか議論されたと思っている。今回、いろいろ整理をしていただいた結果、ATENAは第三者性は有していない、審査、検査

を行う組織ではないということと思う。ピアレビュー的な立場に立つのか、より何か組織的な対応をするのか、現時点ではそこまでは考えていないものの、なるべく透明性を確保するというところだと思う。川内1号の工事を対応しながらPDCAを回して、ATENAの役割分担を、検討していただいたほうがよいと思う。（大島原子力規制部長）

ATENA:今、まさに川内1号機の工事で、九州電力と調整しながら進めており、しっかりシステムを作り上げて、そういうことが普通に行えるような形に持っていきたい。（谷川部長 ATENA 技術班）

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

1. はじめに	2
2. 基本方針	3
3. 技術要件書の概要	5
4. 事業者の要件整合報告	7
5. ATENAの要件整合確認	11
6. 要件整合確認以降の対応方針について	12
7. 事業者自主検査の対象	13
8. 事業者自主検査の内容	16
9. 自律的対応に係る事業者の管理体制等	23
(添付1) 技術要件書の記載内容	25
(添付2) 要件整合報告書(例)	33
(添付3) 悪影響防止について	34
(添付4) 有効性評価で想定している運転操作等(例)	38

- (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)

4

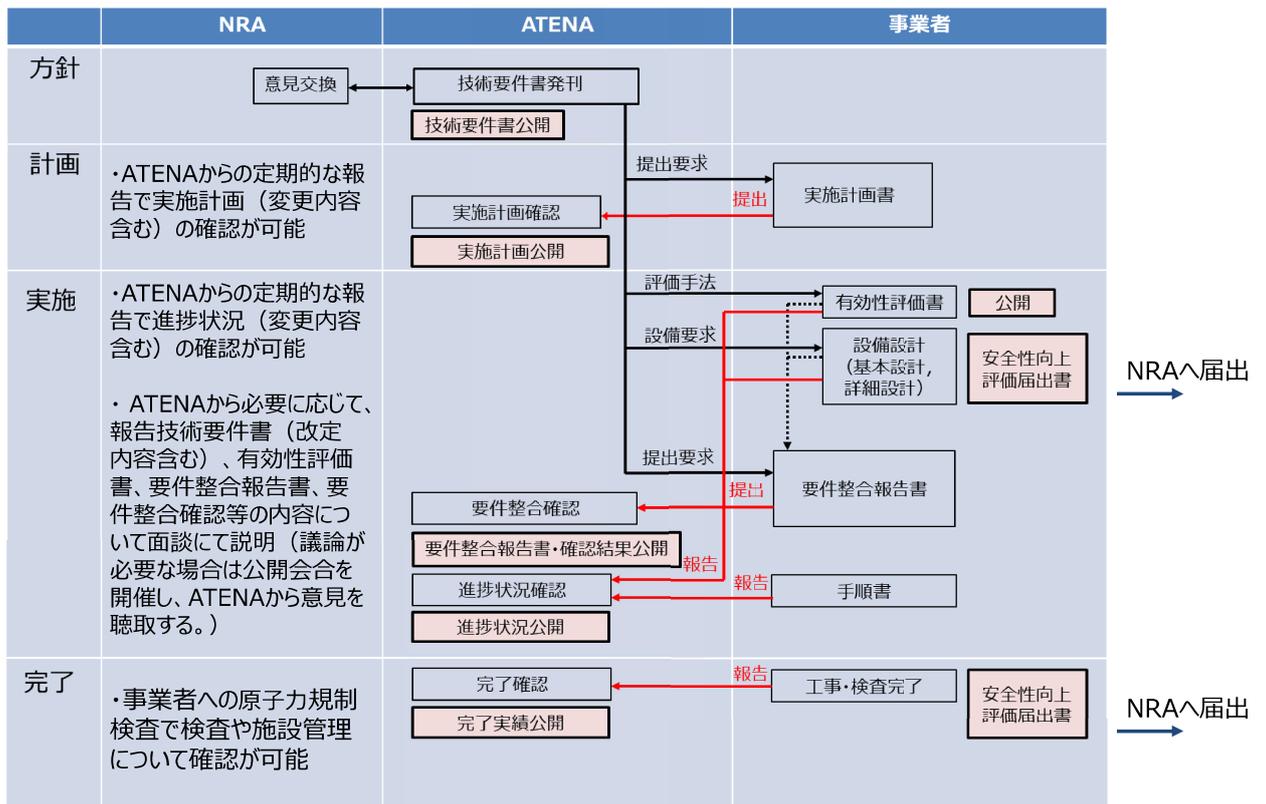


図1 基本方針に基づく対応フロー

3. 技術要件書の概要 (1/2)

5

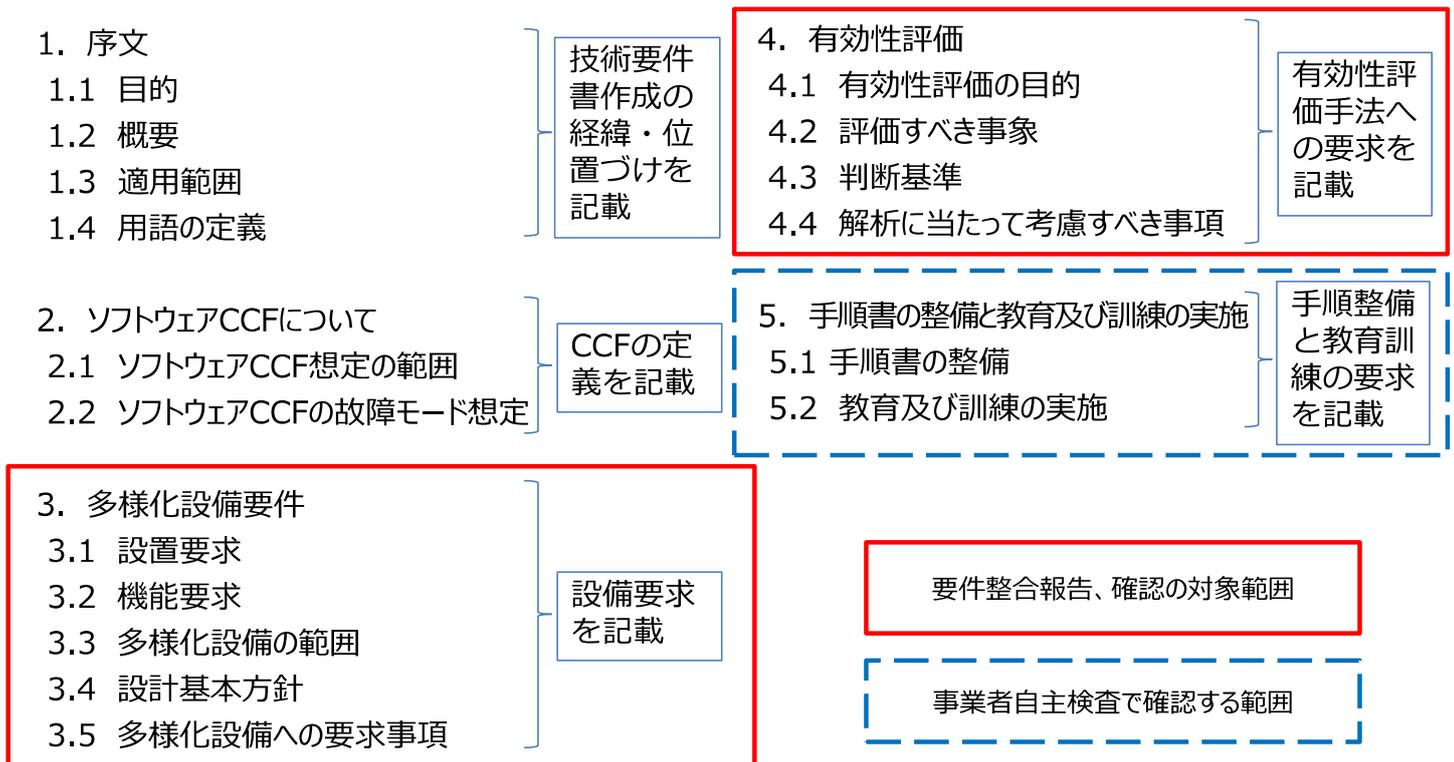
(1) 目的

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) 技術要件書の目次 (各章の要求事項は添付 1 参照)



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。

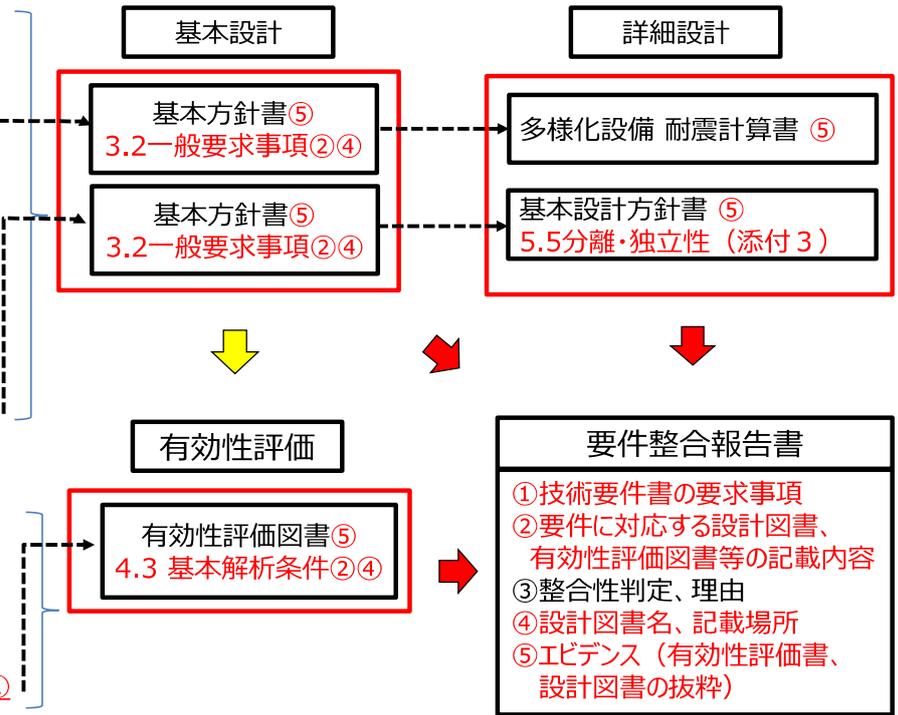
【具体的な例】

- ・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) 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) 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		設計図書
	要求内容	記載内容 (概要)	
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に、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いなければならない。	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、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、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アグラム ・補機インターロック線図

(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。

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
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	・ロジック検査 ・警報機能検査 ・指示性能検査
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	—

(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	—

(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た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)

16

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)

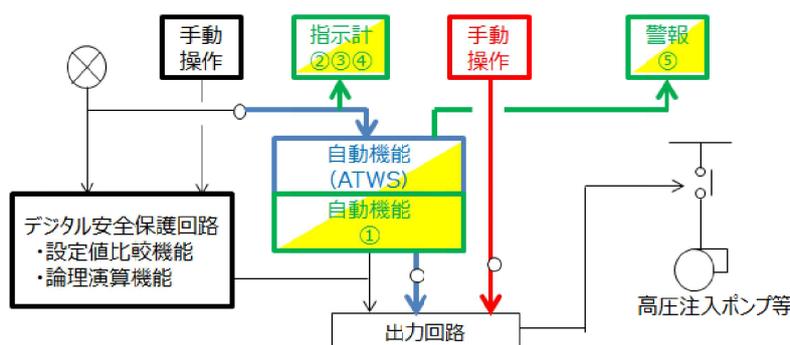
17

(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	<ul style="list-style-type: none"> ・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	<ul style="list-style-type: none"> ・補助給水起動 ・主蒸気隔離 		
	自主設備	<ul style="list-style-type: none"> ・原子炉トリップ ・主給水隔離 	<ul style="list-style-type: none"> ・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 	<ul style="list-style-type: none"> ・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	<ul style="list-style-type: none"> 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)

原子炉制御室

多様化設備



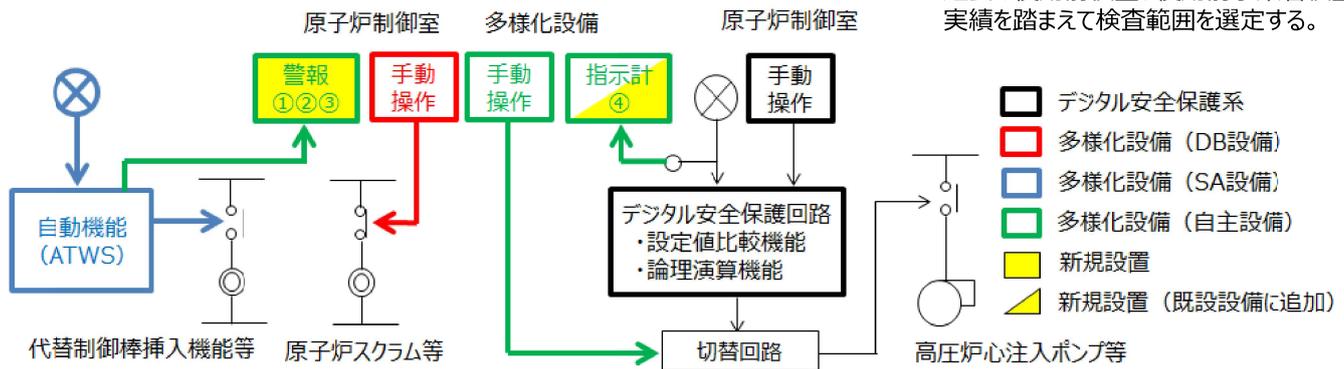
※多様化設備のうち、既設流用箇所については、過去の使用前検査、使用前事業者検査等の実績を踏まえて検査範囲を選定する。

- 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)

(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				
	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。



(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	□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： 保守課

検査担当箇所： 安全品質保証統括室

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再循環サンプル水位	—

⑤ 運用に係る検査

検査項目	確認内容
手順書の整備	<ul style="list-style-type: none"> ○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 <p>【主な確認項目】</p> <ul style="list-style-type: none"> ・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。

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	<ul style="list-style-type: none"> ○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 <p>【主な確認項目】</p> <ul style="list-style-type: none"> ・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

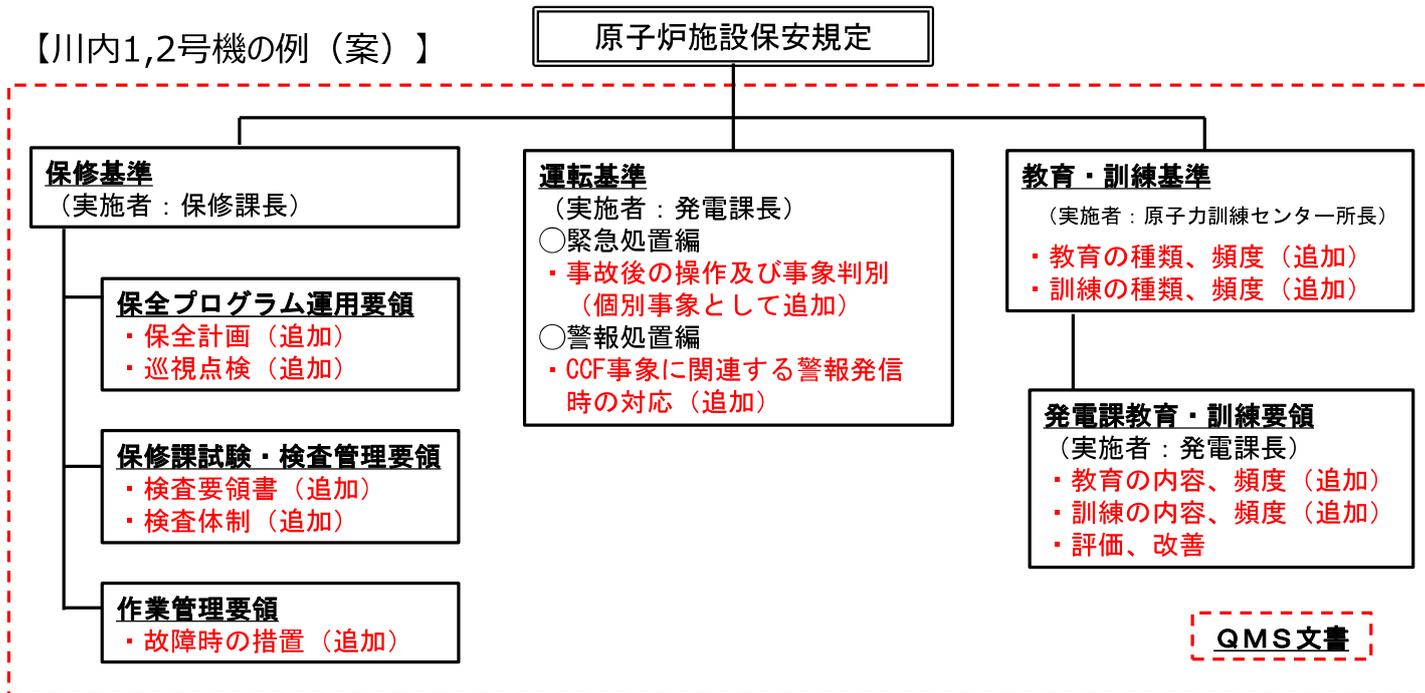
- 保安規定に基づく規定文書の中で管理する。(保修基準)
- 多様化設備が故障等により機能喪失した場合の代替措置等の対応方針を検討する。

(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。

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動作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)

26

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)

27

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ないものを言う。
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。

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。

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。

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	<ul style="list-style-type: none"> ・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	<ul style="list-style-type: none"> ・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。

4.有効性評価 (続き)	概要
4.4.4 常用系機能に対する仮定	<ul style="list-style-type: none"> ・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、事象の過程で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	<p>(1) 機器条件</p> <ul style="list-style-type: none"> ・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。 <p>(2) 操作条件</p> <ul style="list-style-type: none"> ・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	<p>(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。</p> <p>(2) 現実的な計算モデルを使用しても良い。</p> <p>(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。</p>

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システム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、原子炉停止システム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

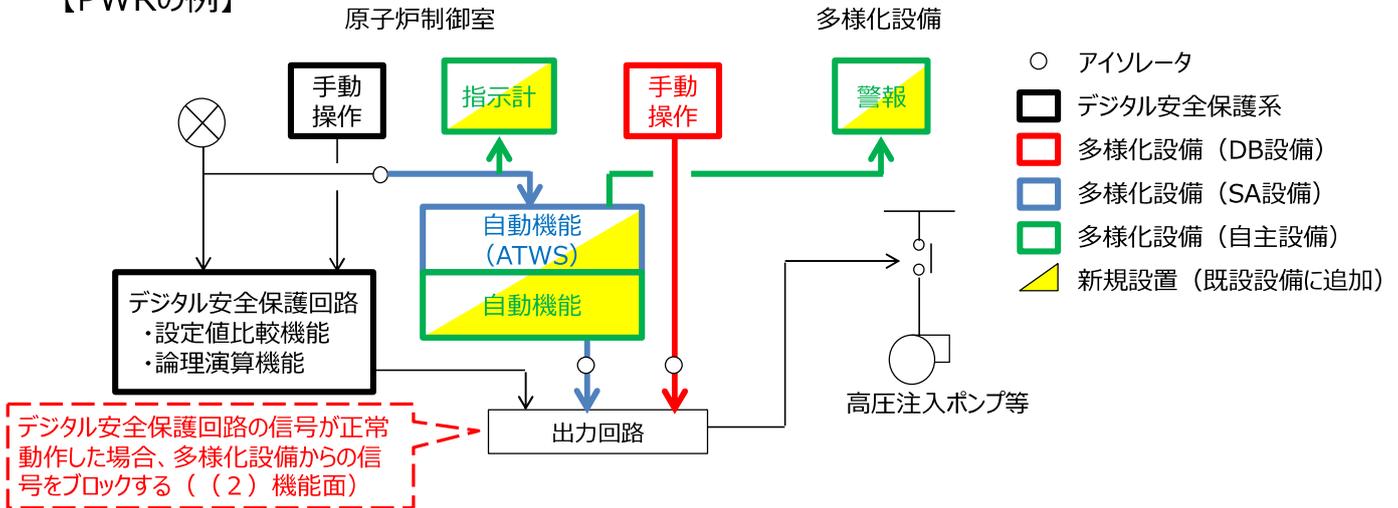
本要件整合報告書は、2023年1月31日にATENAが事業者から受領したものであり、現在、ATENAが行っている要件整合確認の内容によっては、ATENAの改定指示により内容が変わる可能性がある。

(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。

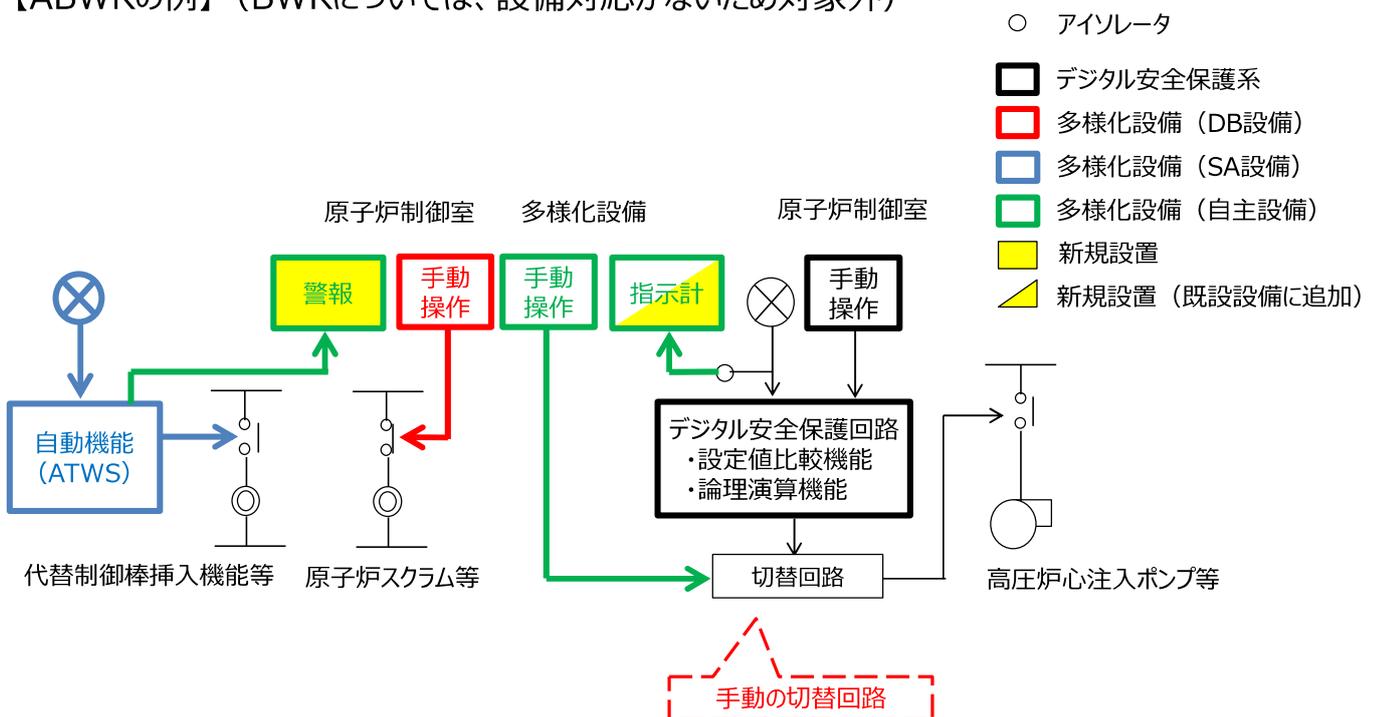
- 電気的分離：多様化設備とデジタル安全保護回路の電気的分離を図る観点から、信号の取り合い部分にはアイソレータ（絶縁回路）を設置している。
- 物理的分離：多様化設備とデジタル安全保護回路の物理的分離を図る観点から、多様化設備は安全系と独立して設置している。

【PWRの例】



(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)



(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。

(3) 運転操作面

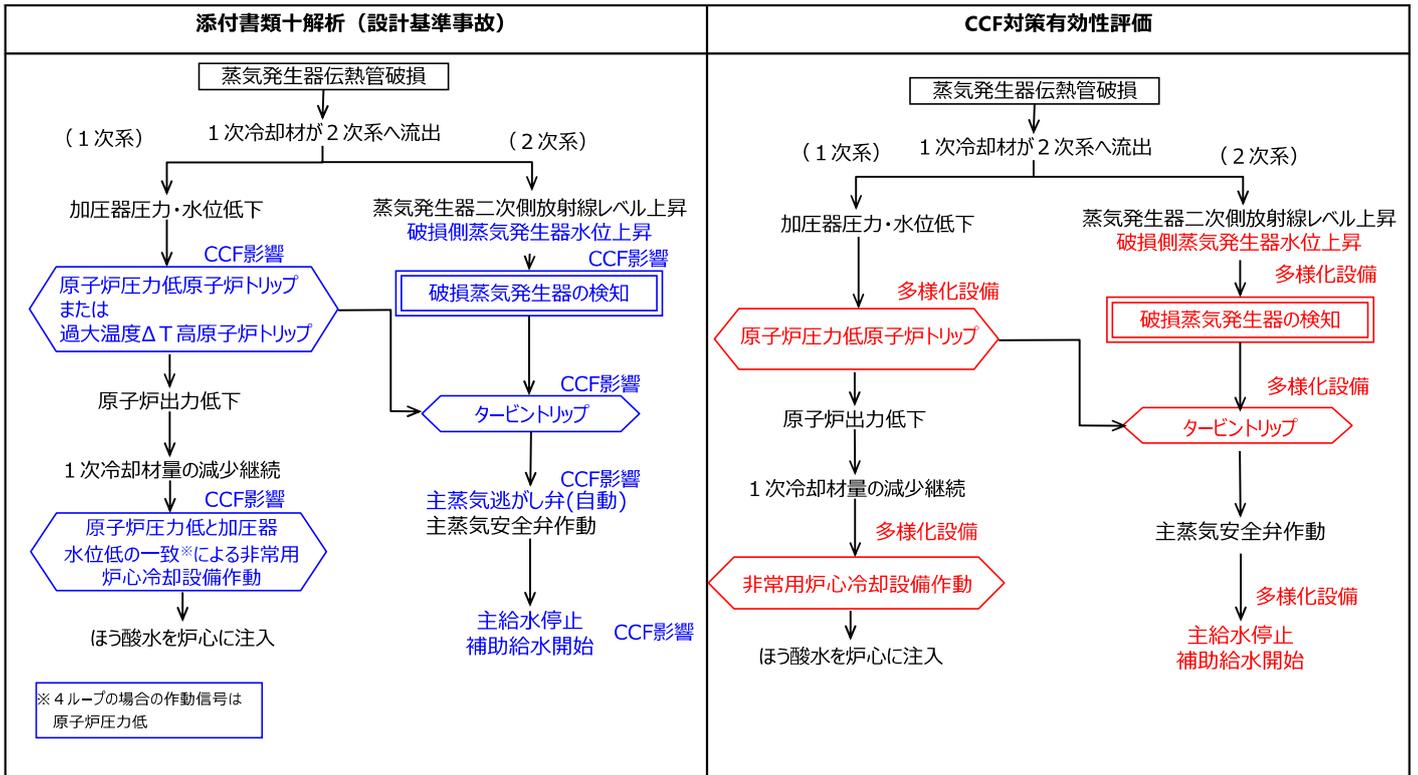
運転時の異常な過渡変化又は設計基準事故とソフトウェアCCFの重畳による事象として、**独立した手順書**を整備することで、確実な事象判別、誤操作防止を図る。

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】

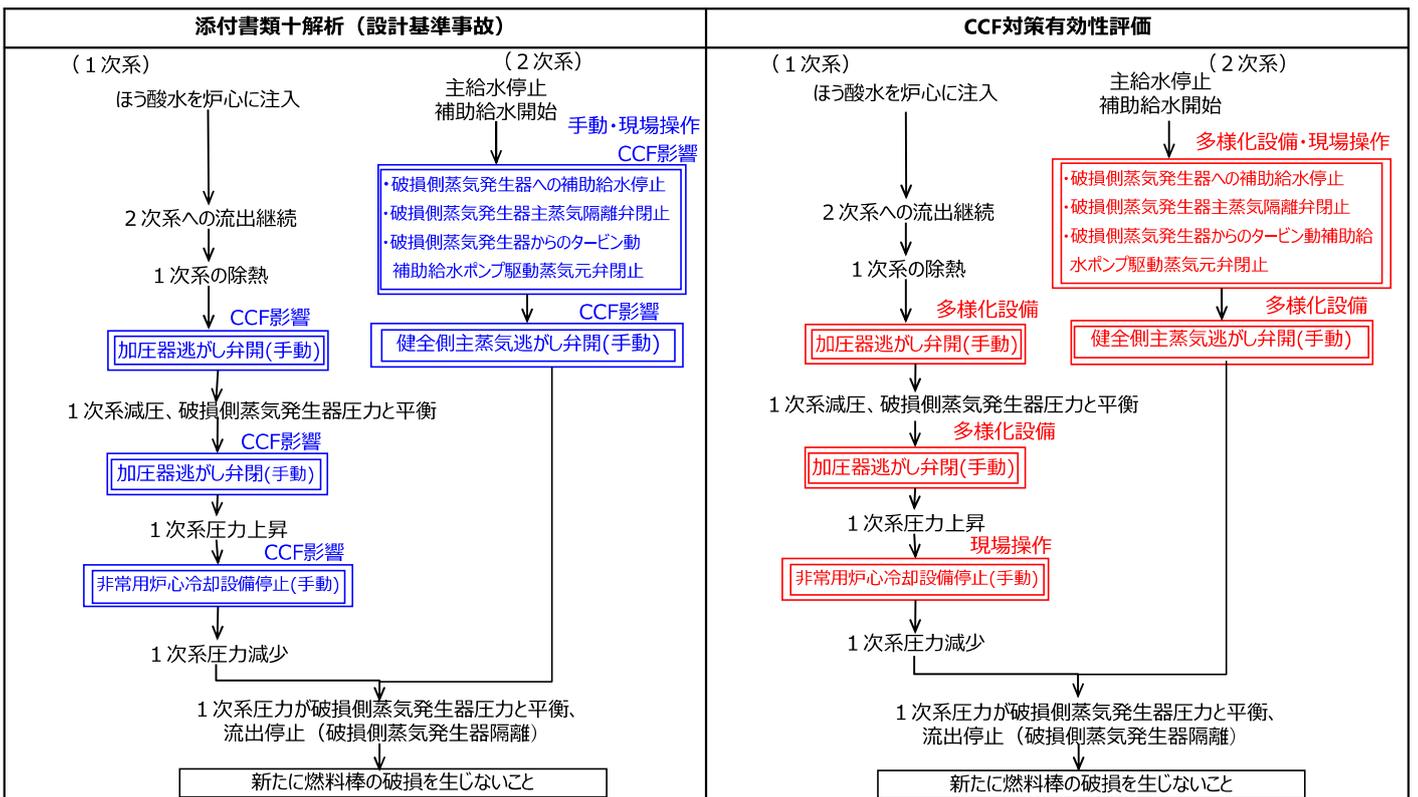
運転時の異常な過渡変化又は設計基準事故が発生した際に、デジタル安全保護回路の安全機能の喪失によって、原子炉停止系統及び工学的安全系施設が自動作動していないことを運転員が認知した場合に、その要因がソフトウェアCCFの重畳によることを判断した上で、必要な運転操作を実施し、判断基準を概ね満足した状態で事象を収束することができるための手順書を整備すること。

○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)



川内原子力発電所1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対策 に係る工事への対応について

九州電力株式会社
2023年3月20日

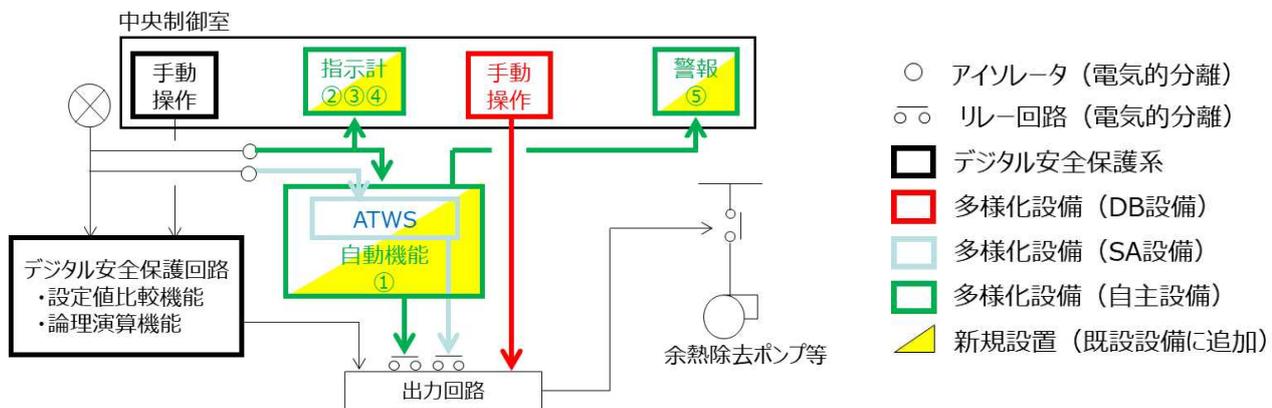
目次

1. はじめに
2. 川内1号機 多様化設備の概要
3. 川内1号機 デジタル安全保護系への波及的影響防止について
4. 川内1号機 自主検査の対象
5. 川内1号機 自主検査の内容
6. 川内1号機 多様化設備の運用開始後の管理体制等

1. はじめに

- 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（以下、デジタルCCF対策）については、従来から自主対策として自主設備の「多様化自動作動設備」を設置して対応してきた。
- 自主設備の「多様化自動作動設備」のうち、ATWS機能については、新規規制基準の重大事故等対処設備（SA設備）として認可を受けている。
- 今回、ATENAの技術要件書の要求事項（CCF事象とLOCA事象の重畳）にも対処できるように、自動作動機能（高圧／低圧注入系起動）、指示計（格納容器再循環サンプル広域水位 他）及び警報（加圧器圧力異常低（高圧／低圧注入系作動））を新規設置するための工事を実施する。
- 2023年1月31日（2023年3月6日一部改訂）に川内1,2号機の要件整合報告書をATENAに提出し、ATENAによる要件整合確認結果（整合性に問題なし）が2023年3月14日に公開された。
- 今後、2023年3月末から4月上旬にかけてデジタルCCF対策工事に係る自主検査を実施し、4月中旬にはデジタルCCF対策設備の使用を開始する計画である。

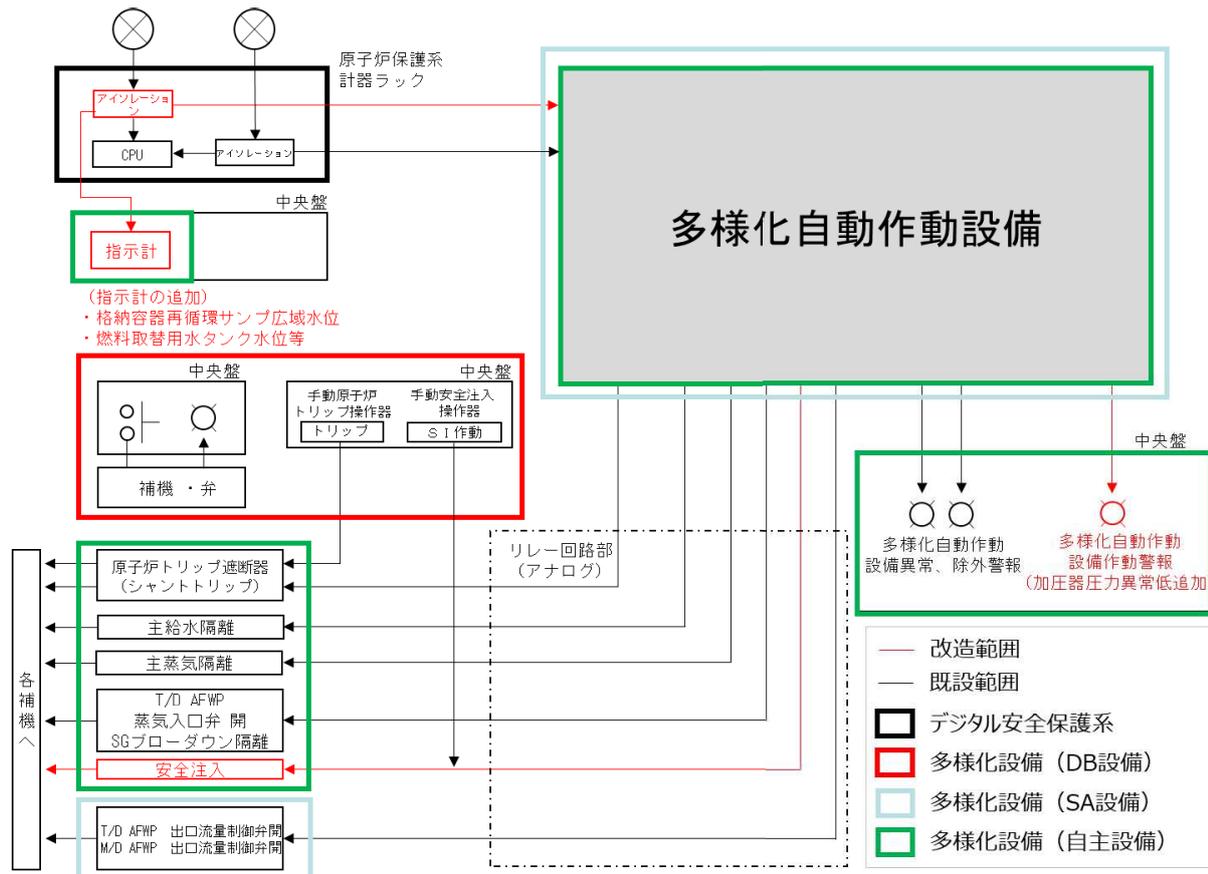
2. 川内1号機 多様化設備の概要 (1/2)



設備区分	自動機能	手動操作	指示計	警報
既設 流用	DB 設備	—	—	—
	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	—	・ 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	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ル広域水位	⑤ 加圧器圧力異常低（高圧／低圧注入系作動）

2. 川内1号機 多様化設備の工事概要 (2/2)

【多様化設備のシステム概略図】



4

3. 川内1号機 デジタル安全保護系への波及的影響防止について (1/2)

(1) 設備面

多様化設備からデジタル安全保護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、多様化設備はデジタル安全保護系と独立して設置している。

(2) 機能面

- 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には、多様化設備による原子炉トリップ、主蒸気隔離、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 補助給水系が正常に作動した場合には、多様化設備による補助給水起動信号を自動的にブロックする。
 - ④ 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。

3. 川内1号機 デジタル安全保護系への波及的影響防止について (2/2)

(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。

なお、設備設計は手順書に求められる内容（監視機能、操作内容）を考慮して行っている。

また、手順書が規定文書として制定されていることを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。

6

4. 川内1号機 自主検査の対象 (1/3)

技術要件書の要求項目に対して、自主検査で確認する主な対象を以下に示す。

(1) 技術要件書「3. 多様化設備要件」の要求項目

技術要件書の要求項目	要件整合報告書で確認	主な自主検査の対象
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 ・指示計性能検査
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	安全保護回路への波及的影響防止	○状態確認検査 ・据付確認検査 ○機能及び性能に係る検査 ・ロジック検査
	耐環境性、耐震性、操作性、監視性 供給電源、設備の共用、試験可能性、 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	—

4. 川内1号機 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	主な自主検査の対象
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	—

8

4. 川内1号機 自主検査の対象 (3/3)

(2) 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	主な自主検査の対象
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た確な対応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。

5. 川内1号機 自主検査の内容 (1/2)

(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 指示計性能検査
状態確認検査	据付確認検査（アイソレーションカード等）
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：本店及び保修課

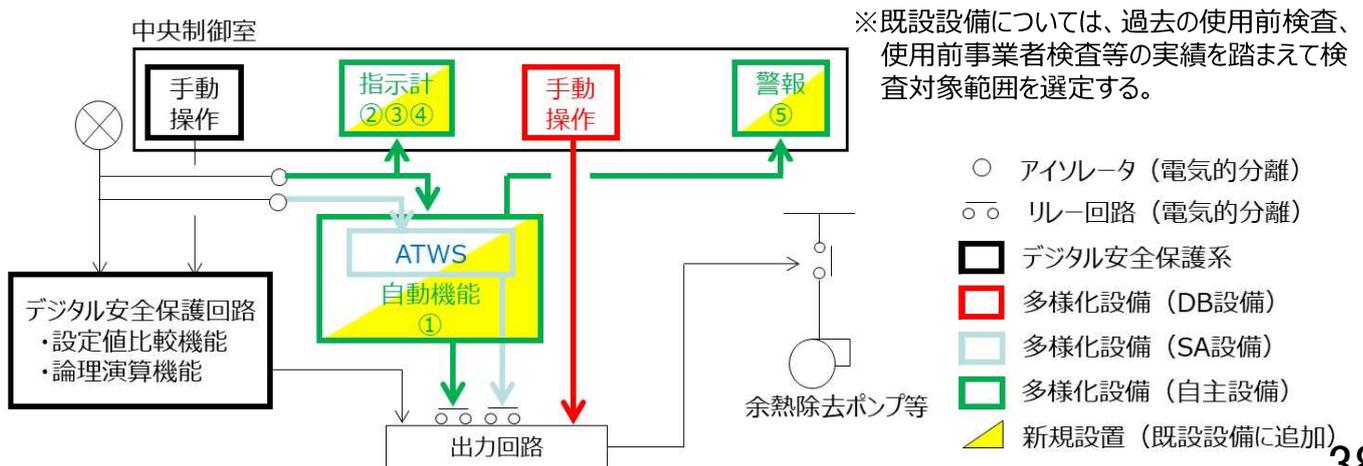
検査担当箇所：安全品質保証統括室

10

5. 川内1号機 自主検査の内容 (2/2)

(3) 検査対象範囲

検査項目	検査方法※
特性検査	新規設置の多様化設備 既設設備の多様化設備（DB設備、SA設備、自主設備）
機能及び性能に係る検査	
状態確認検査	アイソレーションカード等



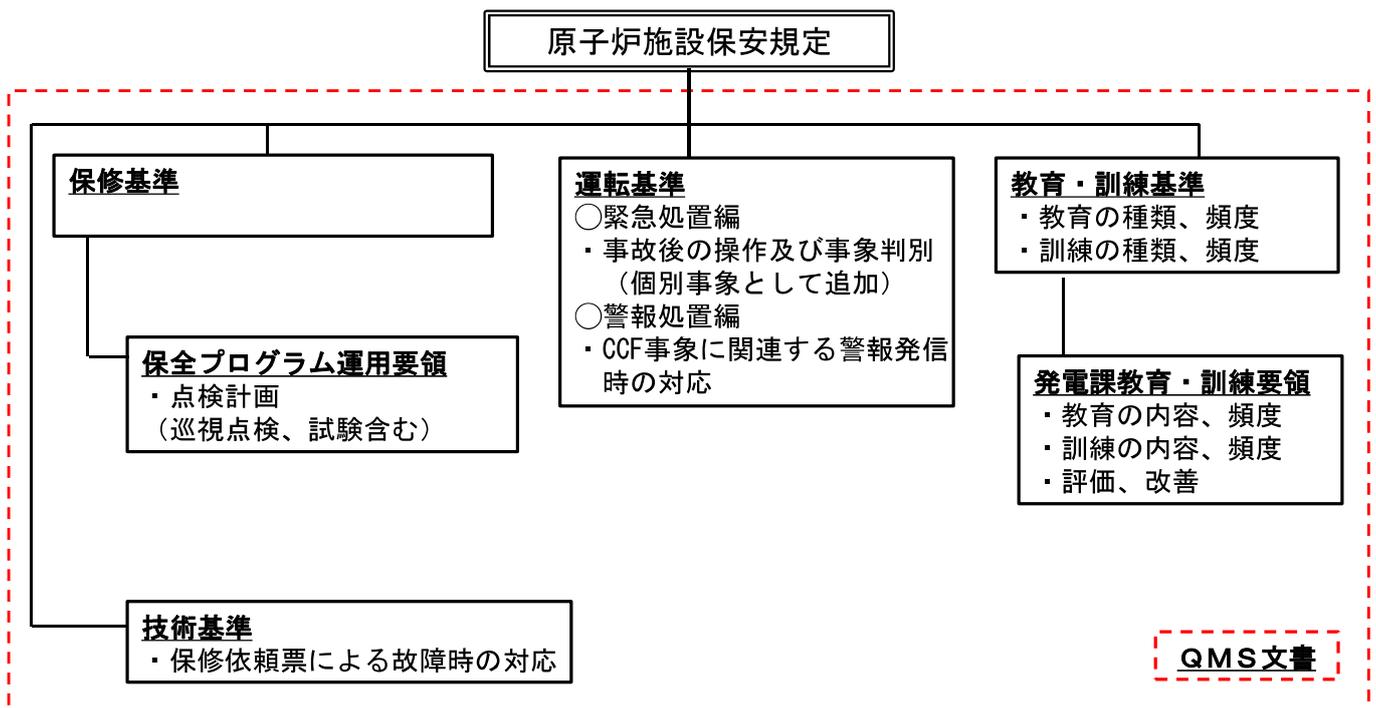
6. 川内1号機 多様化設備の運用開始後の管理体制等 (1/2)

- (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を実施する。(保守基準)
 - ・点検計画(保全重要度、点検頻度、点検方法)
 - ・「重大事故等安全停止回路機能検査」と同等の特性試験、機能・性能試験を実施する。
- (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
- 故障時に速やかに復旧可能とするために必要な予備品を確保する。
 - 多様化設備が故障等により機能喪失した場合の対応については、保安規定に基づく規定文書の中で管理する。(技術基準)
 - ・ 保守依頼票にて対応を行い以下の処置を行う。
 - ・ 多様化設備の故障箇所がSA要求機能と切り分けできない場合は、SA設備の保安規定に従い対応する。
 - ・ 故障時に早期復旧できない場合は、目視点検により本設設備であるデジタル安全保護系の健全性を確認する。
- (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。

12

6. 川内1号機 多様化設備の運用開始後の管理体制等 (2/2)

保全計画、手順書の整備および教育・訓練、故障時の対応ならびに管理体制に係る文書体系を以下に示す。



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 3月20日
原子力エネルギー協議会

目次

1

1. はじめに
2. 要件整合確認結果（詳細設計）の公開について
3. 産業界としての基本方針
4. 要件整合確認（詳細設計）以降の対応方針について
 - （添付1）川内1,2号機 要件整合報告書（詳細設計）
 - （添付2）ATENAによる要件整合確認要領（詳細設計）
 - （添付3）要件整合確認（手順書）の確認内容

- (1) 2020年1月29日の原子力規制委員会（NRA）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NRA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」という。）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状況を公開するとともに、NRAに報告を行っている状況である。
- (3) 現在、事業者は計画通りに対策を進めており、2023年1月に最早プラントの要件整合報告書（詳細設計）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) 2023年2月17日のNRA公開会合では、要件整合確認と事業者の自主検査等に関する産業界の方針について説明した。
- (5) ATENAは、2023年3月14日に川内1,2号機の要件整合確認結果（詳細設計）を公開した。
- (6) 今回の公開会合では、2023年2月17日のNRA公開会合での議論を踏まえ、要件整合確認（詳細設計）以降のATENAの対応方針について説明する。

2. 要件整合確認結果（詳細設計）の公開について

- (1) デジタルCCF対策に係る安全対策のうち基本設計、詳細設計及び有効性評価について、ATENAは、2023年1月末に、川内1,2号機、大飯3,4号機、柏崎刈羽7号機の要件整合報告書（詳細設計）を受領した。
- (2) 最早プラントである川内1,2号機（川内1号機は3月末に工事完了・検査開始予定）の要件整合報告書（詳細設計）（添付1参照）について、ATENAによる要件整合確認（添付2参照）を実施した結果、**技術要件書の各要求事項に対して全て整合していることを確認した。**
- (3) 以上を踏まえて、ATENAは、川内1,2号機の基本設計、詳細設計及び有効性評価について、ATENA技術要件書の各要求事項に基づき適切に実施されていると評価し、ATENAの確認結果及び川内1,2号機の要件整合報告書（詳細設計）を2023年3月14日に公開した。

ATENAと事業者は、デジタルCCF対策を以下の基本方針に基づき自律的かつ計画的に進めている。

- (1) ATENAは、技術要件書を事業者に提示し、デジタルCCF対策の実施を要求する。
- (2) 事業者は、技術要件書に基づき、事業者の責任において以下の対応を行う。
 - ①設備設計及び有効性評価の実施
 - ②工事・検査の実施
- (3) 事業者は、ATENAに対して以下の報告を行い、ATENAは確認結果を公開する。
 - ①要件整合報告書
 - ②工事・検査等完了報告書

4. 要件整合確認（詳細設計）以降の対応方針について（1/7）

- (1) ATENAは、要件整合確認（詳細設計）以降の検査、手順書の整備、運用開始後の管理体制等についても、**ATENAのガバナンスの下で**、事業者に対して追加対応を要求する。
- (2) ATENAは、事業者に要求した追加対応に関して、事業者から提出された記録等の確認を行い、確認結果を公開する。
- (3) 安全保護回路への波及的影響防止については、その重要性に鑑み、事業者自主検査にATENAまたは第3者機関が現場で同席する。
- (4) ATENAは、ホールドポイントを設けて事業者のプロセスを管理する。
- (5) ATENAは、デジタルCCF-WGにおいて、対応全般に関わる改善事項や良好事例を抽出し技術要件書や要領書への反映を行うことにより、CCF対策が自主対策として継続的に実施されるようPDCAを回す。

(1) ATENAが事業者に要求する追加対応

ATENAは、事業者に以下の追加対応を要求する。

- ① 要件整合報告（手順書）
事業者は、技術要件書「5. 手順書の整備と教育及び訓練の実施」の要求事項について、要件整合報告書(手順書)を提出すること。
- ② 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し、検査記録を提出すること。
- ③ 運用開始後の管理体制
事業者は、デジタルCCF対策に係る保全計画、手順書、教育訓練、故障時の措置等について、保安規定に基づく規定文書及び保安管理体制で管理し、管理文書を提出すること。
- ④ 品質保証体制
事業者は、設計管理について、設工認対象の工事と同等のプロセスで管理し、管理記録を提出すること。

(2) ATENAによる確認

ATENAは、(1) で事業者に要求した追加対応について、下記の確認を行う。

- ① 要件整合確認（手順書）
事業者から提出された要件整合報告書(手順書)及びエビデンス(手順書、訓練方針書)について、要件整合確認（詳細設計）と同様の確認を行う。（添付3参照）
- ② 事業者自主検査結果の確認
事業者自主検査の記録により、以下を確認する。
 - ・使用前事業者検査と同等のプロセスで検査項目が抽出されていること。
 - ・使用前事業者検査と同等の検査体制で実施されていること。
 - ・全ての検査が完了し、合格していること。
- ③ 運用開始後の管理体制の確認
保全計画、手順書、教育訓練、故障時の措置等について、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ことが規定されていることを確認する。
- ④ 品質保証体制の確認
設計管理方法について、設工認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。

（3）安全保護回路への波及的影響防止への対応

事業者は、技術要件書「3.5.8安全保護回路への波及的影響防止」の要求事項に対して、設計上考慮している多様化設備と安全保護回路の電氣的・物理的分離を、以下の方法で確認を行う。

- ① 事業者は、事業者自主検査において責任を持って以下の確認を行う。
 - ・安全保護系盤内でアイソレーターが所定の位置に設置されていること。
 - ・多様化設備がデジタル安全保護系と独立した盤に設置されていること。
 - ・多様化設備の自動作動阻止機能が正常に動作すること。（PWRの場合）
- ②安全保護回路への波及的影響防止については、その重要性に鑑み、事業者自主検査にATENAまたは第3者機関が現場で同席する。

（4）ATENAによるプロセス管理

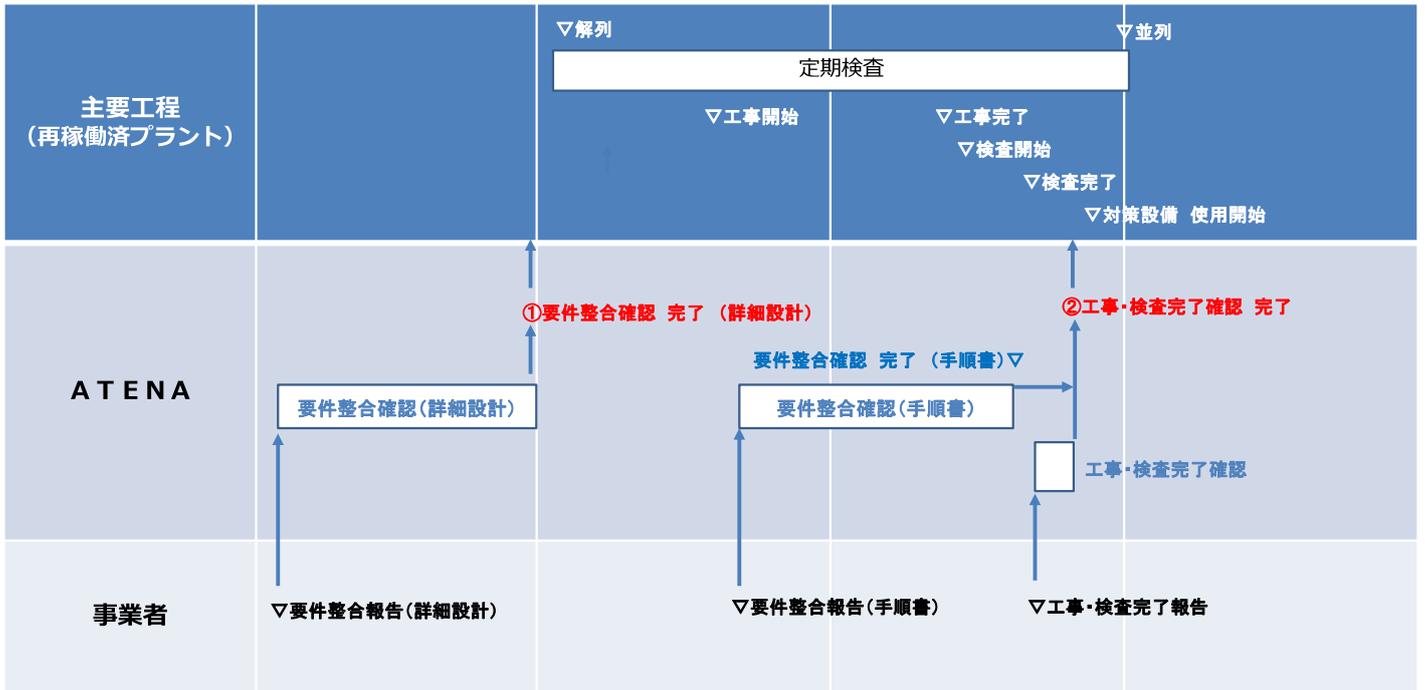
ATENAは、今後、以下のホールドポイントを設けて事業者のプロセスを管理する。

- ① ATENAは、工事開始前までに、要件整合確認(詳細設計)を実施する。
(ATENAは、確認結果を事業者に通知するとともに速やかに公開する。)
- ② ATENAは、対策設備の使用開始前までに、要件整合確認（手順書）及び工事・検査完了確認を実施する。（ATENAは、確認結果を事業者に通知するとともに速やかに公開する。）

ATENAは、事業者に対して年・月ベースの実施計画の提出と計画変更時の速やかな報告を求め管理する。

ATENAは事業者の工事・検査開始や使用開始を中止する権限を有していないが、事業者は上記①及び②のホールドポイントを経て対策設備の使用を開始することとする。

①② : ホールドポイント



4. 要件整合確認 (詳細設計) 以降の対応方針について (6/7)

(5) デジタルCCF対策に係る継続的改善について

ATENAは、設計段階や設計段階以降の事業者の現場での活動で得られた気づきを、デジタルCCF-WGで定期的に抽出し、改善事項として技術要件書への反映等を行う。(定期的な活動としてルール化し、定着を図る。)

① 設計段階

詳細設計・有効性評価における気づき事項については、既にCCF-WGで抽出し技術要件書Rev1(2022.10.05改定発刊)に反映している。

② 設計段階以降

手順書整備・検査・訓練・運用段階における気づき事項についても、定期的にCCF-WGで抽出し、改善事項や良好事例として技術要件書や要件整合確認要領への反映、他プラントへの水平展開を行う。(ATENAは、必要に応じて現場にも出向き、意見交換を行う。)

（6）ATENAの力量と独立性について

ATENAは事業者に対する第三者性を有しておらず、かつ審査・検査を行う組織ではない。

ATENAは、要件整合確認や工事・検査完了確認において、設計図書 of 技術要件書に対する整合性や検査記録などの確認結果を公開することにより、透明性を確保する。

要件整合確認や工事・検査完了確認を行うATENAの要員は、以下とする。

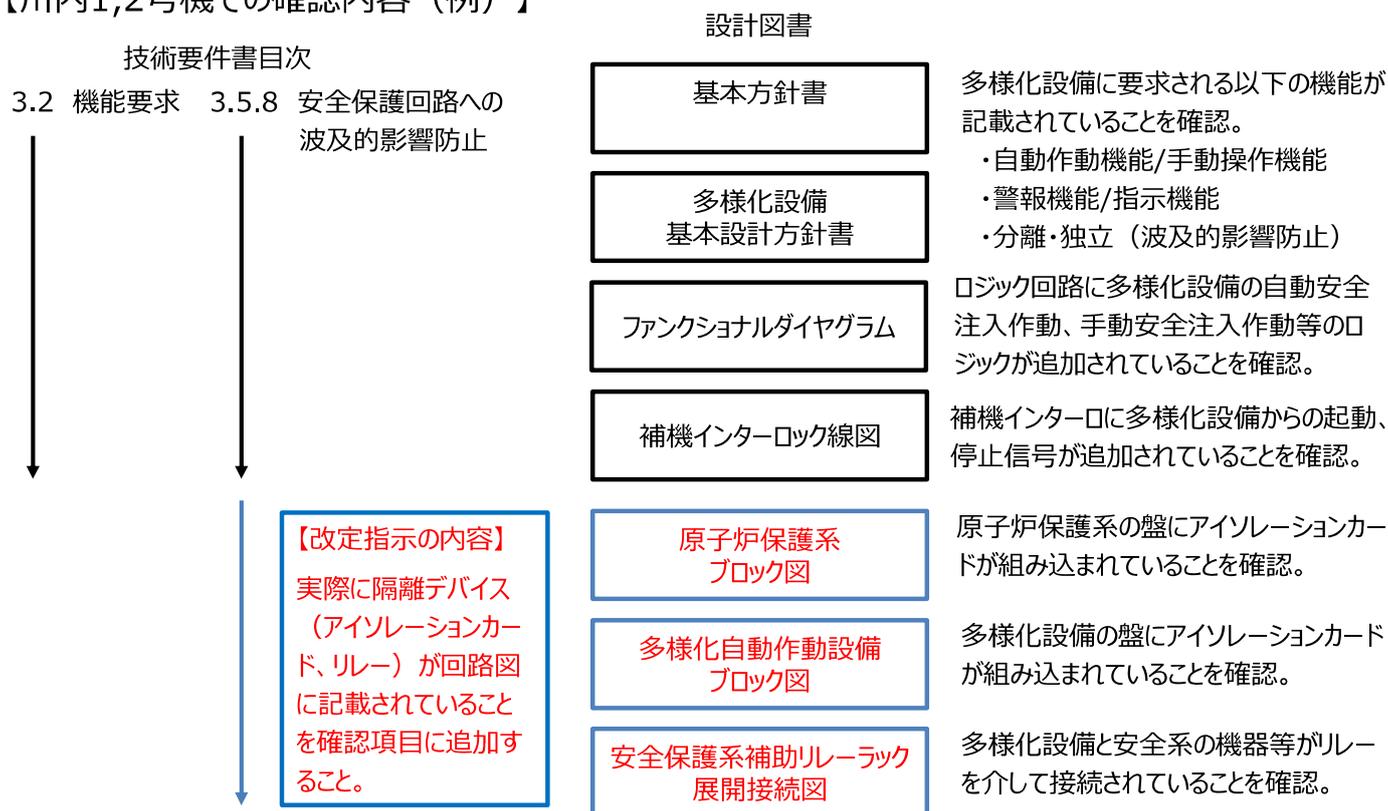
- ・ 業務経歴を基に力量を確認し、確認要員リストに登録して管理する。
- ・ 確認要員リストの中から、当該工事の設備設計等に直接関わっていない者を選定する。
- ・ 確認要員には、必要に応じてデジタルCCF-WGメンバーも含める。

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（詳細設計）

別冊資料参照

- ATENAは、事業者から提出された**要件整合報告書 (詳細設計) 及びエビデンス(有効性評価書、設計図書)**に対して要件整合確認を行う。
- 確認方法は、下記の確認項目によるチェックシート形式とし、**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、要件整合確認書 (詳細設計) 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抽出されていること。
 - 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 多様化設備設計と有効性評価の関連する項目が紐づけられていること。
- ATENAは、ATENAの確認結果及び事業者の要件整合報告書 (詳細設計) を速やかにHPで公開するとともに、NRAに報告する。

【川内1,2号機での確認内容 (例)】



○技術要件書「5.手順書の整備と教育及び訓練の実施」の要求項目に対して、事業者から提出された要件整合報告書(手順書)及びエビデンス(手順書、訓練方針書)の確認を行う。

技術要件書の要求内容	確認内容
<p>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。</p>	<ul style="list-style-type: none">・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が整備されていること。・必要な手順書への移行の方法が明確になっていること。・運転操作を行う場合の判断条件及び操作場所が記載されていること。・プラント状態を監視するための計器及びその設置場所が手順書に記載されていること。
<p>5.2 教育及び訓練の実施 整備された手順書に従いたく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。</p>	<ul style="list-style-type: none">・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、教育及び訓練が計画されていること。