

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
実施状況等の確認要領

改定履歴

| 改定年月 | 版 | 改定内容 | 備考 |
|-------------|--------|--|--------------|
| 2020年12月24日 | Rev. 0 | 新規制定 | |
| 2021年1月15日 | Rev. 1 | ATENA の確認プロセス, 確認体制の明確化による修正 他 | 目次, 3, 4 ページ |
| 2023年7月14日 | Rev. 2 | 要件整合確認(手順書), 工事・検査完了確認, ATENA によるプロセス管理の追加, 基本方針に基づく対応フローの修正 他 | |
| 2023年7月24日 | Rev. 3 | 業務プロセスの継続的改善に関する運用の明確化 他 | |
| 2023年10月20日 | Rev. 4 | ATENA による技術課題管理、要件整合確認(詳細設計)の修正 他 | |

目次

| | |
|--------------------------------|----|
| 1. 目的 | 1 |
| 2. 基本的な取り組み方針 | 1 |
| 3. 実施計画確認および進捗状況確認の具体的な方法 | 3 |
| 4. 要件整合確認（詳細設計）の具体的な方法 | 4 |
| 5. 要件整合確認（手順書）の具体的な方法 | 5 |
| 6. 工事・検査完了確認の具体的な方法 | 7 |
| 7. ATENAによるプロセス管理 | 8 |
| 8. ATENAによる技術課題管理 | 8 |
| 9. 本取り組みのATENAの確認体制 | 9 |
| 10. 技術要件書の改定 | 9 |
| 11. 業務プロセスの継続的改善 | 10 |
| 添付資料 1 実施計画及び実績報告フォーマット | |
| 添付資料 2 要件整合性報告書（詳細設計）の記載フォーマット | |
| 添付資料 3 要件整合性報告書（手順書）の記載フォーマット | |
| 添付資料 4 工事開始及び検査開始の計画報告フォーマット | |

1. 目的

本要領は、国内の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原子力事業者（以下、「事業者」という。）の取り組み状況の確認等を的確に実施するため、具体的な実施方法等を定めるものである。

2. 基本的な取り組み方針

事業者が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を実施するにあたっての基本的な取り組み方針は、以下のとおりとする。

(1) 事業者は、原子力エネルギー協議会（以下、「ATENA」という。）第11回ステアリング会議（2020年1月9日開催）で決議した「デジタル安全保護回路のソフトウェア共通要因故障（以下、「ソフトウェアCCF」という。）対策」を、責任を持って自律的、かつ計画的に実施する。

(2) ATENAは、有効性評価手法および設備設計要求を明確にした技術要件書（「ATENA 20-ME05 Rev.1 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」）（以下、「技術要件書」という。）を発刊し、事業者に提示するとともに、各事業者に対して、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（詳細設計）の提出
- ④ 要件整合報告書（手順書）の提出
- ⑤ 工事・検査完了報告書の提出
- ⑥ 進捗状況の報告（半期ごと）

(3) 事業者は、(2)の対応を行うとともに、対策の計画および対策が完了の時点で安全性向上評価届出書を原子力規制委員会（以下、「NRA」という。）に提出する。

なお、再稼働前のプラントについては、(2)①実施計画書のATENAへの提出をもってこれに替える。

(4) ATENAは、以下の項目について、ATENAホームページ（以下、「HP」という。）に公開する。

- ① 技術要件書発行及び安全対策の実施要求
- ② 実施計画確認
- ③ 実施状況確認
- ④ 要件整合確認
- ⑤ 工事・検査完了確認

また、ATENA は、NRA に半期ごとに進捗状況を報告する。さらに、NRA から公開情報に関する問合せがあれば回答するとともに、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 および事業者は、ワーキンググループ（以下、「ATENA-WG」という。）等を通じて、対策実施状況、良好事例等の情報共有を継続して行う。

また、これらの基本方針に基づく対応フローを図-1 に示す。

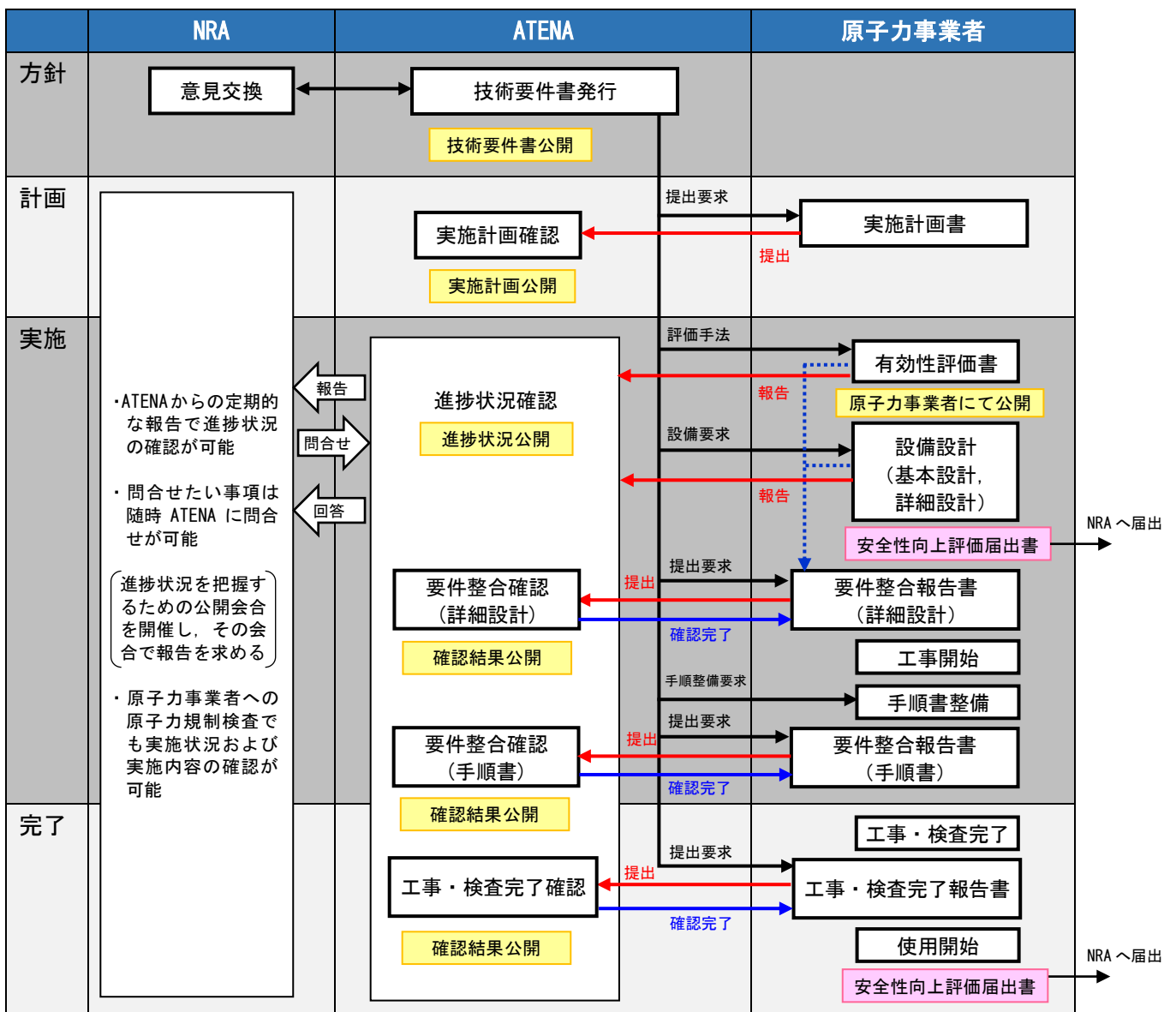


図-1 基本方針に基づく対応フロー

3. 実施計画確認および進捗状況確認の具体的な方法

事業者が実施する対策等の実施計画および進捗状況の確認は、以下のとおり実施する。

- (1) 事業者は、ATENA からの計画書提出要求に基づき、対策内容およびそれぞれのプロセス^{※1}の完了予定時期を示した実施計画書を ATENA に提出する。
実施計画及び実績報告フォーマットを添付資料 1 に示す。

- (2) ATENA は、各事業者から提出された実施計画書について確認を行い、その後、確認結果を HP で公開する。

ATENA の実施計画書の確認プロセスとしては、ATENA は、各事業者から提出された実施計画書について、必要に応じて事業者と協議をしながら、内容の確認を行い、その結果を取りまとめる。その確認結果について、ATENA 役員の承認を得る。その後、運営会議およびステアリング会議に報告する。

- (3) 事業者は、ATENA からの対策の進捗状況報告要求に基づき、半期ごとに、それぞれのプロセス^{※1}の進捗状況を ATENA に報告する。その際、事業者は、計画通りに実施できていない場合には、その理由を付して報告する。

- (4) ATENA は、各事業者から報告された実施計画の変更及び進捗状況について確認を行い、その後、確認結果を HP で公開する。

ATENA の進捗状況の確認プロセスとしては、ATENA は、各事業者から報告された進捗状況について、必要に応じて事業者と協議をしながら、内容の確認を行い、その結果を取りまとめる。その確認結果について、ATENA 役員の承認を得る。また、ATENA 役員の承認を得た内容を運営会議及びステアリング会議に報告する。

- (5) ATENA は、半期ごとに、確認した進捗状況について NRA に報告する。

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ともに、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。

^{※1} それぞれのプロセスとは、「有効性評価」、「基本設計」、「詳細設計」、「要件整合報告（詳細設計）」、「要件整合報告（手順書）」および「工事・検査完了報告」をいう。

4. 要件整合確認（詳細設計）の具体的な方法

(1) 事業者は、要件整合確認（詳細設計）が実施できた段階で、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（詳細設計）を取りまとめ、原子力本部長の責任の下、ATENAに提出する。

要件整合報告書（詳細設計）の記載フォーマットを添付資料2に示す。

(2) ATENAは、提出された事業者の要件整合報告書（詳細設計）に対して、下記の確認項目によるチェックシート形式で確認を行い、要件整合確認書（詳細設計）として取りまとめる。確認においては、必要に応じて改訂指示を出す。また、必要に応じてWGの専門家に意見照会を実施する。

【確認項目】

- ① 技術要件書の要求内容が漏れなく抽出されていること。
- ② 記載内容（概要）の欄に、設備仕様や有効性評価結果が記載され、要求内容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。

なお、技術要件書「3.5.8 安全保護回路への波及的影響防止」に関して、多様化設備はデジタル安全保護回路に対して隔離デバイス（アイソレータ等）による電氣的分離又は異なる筐体に設備を収納する等の物理的分離を考慮した設計であることが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。

(3) (2) の確認の結果について、ATENA 役員の承認をもって決定することとし、運営会議及びステアリング会議には事後に報告する取扱いとする。

(4) ATENAは、事業者の要件整合報告書（詳細設計）およびその確認結果である ATENA の要件整合確認書（詳細設計）を HP で公開する。

5. 要件整合確認（手順書）の具体的な方法

- (1) 事業者は、要件整合確認（手順書）が実施できた段階で、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（手順書）を取りまとめ、原子力本部長の責任の下、ATENA に提出する。要件整合報告書（手順書）の記載フォーマットを添付資料 3 に示す。
- (2) ATENA は、提出された事業者の要件整合報告書（手順書）に対して、要件整合報告書（詳細設計）に示された設備設計、及び有効性評価で想定した手段と運転操作条件が手順書に記載されており、その手順書に基づき運転員の習熟を図る教育及び訓練計画が定められていることを確認する。

具体的には、受領した要件整合報告書（手順書）及びそのエビデンス（手順及び教育訓練に係る規定文書）に対して、表 1 に示す確認内容及び確認の観点に基づき確認を行い、要件整合確認書（手順書）として取りまとめる。確認においては、必要に応じて改訂指示を出す。
- (3) (2) の確認の結果について、ATENA 役員の承認をもって決定することとし、運営会議及びステアリング会議には事後に報告する取扱いとする。
- (4) ATENA は、事業者の要件整合報告書（手順書）およびその確認結果である ATENA の要件整合確認書（手順書）を HP で公開する。

表 1 要件整合確認（手順書）における確認内容及び確認の観点

| 技術要件書の要求 | 確認内容 | 確認の観点 |
|---------------|---|--|
| 5.1 手順書の整備 | 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記載されていること。 | ① デジタル安全保護回路の自動作動が要求される状況において、デジタル安全保護回路が作動せずに多様化自動作動設備の自動作動や警報発信によってソフトウェア CCF 事象の発生を認知する手段と手順が記載されているか。 (PWR) その上で、ソフトウェア CCF 事象と重畳して発生している起因事象を判別する手順が記載されているか。(BWR では起因事象の判別は行わない。) |
| | 所定の手順に移行する方法が明確になっていること。 | ② (PWR) 起因事象を判別した結果から、所定の手順に移行する方法が記載されているか。 (BWR) ソフトウェア CCF 事象の発生を認知し、所定の手順に移行する方法が記載されているか。 |
| | 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。 | ③ 運転操作を行う場合の手段（自動作動機能、手動機能、警報機能、指示機能）とその判断条件（設定値や状態表示）及び操作・監視を行う場所（盤略号など）が記載されているか。 |
| | プラント状態を監視するための手段及びその設置場所が記載されていること。 | ④ 原子炉停止系統及び工学的安全施設の作動状況、多様化自動作動設備の作動状況及び手動操作によるプラント状態を監視するための手段（警報機能、指示機能など）及び監視を行う場所（盤略号など）が記載されているか。 |
| 5.2 教育及び訓練の実施 | 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。 | ⑤ デジタル安全保護回路のソフトウェア CCF の対応について運転員の習熟を図る教育及び訓練計画が記載されているか。 |

6. 工事・検査完了確認の具体的な方法

- (1) 事業者は、設計から検査実施までの品質保証体制、事業者自主検査結果及び運用開始後の管理体制について、表2に示す確認項目及び確認内容に基づき工事・検査完了報告書を取りまとめ、原子力本部長の責任の下、ATENAに提出する。

表2 確認項目及び確認内容

| 確認項目 | 確認内容 |
|------------|---|
| 品質保証体制 | 設計から検査実施までの品質保証体制について、設計及び工事計画認可申請／届出（以下、「設工認」という。）の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。 |
| 事業者自主検査結果 | <ul style="list-style-type: none">・使用前事業者検査と同等のプロセスで検査項目、検査内容、検査対象範囲が選定されていること。（様式8相当の整理）・既設設備については、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対象範囲が選定されていること。・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。・全ての検査項目について、判定基準を満足していること。 |
| 運用開始後の管理体制 | 保全計画、手順書の整備と教育及び訓練、故障時の対応及び日常管理について、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。 |

- (2) ATENA は、提出された事業者の工事・検査完了報告書及びそのエビデンスに対して、表2に示す確認項目及び確認内容に基づき確認を行い、工事・検査完了確認書として取りまとめる。確認においては、必要に応じて改定指示を出す。

- (3) ATENA（第3者機関含む）は、デジタル安全保護回路への波及的影響防止に係る要求事項に対して、表3に示す電气的分離及び物理的分離に関する事業者自主検査に同席し、事業者が使用前事業者検査と同等の検査体制で目視確認を行い、全ての検査項目、検査対象に対して検査が完了し、判定基準を満足していることを確認する。
- また、ATENA（第3者機関含む）から指摘があった場合、検査実施要領書の不適合管理に基づき対応する方針であることが、検査実施要領書又はオーソライズ資料（業務決定文書等）に定められていることを確認する。

表 3 現場同席の確認対象となる事業者自主検査

| No. | 確認項目 | 検査内容 |
|-----|-------|--|
| 1 | 電气的分離 | デジタル安全保護回路と多様化設備が部分的に設備を共用する場合には、隔離デバイス(アイソレータ等)が所定の位置に設置されていることを確認する。 |
| 2 | 物理的分離 | デジタル安全保護回路と多様化設備が部分的に設備を共用しない場合には、異なる筐体に設備が設置されていることを確認する。 |

(4) (2) の確認の結果について、ATENA 役員の承認をもって決定することとし、運営会議及びステアリング会議には事後に報告する取扱いとする。

(5) ATENA は、事業者の工事・検査完了報告書およびその確認結果である ATENA の工事・検査完了確認書を HP で公開する。

7. ATENA によるプロセス管理

(1) 事業者は、工事開始及び検査開始の計画(年月ベース)が決まった段階で、ATENA に報告する。また、計画変更の場合は、速やかに ATENA に報告を行う。

工事開始、検査開始及び使用開始の計画報告フォーマットを添付資料 4 に示す。

(2) ATENA は、各事業者の工事開始、検査開始及び使用開始の計画(年月ベース)を管理し、以下のプロセス管理を行う。また、ATENA は、事業者が ATENA の確認結果の通知をもって工事開始や対策設備の使用を開始する運用を文書に定めていることを確認する。

①事業者の工事開始前までに、ATENA の要件整合確認(詳細設計)を完了し、確認結果を事業者に通知する。

事業者は、ATENA の確認結果の通知をもって、工事を開始する。

②事業者の対策設備の使用開始前までに、ATENA の要件整合確認(手順書)及び工事・検査完了確認を完了し、確認結果を事業者に通知する。

事業者は、ATENA の確認結果の通知をもって、対策設備の使用を開始する。

8. ATENA による技術課題管理

(1) 事業者及びメーカーは、許認可実績のない手法、工法や設備を使用する等、新たな課題について幅広く抽出し、それぞれ各プラントに対し最低 3 件の課題を、その技術的論点を明確にした上で要件整合報告書提出の原則 3 か月前までに、ATENA に文書で連絡する。

- 課題の例
- ・許認可実績のない解析手法・コードを適用する場合
 - ・技術基準規則・民間規格への適合性に課題がある場合
 - ・技術基準規則・民間規格の解説に記載された例と相違する場合

- ・ エンドースが予定されている民間規格に相違する場合
- ・ 許認可実績のない設備設計や判断基準を適用する場合

(2) ATENA は、抽出された技術課題に対して、必要に応じて ATENA-WG の専門家に意見照会を行い、対応方針を取り纏め事業者に連絡する。

(3) ATENA は、必要に応じて NRA とコミュニケーションを図る。

(4) 事業者は、ATENA が取り纏めた「課題に対する対応方針」を受領後、対応方針に沿って必要に応じて妥当性を示す資料を添付し、要件整合報告書（詳細設計）を ATENA に提出する。

- 資料例
- ・ 有効性評価において許認可実績のない解析コードを適用する場合は、当該コードの妥当性確認及び検証の適切性について説明する資料。
 - ・ 多様化設備から安全保護系への波及的影響防止については、技術基準規則や民間規格 (JEAC4620-2020) への適合性について説明する資料。

9. 本取り組みの ATENA の確認体制

本取り組みにおける ATENA の確認体制は、図-2 のとおりである。

確認は、ATENA 担当部長の下、ATENA 確認チームにて実施する。なお、ATENA 確認チームの人選にあたっては、当該プラントのソフトウェア CCF 対策設備の設計・有効性評価などに直接関わっていないことを条件に、業務経歴をもとに力量を確認する。

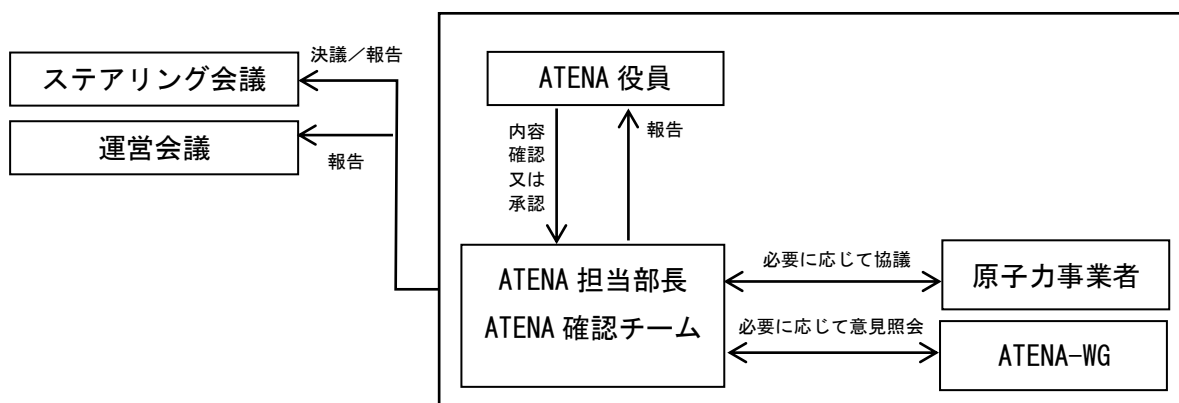


図-2 ATENA の確認体制

10. 技術要件書の改定

ATENA は、事業者の対策検討の進捗によりその内容が詳細化された場合やソフトウェア GCF に関する新知見が得られた場合には、技術要件書への反映の有無を確認し、必要に応じて改定を行う。

11. 業務プロセスの継続的改善

ATENA は、対象プラントの業務プロセスが一巡した時点、ならびに業務プロセスの遂行上、改善の必要性が認められる都度、業務プロセスの変更の要否を検討のうえ、変更が必要となる場合は本確認要領の変更案を作成し、ATENA 役員の承認を得て改定を行う。

以 上

実施計画及び実績報告フォーマット

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の実実施計画及び実績

作成日 : _____
 原子力事業者名 : _____
 発電所名 : _____

| 実施する対策内容 | | 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 (詳細設計) | 要件整合報告 (手順書) | 工事・検査 完了報告 | |
| | 予定 | | | | | | | |
| | 実績 | | | | | | | |

要件整合性報告書（詳細設計）の記載フォーマット
（3. 多様化設備要件）

| 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。 | 設備図書の該当箇所の記載内容の概要を記載する。 | ○ | 設計図書の記載内容が要求内容に整合している理由を記載する。 | 確認した設計図書名とその該当箇所を記載する |
| 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。 | <div style="border: 1px solid black; padding: 5px; width: fit-content; margin: 10px auto;"> 除外規定等を適用しない場合は、該当なし「—」を記入する。 </div> <p style="text-align: center;">—</p> | — | 該当しない理由を記載する。(除外規定等を適用しない等) | 設計図書に記載(除外規定等を適用しない等)がある場合は、確認した設計図書名とその該当箇所を記載する。 理由欄で説明できる場合は、「—」を記載してもよい。 |

(判定記号) ○ : 整合有 — : 該当し

要件整合性報告書（詳細設計）の記載フォーマット
（４．有効性評価）

| 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 | | | |
|---|----------------------------|-------|----------------------------------|---|
| | 記載内容(概要) | 要件整合性 | | 有効性評価図書 |
| | | 判定 | 理由 | |
| 要求内容 | | | | |
| 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。 | 有効性評価図書の該当箇所の記載内容の概要を記載する。 | ○ | 有効性評価図書の記載内容が要求内容に整合している理由を記載する。 | 確認した有効性評価図書名とその該当箇所を記載する |
| 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。 | — | — | 該当しない理由を記載する。(他の判断基準を用いない等) | 有効性評価図書に記載(他の判断基準を用いない等)がある場合は、確認した有効性評価図書名とその該当箇所を記載する。 理由欄で説明できる場合は、「—」を記載してもよい。 |

他の判断基準を用いない場合は、該当なし「—」を記入する。

(判定記号) ○ : 整合有 — : 該当し

要件整合性報告書（手順書）の記載フォーマット
 （5. 手順書の整備と教育及び訓練の実施）

| ATENA 技術要件書 | ソフトウェア CCF 対策手順書、教育及び訓練の要件整合性 | | | |
|--|---|-------|---|--------------------------------|
| | 記載内容(概要) | 要件整合性 | | 規定文書 |
| 要求内容 | | 判定 | 理由 | |
| 5.1 手順書の整備 | | | | |
| <p>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。</p> | <p>手順書の整備方針および整備した手順の種類や具値的な内容を記載する。</p> | ○ | <p>本文表1に示す確認内容及び確認の観点に基づき、規定文書に手順が定められていることを確認し、その確認結果を記載する。</p> | <p>確認した個別の手順書名を記載する</p> |
| 5.2 教育及び訓練の実施 | | | | |
| <p>運転員には、運転時の異常な過渡変化又は設計基準事故とソフトウェア CCF が重畳する事象に対して、整備された手順書に従一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。</p> | <p>手順書に従一的確な対処をするために教育及び訓練を実施する計画(対象者、頻度)が定められていることを記載する。</p> | ○ | <p>本文表1に示す確認内容及び確認の観点に基づき、規定文書に運転員の習熟を図る教育及び訓練計画が記載されていることを確認し、その確認結果を記載する。</p> | <p>確認した規定文書名およびその該当箇所を記載する</p> |

工事開始及び検査開始の計画報告フォーマット

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のうち工事・検査及び手順書整備の実施計画及び実績（詳細）

作成日： _____
 原子力事業者名： _____
 発電所名： _____

| ユニット名 | | 工事・検査及び手順書整備予定時期 | | | | | | 備考 |
|-------|----|------------------|----|------|------|-------|------|----|
| | | 定検回次 | 解列 | 工事開始 | 検査開始 | 手順書整備 | 使用開始 | |
| | 予定 | | | | | | | |
| | 実績 | | | | | | | |