大飯発電所３号機及び４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確認書（詳細設計）

2023年　8月28日

原子力エネルギー協議会

1. はじめに

関西電力(株)は，大飯発電所 3 号機及び 4 号機の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。)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，技術要件書※の「3. 多様化設備要件」及び「4. 有効性評価」の各要求内容に整合しているかの確認を行い，2023 年 1 月 27 日に「大飯発電所 3 号機及び 4 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」を ATENA に提出した。

ATENA は，受領した要件整合報告書の確認を行い，記載内容の追加及び記載の適正化が必要と判断し，2023 年 4 月 13 日に関西電力(株)に対して要件整合報告書の改訂を指示し，関西電力(株)は 2023 年 4 月 21 日に「大飯発電所 3 号機及び 4 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)(以下，「要件整合報告書(詳細設計)」という。)」として改訂版を ATENA に提出した。

また，ATENA は、2023 年 8 月 2 日に関西電力(株)に対して先行プラントの対応を踏まえた記載フォーマットの統一を指示し，関西電力(株)は 2023 年 8 月 18 日に要件整合報告書(詳細設計)(改訂 1)として改訂版を ATENA に提出した。

ATENA は，受領した要件整合報告書(詳細設計)(改訂 1)の確認を行い，確認結果を本要件整合確認書(詳細設計)として取りまとめた。

※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(ATENA 20-ME05 Rev.1)

2. 確認方法

要件整合確認(詳細設計)は，技術要件書の各要求内容に対して下記の確認項目についてチェックシート形式で確認を行った。

なお，今回の要件整合確認(詳細設計)における確認体制及び確認フローについて添付資料 1 に，改訂指示の内容について添付資料 2 に示す。

【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。
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. 要件整合確認結果

(1)「3. 多様化設備要件」

多様化設備に対する要件整合性について，以下に示す技術要件書の各要求内容に対して，要件整合報告書(詳細設計)(改訂 1)及び各設計図書の記載内容を確認した結果，全ての要求内容に対して整合していることを確認した。

なお，技術要件書の「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)による電気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を設計図書により確認した。

各要求内容に対する確認結果については表 1 に示す。

【技術要件書の各要求内容】

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

(2)「4. 有効性評価」

有効性評価に対する要件整合性について，以下に示す技術要件書の各要求内容に対して，要件整合報告書(詳細設計)(改訂 1)及び有効性評価図書の記載内容を確認した結果，全ての要求内容に対して整合していることを確認した。

各要求内容に対する確認結果については表 2 に示す。

【技術要件書の各要求内容】

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. まとめ

要件整合報告書(詳細設計)(改訂 1)の確認の結果，技術要件書の「3. 多様化設備要件」及び「4. 有効性評価」の各要求内容に対して全て整合していることを確認した。

5. 添付資料

添付資料 1 要件整合確認における確認体制及び確認フロー
添付資料 2 大飯発電所 3 号機及び 4 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) コメント処理表

表１　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確認結果
【対象：大飯発電所３号機及び４号機（多様化設備要件）】

（記号）○：整合性有　－：該当なし

ATENA 技術要件書	事業者の要件整合報告の内容				ATENA による要件整合確認結果※				
	記載内容（概要）	要件整合性		設計図書					
要求内容		判定	理由		①	②	③	④	⑤
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。 なお、共通要因故障対策設備のうち設計基準対象施設及び重大事故等対処設備を兼ねる設備については、機器仕様に変更がないため、既存設備状態を示す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(38/55) ・共通要因故障対策設備基本設計方針書 1 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。	－	－	多様化設備を設置する計画であるため、考慮しない。	・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(38/55)	－	－	－	－	－

※確認要領：確認項目①②③④⑤の欄ごとに確認結果を記入（確認できた場合「✓」，該当なしの場合「-」を記入）
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。
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。

表１　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確認結果
【対象：大飯発電所３号機及び４号機（多様化設備要件）】

（記号）○：整合性有　－：該当なし

ATENA 技術要件書	事業者の要件整合報告の内容				ATENA による要件整合確認結果※				
	記載内容（概要）	要件整合性		設計図書					
要求内容		判定	理由		①	②	③	④	⑤
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の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 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 安全保護アナログ盤作動警報 加圧器圧力低安全注入作動警報 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 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。 なお、共通要因故障対策設備のうち設計基準対象施設及び重大事故等対処設備を兼ねる設備については、機器仕様に変更がないため、既存設備状態を示す図書により確認した。	・共通要因故障対策設備基本設計方針書6.1章 ・原子炉制御保護系ファンクナルダイヤグラム　シート21 ・補機インターロック線図 SHEET NO.4-6	✓	✓	✓	✓	✓

※確認要領：確認項目①②③④⑤の欄ごとに確認結果を記入（確認できた場合「✓」，該当なしの場合「-」を記入）
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。
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。

表１　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確認結果
【対象：大飯発電所３号機及び４号機（多様化設備要件）】

（記号）〇：整合性有　－：該当なし

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、中央制御室に上記の「安全保護アナログ盤作動警報」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る。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 (38/55)	✓	✓	✓	✓	✓

※確認要領：確認項目①②③④⑤の欄ごとに確認結果を記入（確認できた場合「✓」，該当なしの場合「-」を記入）
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。
③要件整合判定が全て「〇」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。

表１　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確認結果
【対象：大飯発電所３号機及び４号機（多様化設備要件）】

（記号）〇：整合性有　－：該当なし

ATENA 技術要件書	事業者の要件整合報告の内容				ATENA による要件整合確認結果※				
	記載内容（概要）	要件整合性		設計図書					
要求内容		判定	理由		①	②	③	④	⑤
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①～⑦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 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 安全保護アナログ盤 （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 安全保護アナログ盤作動警報 加圧器圧力低安全注入作動警報 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 原子炉安全保護計装盤（炉外核計測装置含むアナログ回路部） 補機制御設備（安全保護シーケンス盤）	○	多様化設備である共通要因故障対策設備の対象範囲について、当該プラントの安全保護回路のデジタル化の範囲に応じて選定されたことも含めて、設計図書にて明確化されていることを確認した。	・共通要因故障対策設備基本設計方針書 2 章、6.1.1 章、6.1.2 章、6.1.4 章、6.1.5 章、図 6-1	✓	✓	✓	✓	✓

※確認要領：確認項目①②③④⑤の欄ごとに確認結果を記入（確認できた場合「✓」，該当なしの場合「-」を記入）
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。
③要件整合判定が全て「〇」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。

表１　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確認結果
【対象：大飯発電所３号機及び４号機（多様化設備要件）】

（記号）〇：整合性有　－：該当なし

ATENA 技術要件書	事業者の要件整合報告の内容				ATENA による要件整合確認結果※				
	記載内容（概要）	要件整合性		設計図書					
要求内容		判定	理由		①	②	③	④	⑤
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確認した。 なお、共通要因故障対策設備のち設計基準対象施設及び重大事故等対処設備を兼ねる設備については、機器仕様に変更がないため、既存設備状態を示す図書により確認した。	－	－	－	－	－	－

※確認要領：確認項目①②③④⑤の欄ごとに確認結果を記入（確認できた場合「✓」，該当なしの場合「-」を記入）
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。
③要件整合判定が全て「〇」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。

表１　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確認結果
【対象：大飯発電所３号機及び４号機（多様化設備要件）】

（記号）○：整合性有　－：該当なし

ATENA 技術要件書	事業者の要件整合報告の内容				ATENA による要件整合確認結果※				
	記載内容（概要）	要件整合性		設計図書					
要求内容		判定	理由		①	②	③	④	⑤
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(38/55) ・共通要因故障対策設備基本設計方針書 5.2 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 (39/55) ・共通要因故障対策設備基本設計方針書 5.16 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。	・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 (39/55) ・共通要因故障対策設備基本設計方針書 5.3.1 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。	―	―	ハード回路を用いた設計とする計画であるため、考慮しない。	・共通要因故障対策設備基本設計方針書 5.3.1 章	―	―	―	―	―

※確認要領：確認項目①②③④⑤の欄ごとに確認結果を記入（確認できた場合「✓」，該当なしの場合「-」を記入）
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。
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。

表１　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確認結果
【対象：大飯発電所３号機及び４号機（多様化設備要件）】

（記号）○：整合性有　－：該当なし

ATENA 技術要件書	事業者の要件整合報告の内容				ATENA による要件整合確認結果※				
	記載内容（概要）	要件整合性		設計図書					
要求内容		判定	理由		①	②	③	④	⑤
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（39/55） ・共通要因故障対策設備基本設計方針書 5.9 章	✓	✓	✓	✓	✓
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安全保護アナログ盤については、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（39/55） ・共通要因故障対策設備基本設計方針書 5.8 章 ・安全保護アナログ盤 耐震解析計算書	✓	✓	✓	✓	✓
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、安全系計装用無停電電源母線（インバータ）に接続される計装用電源装置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（39/55） ・共通要因故障対策設備基本設計方針書 5.14 章 ・所内単線結線図 ・計装用電源単線結線図	✓	✓	✓	✓	✓
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、2つ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。	○	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（39/55） ・共通要因故障対策設備基本設計方針書 5.17 章	✓	✓	✓	✓	✓

※確認要領：確認項目①②③④⑤の欄ごとに確認結果を記入（確認できた場合「✓」，該当なしの場合「-」を記入）
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。
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。

表１　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確認結果
【対象：大飯発電所３号機及び４号機（多様化設備要件）】

（記号）○：整合性有　－：該当なし

ATENA 技術要件書	事業者の要件整合報告の内容				ATENA による要件整合確認結果※				
	記載内容（概要）	要件整合性		設計図書					
要求内容		判定	理由		①	②	③	④	⑤
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、定期事業者検査時において、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（39/55） ・共通要因故障対策設備基本設計方針書 5.5 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に対して隔離デバイス（アイソレータ等）による電気的分離及び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（39/55） ・共通要因故障対策設備基本設計方針書 5.4 章 ・原子炉保護系ブロック図 ・安全保護シーケンス盤装置ロジック図	✓	✓	✓	✓	✓
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。	○	多様化設備である共通要因故障対策設備が仮に火災・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。 また、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（39/55） ・共通要因故障対策設備基本設計方針書 5.12 章	✓	✓	✓	✓	✓

※確認要領：確認項目①②③④⑤の欄ごとに確認結果を記入（確認できた場合「✓」，該当なしの場合「-」を記入）
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。
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。

表１　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確認結果
【対象：大飯発電所３号機及び４号機（多様化設備要件）】

（記号）○：整合性有　－：該当なし

ATENA 技術要件書	事業者の要件整合報告の内容				ATENA による要件整合確認結果※				
	記載内容（概要）	要件整合性		設計図書					
要求内容		判定	理由		①	②	③	④	⑤
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（39/55） ・共通要因故障対策設備基本設計方針書 5.10 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、原則として中央制御室に設置する。また、手動操作器は誤操作防止を考慮した設計とする。	○	誤操作防止を考慮した手動操作器及び表示を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（39/55） ・共通要因故障対策設備基本設計方針書 5.13.1 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。	－	－	手動操作器は中央制御室に設置済みであるため考慮しない。	・デジタル安全保護系共通要因故障対策基本方針書 2.3 章（18/55） ・共通要因故障対策設備基本設計方針書 6.1.2 章	－	－	－	－	－

※確認要領：確認項目①②③④⑤の欄ごとに確認結果を記入（確認できた場合「✓」，該当なしの場合「-」を記入）
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。
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。

表１　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確認結果
【対象：大飯発電所３号機及び４号機（多様化設備要件）】

（記号）○：整合性有　－：該当なし

ATENA 技術要件書	事業者の要件整合報告の内容				ATENA による要件整合確認結果※				
	記載内容（概要）	要件整合性		設計図書					
要求内容		判定	理由		①	②	③	④	⑤
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」で示した安全保護アナログ盤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 (39/55) ・共通要因故障対策設備基本設計方針書 5.13.1 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（安全保護アナログ盤）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安全保護アナログ監視パネルに警報が表示される設計とする。	○	安全保護アナログ盤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。	・共通要因故障対策設備基本設計方針書 5.13.1 章、6.1.4 章、6.1.5 章	✓	✓	✓	✓	✓

※確認要領：確認項目①②③④⑤の欄ごとに確認結果を記入（確認できた場合「✓」，該当なしの場合「-」を記入）
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。
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。

表 2　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確認結果
【対象：大飯発電所 3 号機及び 4 号機（有効性評価）】

（記号）○：整合性有　－：該当なし

ATENA 技術要件書	事業者の要件整合報告の内容				ATENA による要件整合確認結果※				
	記載内容（概要）	要件整合性		有効性評価図書					
要求内容		判定	理由		①	②	③	④	⑤
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、アナログ回路で構成される現行措置の多様化設備の作動により原子炉トリップに至るため、「重大事故等対策の有効性評価」の1つである原子炉停止機能喪失（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、多様化設備等を用いて事象対応を行う場合における運転操作や操作時間が許可処分済みの設置変更許可申請書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、ソフトウェアCCF の重畳を考慮した場合でも、許可処分済みの設置変更許可申請書添付書類十解析に対して、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。	○	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） 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）	✓	✓	✓	✓	✓

※確認要領：確認項目①②③④⑤の欄ごとに確認結果を記入（確認できた場合「✓」，該当なしの場合「-」を記入）
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。
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。

表 2　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確認結果
【対象：大飯発電所 3 号機及び 4 号機（有効性評価）】

（記号）○：整合性有　－：該当なし

ATENA 技術要件書	事業者の要件整合報告の内容				ATENA による要件整合確認結果※				
	記載内容（概要）	要件整合性		有効性評価図書					
要求内容		判定	理由		①	②	③	④	⑤
・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.228） 4.6.3.3 燃料集合体の落下 （P.230）	✓	✓	✓	✓	✓
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）	✓	✓	✓	✓	✓

※確認要領：確認項目①②③④⑤の欄ごとに確認結果を記入（確認できた場合「✓」，該当なしの場合「-」を記入）
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。
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。

表 2　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確認結果
【対象：大飯発電所 3 号機及び 4 号機（有効性評価）】

（記号）○：整合性有　－：該当なし

ATENA 技術要件書	事業者の要件整合報告の内容				ATENA による要件整合確認結果※				
	記載内容（概要）	要件整合性		有効性評価図書					
要求内容		判定	理由		①	②	③	④	⑤
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）	✓	✓	✓	✓	✓
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，判断基準を概ね満足しながら，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）	✓	✓	✓	✓	✓
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	✓	✓	✓	✓	✓

※確認要領：確認項目①②③④⑤の欄ごとに確認結果を記入（確認できた場合「✓」，該当なしの場合「-」を記入）
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。
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。

表 2　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確認結果
【対象：大飯発電所 3 号機及び 4 号機（有効性評価）】

（記号）〇：整合性有　－：該当なし

ATENA 技術要件書	事業者の要件整合報告の内容				ATENA による要件整合確認結果※				
	記載内容（概要）	要件整合性		有効性評価図書					
要求内容		判定	理由		①	②	③	④	⑤
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。	〇	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。	—	—	技術要件書の緩和規定の適用は必須ではなく、計装上の誤差の考慮は保守的な設定としている。	4.3 基本解析条件 （P.16,P.17）	—	—	—	—	—
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り、誤作動が起因ではないため、現実的な操作の条件を仮定する必要はない。	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。	〇	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。	〇	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	✓	✓	✓	✓	✓

※確認要領：確認項目①②③④⑤の欄ごとに確認結果を記入（確認できた場合「✓」，該当なしの場合「-」を記入）
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。
③要件整合判定が全て「〇」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。

表 2　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確認結果
【対象：大飯発電所 3 号機及び 4 号機（有効性評価）】

（記号）○：整合性有　－：該当なし

ATENA 技術要件書	事業者の要件整合報告の内容				ATENA による要件整合確認結果※				
	記載内容（概要）	要件整合性		有効性評価図書					
要求内容		判定	理由		①	②	③	④	⑤
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）	✓	✓	✓	✓	✓
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。	多様化設備を含めて単一故障は想定していない。	○	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。	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）	✓	✓	✓	✓	✓
・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。	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を除き作動を仮定しており、多様化設備が作動させる原子炉停止系統、工学的安全施設等の故障及び誤作動が起因となる事象は想定していない。	○	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。	4.3 基本解析条件 （P.14）	✓	✓	✓	✓	✓

※確認要領：確認項目①②③④⑤の欄ごとに確認結果を記入（確認できた場合「✓」，該当なしの場合「-」を記入）
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。
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。

表 2　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確認結果
【対象：大飯発電所 3 号機及び 4 号機（有効性評価）】

（記号）○：整合性有　－：該当なし

ATENA 技術要件書	事業者の要件整合報告の内容				ATENA による要件整合確認結果※				
	記載内容（概要）	要件整合性		有効性評価図書					
要求内容		判定	理由		①	②	③	④	⑤
・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	✓	✓	✓	✓	✓
・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	―	―	―	―	―

※確認要領：確認項目①②③④⑤の欄ごとに確認結果を記入（確認できた場合「✓」，該当なしの場合「-」を記入）
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。
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。

表 2　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確認結果
【対象：大飯発電所 3 号機及び 4 号機（有効性評価）】

（記号）〇：整合性有　－：該当なし

ATENA 技術要件書	事業者の要件整合報告の内容				ATENA による要件整合確認結果※				
	記載内容（概要）	要件整合性		有効性評価図書					
要求内容		判定	理由		①	②	③	④	⑤
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）	✓	✓	✓	✓	✓

※確認要領：確認項目①②③④⑤の欄ごとに確認結果を記入（確認できた場合「✓」，該当なしの場合「-」を記入）
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。
③要件整合判定が全て「〇」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。

要件整合確認（詳細設計）における確認体制及び確認フロー

要件整合確認(詳細設計)における確認体制及び確認フロー

1. 確認体制

今回の要件整合確認(詳細設計)は, 下表に示す ATENA 確認チームにて実施した。

なお, ATENA 確認チームの人選にあたっては, 当該プラントのデジタル 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した。

表 ATENA 確認チーム

	氏名	所属・役職	担当範囲
責任者	[redacted]	原子力エネルギー協議会 技術班 部長	3. 多様化設備要件 4. 有効性評価
担当者	[redacted]	原子力エネルギー協議会 運営班 副部長	3. 多様化設備要件
	[redacted]	原子力エネルギー協議会 運営班 副部長	4. 有効性評価

2. 確認フロー

今回の要件整合確認(詳細設計)は, 以下のフローで実施した。

- ATENA-WG(デジタル CCF-WG)にて要件整合報告書(詳細設計)の記載内容や様式の検討を行い, その検討結果をもとに事業者は要件整合報告書(詳細設計)を取りまとめ, ATENA に提出した。
- ATENA は, 受領した要件整合報告書(詳細設計)に対して, ATENA 確認チームによる要件整合確認を行い, 記載内容の追加及び記載の適正化が必要と判断し, 事業者に対して要件整合報告書(詳細設計)の改訂を指示し, 事業者は要件整合報告書(詳細設計)の改訂版を ATENA に提出した。
- ATENA は、先行プラントの対応を踏まえた記載フォーマットの統一を事業者に指示し, 事業者は要件整合報告書(詳細設計)の改訂版(改訂 1)を ATENA に提出した。
- ATENA 確認チームは, 受領した要件整合報告書(詳細設計)の改訂版(改訂 1)に対して, 要件整合確認を行い, 確認結果を ATENA 役員に報告し, 承認を得た。

大飯発電所３号機及び４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） コメント処理表

大飯発電所 3 号機及び 4 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）
コメント処理表

No.	送付日	ATENA コメント		事業者回答	ATENA 確認結果	
		該当箇所（章・節・行）	コメント内容	コメント反映内容	確認内容	確認日
1	2023.4.13	3.1 設置要求 2 行目 （理由） （設計図書）	技術要件書に規定する除外・緩和規定に対して該当しない場合、該当しない理由を理由欄に記載して下さい。また、設計図書に記載がある場合は、設計図書欄に設計図書の該当箇所を記載して下さい。	理由欄に以下の記載を追加する。 ・多様化設備を設置する計画であるため、考慮しない。 設計図書欄に以下の記載を追加する。 ・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（38/55）	改訂版に反映されていることを確認した。	2023.8.21
2	2023.4.13	3.3 多様化設備の範囲 1行目 （理由）	技術要件書の要求との対応・整合性をより明確に表現するため、例えば「・・・対象範囲については、当該プラントの安全保護回路のデジタル化の範囲等に応じて選定された事も含めて、設計図書にて明確化されていることを確認した。」というような記載の充実をお願いします。	以下の記載に見直す。 ・多様化設備である共通要因故障対策設備の対象範囲について、当該プラントの安全保護回路のデジタル化の範囲に応じて選定されたことも含めて、設計図書にて明確化されていることを確認した。	改訂版に反映されていることを確認した。	2023.8.21
3	2023.4.13	3.5.2 多様性 3 行目 （理由） （設計図書）	技術要件書に規定する除外・緩和規定に対して該当しない場合、該当しない理由を理由欄に記載して下さい。また、設計図書に記載がある場合は、設計図書欄に設計図書の該当箇所を記載して下さい。	理由欄に以下の理由を記載する。 ・ハード回路を用いた設計とする計画であるため、考慮しない。 設計図書欄に以下の記載を追加する。 ・共通要因故障対策設備基本設計方針書 5.3.1 章	改訂版に反映されていることを確認した。	2023.8.21
4	2023.4.13	3.5.5 供給電源 1 行目 （理由）	多様化設備基本設計方針書 5.16 章では「・・・原則として計装用無停電電源母線（インバータ）に接続される計装用電源装置から給電されるものとする」との記載であり、非常用電源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こととの要求内容との整合性が明示的に読み取れるような記載に見直して下さい。	理由欄を以下の記載に見直す。 ・多様化設備である共通要因故障対策設備は、安全系計装用無停電電源母線（インバータ）に接続される計装用電源装置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。 設計図書に以下の資料を追加する。 ・所内単線結線図 ・計装用電源単線結線図	改訂版に反映されていることを確認した。	2023.8.21
5	2023.4.13	3.5.8 安全保護回路への波及的影響防止 （記載内容） （理由） （設計図書）	具体的な対策として、電気的分離（アイソレーションカード）、物理的分離（独立性）、自動作動阻止機能についての詳細を記載内容等に追加し、必要な設計図書と判断の理由も追加する必要がある。	理由欄を以下の記載に見直す。 ・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に対して隔離デバイス（アイソレータ等）による電気的分離及び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を設計図書により確認した。 設計図書に以下の資料を追加する。 ・原子炉保護系ブロック図 ・安全保護シーケンス盤装置ロジック図	改訂版に反映されていることを確認した。	2023.8.21

大飯発電所 3 号機及び 4 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）
コメント処理表

No.	送付日	ATENA コメント		事業者回答	ATENA 確認結果	
		該当箇所（章・節・行）	コメント内容	コメント反映内容	確認内容	確認日
6	2023.4.13	3.5.11 操作性 2 行目 （理由） （設計図書）	技術要件書に規定する除外・緩和規定に対して該当しない場合、該当しない理由を理由欄に記載して下さい。また、設計図書に記載がある場合は、設計図書欄に設計図書の該当箇所を記載して下さい。	理由欄に以下の理由を記載する。 ・手動操作器は中央制御室に設置済みであるため考慮しない。 設計図書欄に以下の記載を追加する。 ・デジタル安全保護系共通要因故障対策基本方針書 2.3 章（18/55） ・共通要因故障対策設備基本設計方針書 6.1.2 章	改訂版に反映されていることを確認した。	2023.8.21
7	2023.4.13	4.2 評価すべき事象 3 行目 （記載内容）	解析を省略する事象について「判断基準に対して影響が軽微である」と評価する理由の説明が省略されており、本書の記載される内容の範囲では、技術要件書に記される解析を省略できる条件に当てはまっているか客観的に判断できないため、条件や比較対象を明確にして説明を追加して下さい。	以下の記載に見直す。 「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、アナログ回路で構成される現行措置の多様化設備の作動により原子炉トリップに至るため、「重大事故等対策の有効性評価」の1つである原子炉停止機能喪失（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、多様化設備等を用いて事象対応を行う場合における運転操作や操作時間が許可処分済みの設置変更許可申請書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、ソフトウェア CCF の重畳を考慮した場合でも、許可処分済みの設置変更許可申請書添付書類十解析に対して、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。	改訂版に反映されていることを確認した。	2023.8.21
8	2023.4.13	4.4.2 解析で想定する現実的な条件等 3 行目 （「記載内容） （理由）	技術要件書に示す緩和規定を適用していないという事が「記載内容（概要）」欄に明記されていない。「理由」欄の記載は技術要件書の緩和規定の適用は必須ではないという事を明記下さい。	記載内容欄は該当なし「―」とする。 理由欄を以下の記載に見直す。 ・技術要件書の緩和規定の適用は必須ではなく、計装上の誤差の考慮は保守的な設定としている。	改訂版に反映されていることを確認した。	2023.8.21

大飯発電所 3 号機及び 4 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）
コメント処理表

No.	送付日	ATENA コメント		事業者回答	ATENA 確認結果	
		該当箇所（章・節・行）	コメント内容	コメント反映内容	確認内容	確認日
9	2023.4.13	4.4.2 解析で想定する現実的な条件等 4 行目 （理由）	「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仮定する必要はない」という解説が判り難いため、要求される技術要件との関連で解説を補足下さい。	理由欄を以下の記載に見直す。 ・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り、誤作動が起因ではないため、現実的な操作の条件を仮定する必要はない。	改訂版に反映されていることを確認した。	2023.8.21
10	2023.4.13	4.4.5 多様化設備に関連する条件(1) 機器条件 1 行目 （記載内容） （理由） （有効性評価図書）	記載内容（概要）欄が「―」となっているが、有効性評価図書の該当箇所の内容を記載し、有効性評価図書欄に該当箇所を記載して下さい。	記載内容（概要）欄を以下の記載に見直す。 ・多様化設備を含めて単一故障は想定していない。 有効性評価図書欄に以下を記載する。 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）	改訂版に反映されていることを確認した。	2023.8.21
11	2023.4.13	4.4.5 多様化設備に関連する条件(1) 機器条件 2 行目 （記載内容） （理由） （有効性評価図書）	記載内容（概要）欄が「－」となっているが、有効性評価図書の該当箇所の内容を記載し、有効性評価図書欄に該当箇所を記載して下さい。	記載内容（概要）欄を以下の記載に見直す。 ・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を除き作動を仮定しており、多様化設備が作動させる原子炉停止系統、工学的安全施設等の故障及び誤作動が起因となる事象は想定していない。 有効性評価図書欄に以下を記載する。 4.3 基本解析条件（P.14）	改訂版に反映されていることを確認した。	2023.8.21