伊方発電所3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）

四国電力株式会社

改訂来歴

番号	年月日	内容	備考
初版	2024/4/25	新規作成	
1	2024/7/3	・詳細設計の結果、警報表示灯の電源について計装用分電盤内の接続先を変更するため、添付資料 1-9 計装用電源単線結線図に反映する。 ・記載の適正化	
―以下余白―			

伊方発電所3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）

目次

Ⅰ．本文

伊方発電所3号機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（以下、「ソフトウェア CCF」という。）緩和対策について、「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）」（以下、「ATENA 技術要件書」という。）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要件整合性の確認を行い、「伊方発電所3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）の提出について（原子力発第 24043 号、令和6年4月25日」を ATENA に提出している。

その後、工事の詳細設計により、共通要因故障対策設備の警報表示灯の電源について、計装用分電盤内の接続先を変更するため、添付書類の添付資料に反映し、再提出を行う。

なお、「5. 手順書の整備と教育及び訓練の実施」については、当社が原子力エネルギー協議会（以下、「ATENA」という。）へ提出した「「デジタル安全保護系のソフトウェア共通要因故障への対応」に基づく安全対策に係る実施状況の定期報告について」（原子力発第 24037 号　令和 6 年 4 月 4 日）において「ハード対策完了までに実施予定」としていることから、本報告書の対象外とする。

1．確認方法

ATENA 技術要件書に記載された要求内容に対して、各要件に対応する設計図書、有効性評価図書等の記載内容を確認し、要求内容ごとに要件整合性の判定及びその理由を記載する。

2．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 ATENA 技術要件書の各要求内容に対して、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。各要求内容に対する確認結果については表1に示す。

【ATENA 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 ATENA 技術要件書の各要求内容に対して、有効性評価図書(「三菱PWR 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有効性評価について※」MHI-NES-1075、三菱重工業株式会社、令和4年6月)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。

※:本図書では代表 3、4 ループの解析結果及びそれらを基にした PWR プラントの有効性評価の検討結果を記載しており、伊方3号機の有効性評価は包含される。

【ATENA 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

（判定記号）○：整合有　－：該当なし

表1 「3. 多様化設備要件」に関する要件整合性確認表(1/8)

ATENA 技術要件書	ソフトウェア CCF 対策設備設計図書の要件整合性			
	記載内容(概要)	要件整合性		設計図書
要求内容		判定	理由	
3.1 設置要求				
デジタル安全保護回路を設ける場合には、代替機能を有する多様化設備を設置しなければならない。	デジタル安全保護回路の代替機能を有する、多様化設備である共通要因故障対策設備を設置する。	○	デジタル安全保護回路がソフトウェア 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(39/56) ・多様化設備基本設計方針書 2 章
ただし、ソフトウェア CCF が発生するおそれがない場合、若しくは運転時の異常な過渡変化又は設計基準事故が発生し、かつ安全保護回路の一部がソフトウェアにより作動するものがある場合で、当該ソフトウェアが機能しない場合を想定しても、他の安全保護回路の安全機能が作動することにより設計基準事故の判断基準を概ね満足することが有効性評価により確認できる場合には、多様化設備を設けなくてもよい。	－	－	多様化設備を設置する計画であるため、該当しない。	・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(39/56)

（判定記号）○：整合有　－：該当なし

表1 「3. 多様化設備要件」に関する要件整合性確認表(2/8)

ATENA 技術要件書	ソフトウェア CCF 対策設備設計図書の要件整合性			
	記載内容(概要)	要件整合性		設計図書
要求内容		判定	理由	
3.2 機能要求				
多様化設備は、運転時の異常な過渡変化又は設計基準事故が発生し、かつソフトウェア CCF により安全機能が喪失した場合においても、設計基準事故の判断基準を概ね満足できるよう、原子炉停止系統、工学的安全施設等を自動、又は手動で作動させることができなければならない。	デジタル安全保護回路が共通要因故障によってその機能をすべて喪失し、かつ運転時の異常な過渡変化、又は設計基準事故が発生した場合でも設計基準事故の判断基準を概ね満足することができる設備を共通要因故障対策設備として設ける。 多様化設備である共通要因故障対策設備には、ソフトウェア CCF 対策として、原子炉停止系統及び工学的安全施設等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(高圧注入／低圧注入)　他 (別表2「共通要因故障対策設備が有する手動作動機能一覧表」参照) ・警報機能 多様化自動作動設備作動警報 加圧器圧力異常低警報　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 蒸気発生器狭域水位指示 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。	・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(39,43,44/56) ・多様化設備基本設計方針書　7.1.1 章、7.1.3 章、7.2.1 章、7.2.2 章 ・原子炉制御保護系ファンクショナルダイヤグラム　シート 22 ・補機インターロック線図　SHEET 4-9
さらに、原子炉停止系統、工学的安全施設等を手動により作動させる場合には、運転員が必要な時間内に操作を開始し、判断基準を概ね満足した状態で事象を収束させることができるよう、運転時の異常な過渡変化又は設計基準事故の発生時に安全保護回路の安全機能動作の異常の発生を認知し、必要な操作の判断を行える機能を設けなければならない。	多様化設備である共通要因故障対策設備を用いて原子炉停止系統、工学的安全施設等を手動操作する場合に、運転員が必要な時間内に開始できるよう、ソフトウェア CCF 対策として必要なパラメータの監視及び共通要因故障対策設備から作動させた原子炉停止系統及び工学的安全施設等の機器の状態の監視が可能な設計とするとともに、ソフトウェア CCF 時に必要な原子炉停止系統及び工学的安全施設等の手動操作ができる設計とする。また、 共通要因故障対策設備が自動作動したことを、吹鳴装置を設け表示灯点灯と共に吹鳴音にて告知する設計とする。	○	多様化設備である共通要因故障対策設備の自動作動機能が動作すると、中央制御室に「多様化自動作動設備作動」警報が発信する。これにより、デジタル安全保護回路がソフトウェア CCF によりすべて機能喪失し、かつ運転時の異常な過渡変化又は設計基準事故が発生したことを検知できる。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(39/56)

（判定記号）○：整合有　－：該当なし

表1 「3. 多様化設備要件」に関する要件整合性確認表(3/8)

ATENA 技術要件書	ソフトウェア CCF 対策設備設計図書の要件整合性			
	記載内容（概要）	要件整合性		設計図書
要求内容		判定	理由	
3.3 多様化設備の範囲				
多様化設備の範囲は、3.2 機能要求を達成するために必要となる、検出器、操作スイッチ、論理回路、指示計・警報等の計測制御設備とする。 この計測制御設備の構成要素は、3.5 多様化設備への要求事項を満足する限り、デジタル安全保護回路のソフトウェア CCF 影響緩和対策として設けた設備以外の設備（安全保護回路の検出器及び操作スイッチ、重大事故等対処設備等）も多様化設備として用いることができる。 また、多様化設備の範囲は、安全保護回路のデジタル化の範囲等により異なるため、多様化設備としてどの設備を選定したか設計図書で明確にする。	多様化設備である共通要因故障対策設備の範囲は以下の①～⑦である。 ① 検出器 蒸気発生器水位検出器 加圧器水位検出器 他 （別表4「共通要因故障対策設備が有する指示機能一覧表」参照） ②操作器 手動原子炉トリップ操作器 手動安全注入操作器（高圧注入／低圧注入） 他 （別表2「共通要因故障対策設備が有する手動作動機能一覧表」参照） ③論理回路 多様化自動作動盤 （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 蒸気発生器狭域水位指示 加圧器水位指示 他 （別表4「共通要因故障対策設備が有する指示機能一覧表」参照） ⑤警報 多様化自動作動設備作動警報 加圧器圧力異常低警報 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 安全保護系計器ラック（アナログ回路部）、炉外核計装盤、安全保護系ロジック盤、安全防護系シーケンス盤	○	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。	・多様化設備基本設計方針書 2 章、7.1.1 章、7.1.3 章、7.2.1 章、7.2.2 章、図 7

（判定記号）○：整合有　－：該当なし

表1 「3. 多様化設備要件」に関する要件整合性確認表(4/8)

ATENA 技術要件書	ソフトウェア CCF 対策設備設計図書の要件整合性			
	記載内容(概要)	要件整合性		設計図書
要求内容		判定	理由	
3.4 設計基本方針				
デジタル安全保護回路は、十分に高い信頼度でソフトウェア設計がなされており、ソフトウェア CCF が発生する可能性は極めて小さく抑えられているため、多様化設備は、運転時の異常な過渡変化又は設計基準事故が発生し、かつソフトウェア CCF により安全機能が喪失するという設計基準を超える事象に対応する設備であることから、多様化設備に対しては、設計上、単一故障を考慮しない。 多様化設備は、設計上、火災・溢水あるいは外的影響(地震を除く)とソフトウェア CCF との重畳を考慮しない。 多様化設備は、ソフトウェア CCF 発生時に安全保護回路の代替機能を有する設備であることから、耐環境性、耐震性、供給電源等は、安全保護回路と同等の条件で機能を発揮できる設計とする。	－	－	本項は基本方針を述べたものであり、具体的には「3.5 多様化設備への要求事項」で、耐環境性、耐震性、供給電源等について個別に確認した。 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。	－

（判定記号）○：整合有　－：該当なし

表1 「3. 多様化設備要件」に関する要件整合性確認表(5/8)

ATENA 技術要件書	ソフトウェア CCF 対策設備設計図書の要件整合性			
	記載内容(概要)	要件整合性		設計図書
要求内容		判定	理由	
3.5 多様化設備への要求事項				
3.5.1 多重性				
多様化設備には、多重性は要求しない。	多様化設備である共通要因故障対策設備自体には多重性は不要である。	○	多様化設備である共通要因故障対策設備は、設計想定外の設備であるため、作動機能の維持について構成機器もしくはチャンネルに単一故障もしくは試験または保守のための使用状態からの取り外しを想定する必要はない設計方針としていることを設計図書により確認した。	・デジタル安全保護系共通要因故障対策基本方針書　3.2 章(39/56) ・多様化設備基本設計方針書　5.3.1 章
3.5.2 多様性				
多様化設備自体には、多様性は要求しない。	多様化設備である共通要因故障対策設備自体には多様性は不要である。	○	多様化設備である共通要因故障対策設備自体には多様性不要とする設計方針としていることを設計図書により確認した。	・デジタル安全保護系共通要因故障対策基本方針書　3.2 章(40/56) ・多様化設備基本設計方針書　5.3.2 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(40/56) ・多様化設備基本設計方針書　5.3.2 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。	・多様化設備基本設計方針書　5.3.2 章
3.5.3 耐環境性				
多様化設備は、4. 有効性評価で対象とする運転時の異常な過渡変化又は設計基準事故とソフトウェア CCF が重畳する状態で想定される環境条件において、その機能を発揮できる設計とすること。	多様化設備である共通要因故障対策設備は、「運転時の異常な過渡変化」又は「設計基準事故」とソフトウェア CCF が重畳する状態で想定される環境条件において、その機能を発揮できる設計とする。	○	多様化設備である共通要因故障対策設備は、設置場所における「運転時の異常な過渡変化」又は「設計基準事故」とソフトウェア CCF が重畳する環境下で所定の機能が果たせる設計としていることを設計図書により確認した。	・デジタル安全保護系共通要因故障対策基本方針書　3.2 章(40/56) ・多様化設備基本設計方針書　5.6 章

（判定記号）○：整合有　－：該当なし

表1 「3. 多様化設備要件」に関する要件整合性確認表(6/8)

ATENA 技術要件書	ソフトウェア CCF 対策設備設計図書の要件整合性			
	記載内容(概要)	要件整合性		設計図書
要求内容		判定	理由	
3.5.4 耐震性				
多様化設備は、基準地震動 Ss による地震力に対し、機能維持する設計とすること。	多様化設備である共通要因故障対策設備は、基準地震動 Ss による地震力に対し、機能維持する設計とする。	○	多様化設備である共通要因故障対策設備は、基準地震動 Ss による地震力に対し機能維持するものとしている。多様化設備のうち設計基準対象施設と兼用しておらず、個別の耐震評価が必要な多様化自動作動盤については、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(耐震解析計算書)により確認した。	・デジタル安全保護系共通要因故障対策基本方針書 3.2 章(40/56) ・多様化設備基本設計方針書 5.5 章 ・多様化自動作動盤(DAAC 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、非常用直流母線に接続される計装用電源装置(インバータ)から給電される設計としていることを設計図書により確認した。	・デジタル安全保護系共通要因故障対策基本方針書 3.2 章(40/56) ・多様化設備基本設計方針書 5.10 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(40/56)
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(40/56) ・多様化設備基本設計方針書 5.3.4 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(40/56) ・多様化設備基本設計方針書 5.3.3 章 ・安全保護系ブロック図 ・安全防護系シーケンス盤装置ロジック図

（判定記号）○：整合有　－：該当なし

表1 「3. 多様化設備要件」に関する要件整合性確認表(7/8)

ATENA 技術要件書	ソフトウェア CCF 対策設備設計図書の要件整合性			
	記載内容(概要)	要件整合性		設計図書
要求内容		判定	理由	
3.5.9 火災防護及び溢水防護				
多様化設備が、火災・溢水の影響を受けたとしても、安全保護回路の安全機能を喪失させない設計とすること。	多様化設備である共通要因故障対策設備は、火災・溢水の影響を受けたとしても、安全保護系の安全機能が喪失しない設計とする。	○	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(40/56) ・多様化設備基本設計方針書　5.8 章
3.5.10 外的事象に対する防護				
多様化設備は、想定される自然現象（地震を除く）、人為による事象、蒸気タービン、ポンプ、その他の機器又は配管の損壊に伴う飛散物等に対して、多様化設備がそれらの影響を受けない設計とすること又は多様化設備がそれらの影響を受けたとしても、安全保護回路の安全機能を喪失させない設計とすること。	多様化設備である共通要因故障対策設備は、想定される自然現象（地震を除く）、人為による事象及び蒸気タービン、ポンプ、その他の機器又は配管の損壊に伴う飛散物等に対して、共通要因故障対策設備が影響を受けない設計とする、又は、共通要因故障対策設備が影響を受けても安全機能が喪失しない設計とする。	○	発電所で考慮する自然現象及び外部人為事象等に対して、共通要因故障対策設備の受ける影響評価を行った結果、これらの事象に対して多様化設備である共通要因故障対策設備が影響を受けない、または影響を受けたとしても、安全保護系の機能を喪失しないことを確認した。 各事象に対する共通要因故障対策設備への影響評価を別表5「共通要因故障対策設備の自然現象、外部人為事象等に対する影響評価整理表」に示す。	・デジタル安全保護系共通要因故障対策基本方針書　3.2 章(40/56)
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(40/56) ・多様化設備基本設計方針書　5.9 章、7.2.1 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(19/56) ・多様化設備基本設計方針書　5.9 章

（判定記号）○：整合有　－：該当なし

表1 「3. 多様化設備要件」に関する要件整合性確認表(8/ 8)

ATENA 技術要件書	ソフトウェア CCF 対策設備設計図書の要件整合性			
	記載内容(概要)	要件整合性		設計図書
要求内容		判定	理由	
3.5.12 監視性				
多様化設備には、運転時の異常な過渡変化又は設計基準事故とソフトウェア CCF が重畳した事象の発生を認知できる警報、事象の判定及び対応操作の判断に必要な監視設備を原子炉制御室に設置すること。	多様化設備である共通要因故障対策設備のうち、事象発生の認知や、事象の判定及び対応操作の判断に必要な警報機能や監視機能は、中央制御室に設置する。	○	運転時の異常な過渡変化又は設計基準事故とソフトウェア CCF が重畳した事象を認知できる警報として、3.2 項、3.3 項及び別表3「共通要因故障対策設備が有する警報機能一覧表」で示した多様化自動作動設備作動警報を中央制御室に告知する設計としていることを設計図書により確認した。 事象の判定及び対応操作に必要な監視設備として、3.2 項、3.3 項及び別表4「共通要因故障対策設備が有する指示機能一覧表」で示した指示計を中央制御室に設置する設計としていることを設計図書により確認した。	・デジタル安全保護系共通要因故障対策基本方針書 3.2 章(40/56) ・多様化設備基本設計方針書 5.9 章、7.1.3 章、7.2.2 章
また、多様化設備が自動で作動した場合には、その作動要因が原子炉制御室に表示される設計とすること。	多様化設備である共通要因故障対策設備の論理回路(多様化自動作動盤)が自動作動した場合には、中央制御室に警報が表示される設計とする。	○	多様化自動作動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。	・多様化設備基本設計方針書 7.1.3 章

（判定記号）○：整合有　－：該当なし

表 2「4. 有効性評価」に関する要件整合性確認表(1/ 13)

ATENA 技術要件書	ソフトウェア CCF 対策有効性評価図書の要件整合性			
	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	
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	○	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）

（判定記号）○：整合有　－：該当なし

表 2「4. 有効性評価」に関する要件整合性確認表(2/ 13)

ATENA 技術要件書	ソフトウェア CCF 対策有効性評価図書の要件整合性			
	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	
	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			4.6.3 被ばく評価への影響 (P.228～P.233)

（判定記号）○：整合有　－：該当なし

表 2「4. 有効性評価」に関する要件整合性確認表(3/ 13)

ATENA 技術要件書	ソフトウェア CCF 対策有効性評価図書の要件整合性			
	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	
	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。			
・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）

（判定記号）○：整合有　－：該当なし

表 2 「4. 有効性評価」に関する要件整合性確認表(4/ 13)

ATENA 技術要件書	ソフトウェア CCF 対策有効性評価図書の要件整合性			
	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	
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)

（判定記号）○：整合有　－：該当なし

表 2 「4. 有効性評価」に関する要件整合性確認表(5/ 13)

ATENA 技術要件書	ソフトウェア CCF 対策有効性評価図書の要件整合性			
	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	
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)

（判定記号）○：整合有　－：該当なし

表 2 「4. 有効性評価」に関する要件整合性確認表(6/ 13)

ATENA 技術要件書	ソフトウェア CCF 対策有効性評価図書の要件整合性			
	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	
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)

（判定記号）○：整合有　－：該当なし

表 2 「4. 有効性評価」に関する要件整合性確認表(7/ 13)

ATENA 技術要件書	ソフトウェア CCF 対策有効性評価図書の要件整合性			
	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	
4.4.2 解析で想定する現実的な条件等				
事象発生前のプラント初期条件は、設計値等に基づく現実的な値を用いること。その場合には、安全設計の妥当性確認に用いる安全解析における解析条件との差異及び根拠を明確にすること。	プラント初期条件及び設定根拠を、解析条件として示している。また、添付書類十解析と異なる条件を用いたものは、差異及び根拠を示している。	○	プラント初期条件及び設定根拠が示されている。	4.3 基本解析条件(P.14) 4.4 運転時の異常な過渡変化(各主要解析条件表) 4.5 設計基準事故(各主要解析条件表) 添付 1-1、添付 1-2
事象発生によって生じる外乱の程度、炉心状態(出力分布、反応度係数等)、機器の容量等は、設計値等に基づく現実的な値を用いること。その場合には、安全設計の妥当性確認に用いる安全解析における解析条件との差異及び根拠を明確にすること。	事象発生による外乱の程度、炉心状態、機器容量等の解析条件及び設定根拠を示している。また、添付書類十解析と異なる条件を用いたものは、差異及び根拠を示している。	○	解析条件及び根拠が示されている。	4.3 基本解析条件(P.14) 4.4 運転時の異常な過渡変化(各主要解析条件表) 4.5 設計基準事故(各主要解析条件表) 添付 1-1、添付 1-2
作動設定点等については計装上の誤差は考慮しなくともよい。	―	―	技術要件書の緩和既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)

（判定記号）○：整合有　－：該当なし

表 2 「4. 有効性評価」に関する要件整合性確認表(8/ 13)

ATENA 技術要件書	ソフトウェア CCF 対策有効性評価図書の要件整合性			
	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	
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、誤操作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。	○	ソフトウェア CCF による機能喪失を解析条件に反映している。	4.3 基本解析条件(P.14) 4.4 運転時の異常な過渡変化(各主要解析条件表) 4.5 設計基準事故(各主要解析条件表)
デジタル安全保護回路を経由しない、自動起動信号又は運転員が事象の発生を認知した場合の手動起動信号により、原子炉停止系統及び工学的安全施設は作動可能とする。	「原子炉格納容器健全性評価」において、デジタル安全保護回路の機能喪失に伴い自動起動しない格納容器スプレイ設備について、手動起動操作を解析条件としている。	○	ソフトウェア CCF による機能喪失への対応操作として、手動起動を解析条件として反映している。	4.3 基本解析条件(P.14) 4.5.8 原子炉格納容器健全性評価(P.196) 添付 1-3 運転員操作条件

（判定記号）○：整合有　－：該当なし

表 2 「4. 有効性評価」に関する要件整合性確認表(9/ 13)

ATENA 技術要件書	ソフトウェア CCF 対策有効性評価図書の要件整合性			
	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	
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)

（判定記号）○：整合有　－：該当なし

表 2 「4. 有効性評価」に関する要件整合性確認表(10/ 13)

ATENA 技術要件書	ソフトウェア CCF 対策有効性評価図書の要件整合性			
	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	
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)

（判定記号）○：整合有　－：該当なし

表 2 「4. 有効性評価」に関する要件整合性確認表(11/ 13)

ATENA 技術要件書	ソフトウェア CCF 対策有効性評価図書の要件整合性			
	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	
・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

（判定記号）○：整合有　－：該当なし

表 2 「4. 有効性評価」に関する要件整合性確認表(12/ 13)

ATENA 技術要件書	ソフトウェア CCF 対策有効性評価図書の要件整合性			
	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	
・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

（判定記号）○：整合有　－：該当なし

表 2 「4. 有効性評価」に関する要件整合性確認表(13/ 13)

ATENA 技術要件書	ソフトウェア CCF 対策有効性評価図書の要件整合性			
	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	
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)

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

1. 原子炉非常停止信号

原子炉非常停止信号の種類	検出器及び作動条件						原子炉非常停止信号を発信させない条件	備考
	検出器の種類	個数	取付箇所		原子炉非常停止に要する信号の個数	設定値		
蒸気発生器水位低（CCF）	蒸気発生器A水位検出器（Ch.Ⅰ）	1	系統名（ライン名）	蒸気発生器A	2	計器スパンの7％以上、かつ、11%以下	正常に原子炉トリップした場合には、共通要因故障対策設備からの作動信号をブロックする。	各検出器は設計基準対象施設と共用 設定値根拠は添付2参照
			設置床	原子炉格納容器EL.24.0m				
	蒸気発生器B水位検出器（Ch.Ⅱ）	1	系統名（ライン名）	蒸気発生器B				
			設置床	原子炉格納容器EL.24.0m				
	蒸気発生器C水位検出器（Ch.Ⅱ）	1	系統名（ライン名）	蒸気発生器C				
			設置床	原子炉格納容器EL.24.0m				

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

原子炉非常停止信号の種類	検出器及び作動条件						原子炉非常停止信号を発信させない条件	備考
	検出器の種類	個数	取付箇所		原子炉非常停止に要する信号の個数	設定値		
加圧器圧力低（CCF）	加圧器圧力検出器（Ch.Ⅰ）	1	系統名（ライン名）	加圧器	2	12.42MPa以上、かつ、12.72MPa以下	正常に原子炉トリップした場合には、共通要因故障対策設備からの作動信号をブロックする。	各検出器は設計基準対象施設と共用 設定値根拠は添付2参照
			設置床	原子炉格納容器 EL.24.0m				
	加圧器圧力検出器（Ch.Ⅱ）	1	系統名（ライン名）	加圧器				
			設置床	原子炉格納容器 EL.24.0m				
加圧器圧力高（CCF）	加圧器圧力検出器（Ch.Ⅰ）	1	系統名（ライン名）	加圧器	2	16.60MPa以上、かつ、16.90MPa以下	正常に原子炉トリップした場合には、共通要因故障対策設備からの作動信号をブロックする。	各検出器は設計基準対象施設と共用 設定値根拠は添付2参照
			設置床	原子炉格納容器 EL.24.0m				
	加圧器圧力検出器（Ch.Ⅱ）	1	系統名（ライン名）	加圧器				
			設置床	原子炉格納容器 EL.24.0m				

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

2. 工学的安全施設等の作動信号

工学的安全施設等の作動信号の種類		検出器及び作動条件						工学的安全施設等の作動信号を発信させない条件	備考
		検出器の種類	個数	取付箇所		工学的安全施設等の作動に要する信号の個数	設定値		
補助給水ポンプ起動信号	蒸気発生器水位低（CCF）	蒸気発生器A水位検出器（Ch.Ⅰ）	1	系統名（ライン名）	蒸気発生器A	2	計器スパンの7%以上、かつ、11％以下	正常に補助給水ポンプが起動した場合、自動で補助給水ポンプ起動信号が阻止される。	各検出器は設計基準対象施設と共用 設定値根拠は添付2参照
				設置床	原子炉格納容器EL.24.0m				
		蒸気発生器B水位検出器（Ch.Ⅱ）	1	系統名（ライン名）	蒸気発生器B				
				設置床	原子炉格納容器EL.24.0m				
		蒸気発生器C水位検出器（Ch.Ⅱ）	1	系統名（ライン名）	蒸気発生器C				
				設置床	原子炉格納容器EL.24.0m				

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

工学的安全施設等の作動信号の種類	検出器及び作動条件					工学的安全施設等の作動信号を発信させない条件	備考
	検出器の種類	個数	取付箇所	工学的安全施設等の作動に要する信号の個数	設定値		
主蒸気ライン隔離信号	（注1）					正常に原子炉トリップした場合には自動で主蒸気ライン隔離信号が阻止される。	（注1）
主給水隔離信号	（注1）					正常に原子炉トリップした場合には自動で主給水隔離信号が阻止される。	（注1）

（注1）蒸気発生器水位低（CCF）、加圧器圧力低（CCF）及び加圧器圧力高（CCF）による原子炉非常停止信号及び蒸気発生器水位低（CCF）による補助給水ポンプ起動信号と同じ

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

工学的安全施設等の作動信号の種類		検出器及び作動条件						工学的安全施設等の作動信号を発信させない条件	備考
		検出器の種類	個数	取付箇所		工学的安全施設等の作動に要する信号の個数	設定値		
安全注入作動信号	加圧器圧力異常低（CCF）	加圧器圧力検出器（Ch.Ⅰ）	1	系統名（ライン名）	加圧器	2	11.03MPa以上、かつ、11.33MPa以下	正常に安全注入が作動した場合には、共通要因故障対策設備からの作動信号をブロックする。	各検出器は設計基準対象施設と共用 設定値根拠は添付2参照
				設置床	原子炉格納容器 EL.24.0m				
		加圧器圧力検出器（Ch.Ⅱ）	1	系統名（ライン名）	加圧器				
				設置床	原子炉格納容器 EL.24.0m				
余熱除去ポンプAミニマムフロー弁開信号	余熱除去ポンプA出口流量低（CCF）	余熱除去ポンプA出口流量検出器（Ch.Ⅲ）	1	系統名（ライン名）	余熱除去A系統	1	$102m^3/h$以上、かつ$128m^3/h$以下	正常に安全注入が作動した場合には、共通要因故障対策設備からの作動信号をブロックする。	検出器は設計基準対象施設と共用 設定値根拠は添付2参照
				設置床	原子炉補助建屋 EL.-0.5m				
余熱除去ポンプAミニマムフロー弁閉信号	余熱除去ポンプA出口流量高（CCF）	余熱除去ポンプA出口流量検出器（Ch.Ⅲ）	1	系統名（ライン名）	余熱除去A系統	1	$249 m^3/h$以上、かつ$271m^3/h$以下	正常に安全注入が作動した場合には、共通要因故障対策設備からの作動信号をブロックする。	検出器は設計基準対象施設と共用 設定値根拠は添付2参照
				設置床	原子炉補助建屋 EL.-0.5m				

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	取付箇所（設置床）	備考
原子炉トリップ		2	原子炉補助建屋 EL.17.0m （中央制御室）	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	全ループ	2		
	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		2		
補助給水流量調整・隔離		3		
主蒸気逃がし弁		3		
加圧器逃がし弁		2		

別表3　共通要因故障対策設備が有する警報機能一覧表

警報の種類		個数	取付箇所（設置床）	備考
多様化自動作動設備作動		1	原子炉補助建屋 EL.17.0m （中央制御室）	設計基準対象施設の警報設備とは異なる設備として、中央盤（原子炉補助盤）に設置する。
ファーストアウト警報	加圧器圧力低	1		
	加圧器圧力高	1		
	蒸気発生器水位低	1		
蒸気発生器水位異常高		1		
加圧器圧力異常低		1		

別表4 共通要因故障対策設備が有する指示機能一覧表

名称	検出器の種類	計測範囲	個数	検出器取付箇所		備考
中間領域 中性子束 （Ch.Ⅰ）	γ線 補償型 電離箱	10^{-11}～5×10^{-3}A (1.3×10^{2}～6.6×10^{10}cm^{-2}・s^{-1})	1	系統名 （ライン名）	－	各検出器～指示計は設計基準対象施設と共用 指示計の取付箇所は原子炉補助建屋EL.17.0m （中央制御室）
				設置床	原子炉格納容器 EL.17.0m	
1次冷却材圧力 （Ch.Ⅲ）	弾性圧力 検出器	0～21.0MPa	1	系統名 （ライン名）	ループC	
				設置床	原子炉格納容器 EL.17.0m	
1次冷却材 低温側温度 （広域） （Ch.Ⅱ）	測温 抵抗体	0～400℃	3	系統名 （ライン名）	ループA、B、C	
				設置床	原子炉格納容器 EL.17.0m	
加圧器水位 （Ch.Ⅰ）	差圧式 水位検出器	0～100％	1	系統名 （ライン名）	加圧器	
				設置床	原子炉格納容器 EL.17.0m	
主蒸気ライン 圧力 （Ch.Ⅲ）	弾性圧力 検出器	0～8.5MPa	1	系統名 （ライン名）	A 主蒸気ライン	
				設置床	原子炉建屋 EL.24.0m	
主蒸気ライン 圧力 （Ch.Ⅲ）	弾性圧力 検出器	0～8.5MPa	2	系統名 （ライン名）	B、C 主蒸気ライン	
				設置床	原子炉建屋 EL.17.0m	

別表4 共通要因故障対策設備が有する指示機能一覧表

名称	検出器の種類	計測範囲	個数	取付箇所		備考
蒸気発生器 狭域水位 (Ch.Ⅰ)	差圧式 水位検出器	0～100%	1	系統名 (ライン名)	蒸気発生器Ａ	各検出器～指示計は設計基準対象施設と共用 指示計の取付箇所は原子炉補助建屋 EL.17.0m (中央制御室)
				設置床	原子炉格納容器 EL.24.0m	
蒸気発生器 狭域水位 (Ch.Ⅱ)	差圧式 水位検出器	0～100%	2	系統名 (ライン名)	蒸気発生器Ｂ、Ｃ	
				設置床	原子炉格納容器 EL.24.0m	
格納容器内 圧力(広域) (Ch.Ⅳ)	弾性圧力 検出器	0～0.35MPa	1	系統名 (ライン名)	－	
				設置床	原子炉建屋 EL.17.0m	
燃料取替用水 タンク水位 (Ch.Ⅰ)	差圧式水位 検出器	0～100%	1	系統名 (ライン名)	燃料取替用水 タンク	
				設置床	原子炉補助建屋 EL.19.0m	
格納容器再循環 サンプ水位(広域) (Ch.Ⅲ)	差圧式水位 検出器	0～100%	1	系統名 (ライン名)	格納容器再循環 サンプＡ	
				設置床	原子炉格納容器 EL.10.0m	

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

（判定記号）○：影響なし　－：該当なし

設置(変更)許可において想定される自然事象等		(参考)設置許可での想定/対策の概要	各事象に対する共通要因故障対策設備への影響評価	
			結果	理由
想定される自然現象(地震除く)	津波	津波防護対象設備(津波防護施設、浸水防止設備、津波監視設備及び非常用取水設備を除く。)を内包する建屋及び区画の設置された敷地において、基準津波による遡上波を地上部から到達又は流入させない等により安全機能を損なうことのない設計とする。	○	多様化設備である共通要因故障対策設備は、当該事象の影響を受けないことを確認した建屋内に設置していることから、本設備への影響はない。
	風(台風)	風荷重を建築基準法に基づき設定し、それに対し機械的強度を有することにより安全機能を損なうことのない設計とする。	○	
	竜巻	最大風速 100m/s の竜巻が発生した場合においても、竜巻による風圧力による荷重、気圧差による荷重及び飛来物の衝撃荷重を組み合わせた荷重等に対して安全機能を損なわないために、飛来物の発生防止対策及び竜巻防護対策を行う。	○	
	凍結	敷地付近での最低気温を考慮し、屋外機器で凍結のおそれのあるものに保温等の凍結防止対策を必要に応じて行うことにより、安全機能を損なうことのない設計とする。	○	

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

（判定記号）○：影響なし　－：該当なし

設置（変更）許可において想定される自然事象等		（参考）設置許可での想定/対策の概要	各事象に対する共通要因故障対策設備への影響評価	
			結果	理由
想定される自然現象（地震除く）	降水	降水に対して、構内排水路で集水し海域へ排出を行うことにより、安全機能を損なうことのない設計とする。	○	多様化設備である共通要因故障対策設備は、当該事象の影響を受けないことを確認した建屋内に設置していることから、本設備への影響はない。
	積雪	積雪荷重を建築基準法に基づき設定し、それに対し機械的強度を有することにより安全機能を損なうことのない設計とする。	○	
	落雷	雷害防止対策として、原子炉格納施設等への避雷針の設置、接地網の布設による接地抵抗の低減等を行うことにより、安全機能を損なうことのない設計とする。	○	
	地滑り	地滑りが発生するおそれのない位置に設置することにより、安全機能を損なうことのない設計とする。	○	
	火山	降下火砕物による直接的影響及び間接的影響のそれぞれに対し、安全機能を損なわない設計とする。	○	

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

（判定記号）○：影響なし　－：該当なし

設置（変更）許可において想定される自然事象等		（参考）設置許可での想定/対策の概要	各事象に対する共通要因故障対策設備への影響評価	
			結果	理由
想定される自然現象（地震除く）	生物学的影響	生物学的事象として、海生生物であるクラゲ等の発生、小動物の侵入を考慮する。クラゲ等の発生に対しては、塵芥による原子炉補機冷却海水設備等への影響を防止するため除塵装置を設置し、必要に応じて塵芥を除去することにより、安全機能を損なうことのない設計とする。また、小動物の侵入に対しては、屋外設置の端子箱貫通部等へのシールを行うことにより、安全機能を損なうことのない設計とする。	○	多様化設備である共通要因故障対策設備は、当該事象の影響を受けないことを確認した建屋内に設置していることから、本設備への影響はない。
	森林火災	過去 10 年間の気象条件を調査し、発電所から直線距離で 10km の間に発火点を設定し、森林火災シミュレーションを用いて影響評価を実施し、影響評価に基づいた防火帯幅を確保すること等により、安全機能を損なうことのない設計とする。	○	
	高潮	敷地の整地レベルを EL.+10mとすることにより、高潮により安全機能を損なうことのない設計とする。	○	

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

（判定記号）○：影響なし　－：該当なし

設置（変更）許可において想定される自然事象等		（参考）設置許可での想定/対策の概要	各事象に対する共通要因故障対策設備への影響評価	
			結果	理由
外部人為行為	近隣工場等の火災	・発電所敷地外 10km 以内の範囲において、火災により安全施設に影響を及ぼすような石油コンビナート施設はない。 ・発電所敷地内に設置する危険物タンク等の火災発生時の輻射熱による外部火災防護施設の建屋の表面温度等を許容温度以下とすることにより、安全機能を損なうことのない設計とする。 ・発電所敷地内への航空機墜落に伴う火災発生時の輻射熱による外部火災防護施設の建屋の表面温度等を許容温度以下とすることにより、安全機能を損なうことのない設計とする。 ・発電所港湾内に入港する船舶の火災発生時の輻射熱による外部火災防護施設の建屋の表面温度等を許容温度以下とすることにより、安全機能を損なうことのない設計とする。 ・石油コンビナート施設の火災、発電所敷地内に設置する危険物タンク等の火災、航空機墜落による火災及び発電所港湾内に入港する船舶の火災に伴うばい煙等発生時の二次的影響に対して、外気を取り入れる換気空調設備、外気を設備内に取り込む機器及び室内の空気を取り込む機器に分類し、影響評価を行い、必要な場合は対策を実施することで、安全機能を損なうことのない設計とする。	○	多様化設備である共通要因故障対策設備は、当該事象の影響を受けないことを確認した建屋内に設置していることから、本設備への影響はない。

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

（判定記号）○：影響なし　－：該当なし

設置(変更)許可において想定される自然事象等		(参考)設置許可での想定/対策の概要	各事象に対する共通要因故障対策設備への影響評価	
			結果	理由
外部人為行為	有毒ガス	外部火災により発生する有毒ガスの影響については、適切な防護対策を講じることにより、安全機能を損なうことのない設計とする。有毒ガス発生時、居住性の確保が必要な場所については、外気取入ダンパの閉止又は閉回路循環運転により、建屋内への有毒ガスの侵入を阻止することで、安全機能を損なうことのない設計とする。幹線道路、鉄道路線、一般航路及び石油コンビナート施設は、発電所から離れており、有毒ガスを考慮する必要はない。	○	多様化設備である共通要因故障対策設備は、当該事象の影響を受けないことを確認した建屋内に設置していることから、本設備への影響はない。
	船舶の衝突	海上交通としては、一般航路が発電所沖合約 13km、阪神－九州間の定期航路が発電所沖合約 18km にあり、発電所から離れている。また、小型船舶が発電所近傍で漂流した場合でも、敷地前面の護岸等に衝突して止まることから取水性に影響はない。仮に海水取水口に向かったとしても、海水取水口の呑口高さが十分低いことから、浮遊する小型船舶が海水取水口呑口に到達する可能性は低く、通水機能が損なわれるような閉塞は生じない。	○	

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

（判定記号）○：影響なし　－：該当なし

設置(変更)許可において想定される自然事象等		(参考)設置許可での想定/対策の概要	各事象に対する共通要因故障対策設備への影響評価	
			結果	理由
外部人為行為	電磁的障害	安全機能を有する原子炉保護設備は、発電用原子炉施設で発生する電磁干渉や無線電波干渉等により機能が喪失しないよう、計測制御回路を構成する安全保護系計器ラック及びケーブルは、ラインフィルタや絶縁回路の設置により、サージ・ノイズの侵入を防止するとともに、鋼製筐体や金属シールド付ケーブルの適用により電磁波の侵入を防止する設計としているため、電磁的障害により安全機能を損なうことはない。	○	多様化設備である共通要因故障対策設備は、ラインフィルタや絶縁回路の設置により、サージ・ノイズの侵入を防止するとともに、鋼製筐体等の適用により電磁波の侵入を防止する設計としている。
その他	タービン等の飛来物	蒸気タービン等の損壊に伴う飛散物により安全性を損なわない設計とする。蒸気タービン及び発電機は、破損防止対策を行うことにより、破損事故の発生確率を低くするとともに、ミサイルの発生を仮に想定しても安全機能を有する構築物、系統及び機器への到達確率を低くすることによって、発電用原子炉施設の安全性を損なわない設計とする。	○	回転機器側で飛散物の発生防止等を行う設計であり、問題ない。

自然事象のうち洪水に関しては、発電所の施設への影響がないことから、影響を及ぼす事象から除外している。

外部人為事象のうちダムの崩壊、爆発に関しては、発電所の施設への影響がないことから、影響を及ぼす事象から除外している。

航空機落下については、航空機落下確率評価を行った結果、防護設計の要否判断の基準を超えないため、航空機落下による防護設計を考慮しないこととしている。

以上

Ⅱ．添付書類

目 次

添付1　「3. 多様化設備要件」における設計図書

添付１－１　デジタル安全保護系共通要因故障対策基本方針書

本資料は、機密に係る情報のため公開できません

添付１－２　多様化設備基本設計方針書

本資料は、機密に係る情報のため公開できません

添付１－３　原子炉制御保護系ファンクショナルダイヤグラム

本資料は、機密に係る情報のため公開できません

添付１－４　補機インターロック線図

本資料は、機密に係る情報のため公開できません

添付１－５　多様化自動作動盤（DAAC 盤）
耐震解析計算書

本資料は、機密に係る情報のため公開できません

添付１－６　安全保護系ブロック図

本資料は、機密に係る情報のため公開できません

添付１－７　安全防護系シーケンス盤　装置ロジック図

本資料は、機密に係る情報のため公開できません

添付１－８　所内単線結線図

本資料は、機密に係る情報のため公開できません

添付１－９　計装用電源単線結線図

本資料は、機密に係る情報のため公開できません

添付2　共通要因故障対策設備の設定値根拠に関する説明書

本資料は、機密に係る情報のため公開できません

添付3 「4. 有効性評価」における有効性評価図書

三菱ＰＷＲ　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有効性評価について

令和４年６月

三菱重工業株式会社

目　　次

略 語 表

ＡＴＥＮＡ	Atomic Energy Association	原子力エネルギー協議会
ＡＴＷＳ	Anticipated Transient Without Scram	原子炉停止機能喪失
ＣＣＦ	Common Cause Failure	共通要因故障
ＣＤ	Discharge Coefficient	流出係数
ＣＶ	Containment Vessel	原子炉格納容器
ＤＮＢＲ	Departure from Nucleate Boiling Ratio	限界熱流束比
ＥＣＣＳ	Emergency Core Cooling System	非常用炉心冷却設備
ＦＰ	Fission Product	核分裂生成物
ＬＯＣＡ	Loss of Coolant Accident	原子炉冷却材喪失事故
ＰＣＭＩ	Pellet-Cladding Mechanical Interaction	ペレットー被覆管機械的相互作用
ＰＣＴ	Peak Cladding Temperature	燃料被覆管最高温度
ＰＷＲ	Pressurized Water Reactor	加圧水型軽水炉
ＲＣＰ	Reactor Coolant Pump	１次冷却材ポンプ
ＲＩＥ	Reactivity Insertion Event	反応度投入事象
ＲＶ	Reactor Vessel	原子炉容器
ＳＧ	Steam Generator	蒸気発生器
ＳＩ	Safety Injection	安全注入

１．まえがき

我国の加圧水型原子力発電プラントにおいては、設備の信頼性及び保守性の向上を目的として 1980 年代頃から常用系設備にデジタル計算機を適用してきており、その良好な運転実績を踏まえ、1990 年代頃からは安全保護回路にもデジタル計算機を適用する事例が増えてきている。デジタル計算機では、設計上の要求機能がソフトウェアによって実現されることから、安全保護回路に適用するソフトウェアの信頼性を確保する取り組みとして、ソフトウェアライフサイクル及び構成管理手法を含めた品質保証活動・検証及び妥当性確認を実施してきた。これらの活動により、ソフトウェアに起因する共通要因故障（以下、「ソフトウェア CCF」と称す。）が発生し、多重化されたデジタル安全保護回路の機能が喪失する可能性は十分低く抑えられている。しかしながら、デジタル安全保護回路を設置した原子力発電事業者（以下、「事業者」と称す。）は、深層防護の観点でより一層の信頼性向上を図るため、デジタル安全保護回路のソフトウェアを介さずに原子炉停止系統や工学的安全施設を作動できる多様化設備（CCF 対策設備）を自主的に設置してきた。

このような状況の中、令和元年度 第 33 回原子力規制委員会（2019 年 10 月 2 日）において、「発電用原子炉施設におけるデジタル安全保護系の共通原因故障対策等に関する検討チーム」（以下、「NRA 検討チーム」と称す。）が設置され、ソフトウェア CCF 対策の規制化に関する議論が進められた。本 NRA 検討チームにおいて、原子力エネルギー協議会（以下、「ATENA」と称す。）と、原子力規制委員会及び原子力規制庁との議論が重ねられた結果、ATENA は NRA 検討チームにおける議論及び国際水準を踏まえ、炉心の著しい損傷防止を重視し、「運転時の異常な過渡変化」または「設計基準事故」とソフトウェア CCF が重畳する可能性は極めて低いものの、ソフトウェア CCF 影響緩和対策としてさらなる対策を自主的かつ計画的に行うことを ATENA ステアリング会議（2020 年 1 月）で決定し、各事業者に対し対策の実施を要求した。

本文献は、上記要求を受けてさらなる自主対策を検討したとともに、それら対策（多様化設備等）により、想定した事象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、適切に対処可能であることを解析等により示すことを目的とする。

なお、本文献の記載内容は、三菱重工業（株）が受託した PWR５電力（関西電力（株）、北海道電力（株）、四国電力（株）、九州電力（株）、日本原子力発電（株））の共同委託の成果に基づく。

2．デジタル安全保護回路のソフトウェア CCF 対策について[(1)]

2.1　ソフトウェア CCF について

ソフトウェア CCF とは、ソフトウェアの不具合に起因して、多重化されたデジタル安全保護回路が同時に故障（機能喪失）する状態をいう。

2.1.1　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。ソフトウェア CCF を想定する範囲の例を図 2.1-1 に示す。

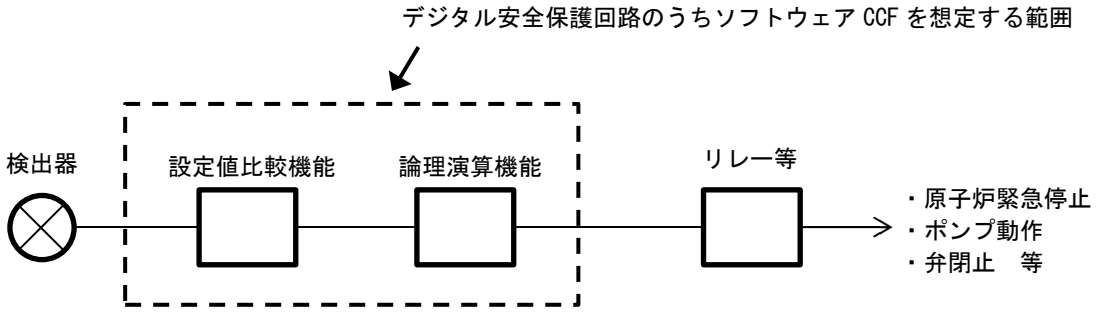


図 2.1-1　安全保護回路のうちソフトウェア CCF を想定する範囲（例）

2.1.2　ソフトウェア CCF 発生時の安全保護回路故障モード想定

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」または「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、工学的安全施設等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。

なお、ソフトウェア CCF の発生により安全保護機能が喪失する場合においても、それ以前に安全保護回路の信号により起動し運転中のポンプ等の機器については、ソフトウェア CCF の影響を受けないものとして機器の作動状態の変化は想定しない。

ここで、ソフトウェア CCF により安全保護機能が誤作動する故障モードについては、機器の誤作動に伴うプラント状態の変化により運転員が認知または多様化設備の作動が要求される状態となること、加えて、原子炉停止系統や工学的安全施設等

の誤作動は「運転時の異常な過渡変化」または「設計基準事故」に包絡されることから、有効性評価では安全保護機能が喪失する状態を想定する。

2.2 ソフトウェア CCF 対策について

2.2.1 設置要求

デジタル安全保護回路を設ける場合には、ソフトウェア CCF 対策として、代替作動機能を有する多様化設備を設置することが、ATENA が策定したソフトウェア CCF 対策に係る技術要件書[(1)]（以下、「ATENA ガイド」と称す。）により要求されている。

ただし、ソフトウェア CCF が発生するおそれがない場合もしくは「運転時の異常な過渡変化」または「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（後述）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とされている。

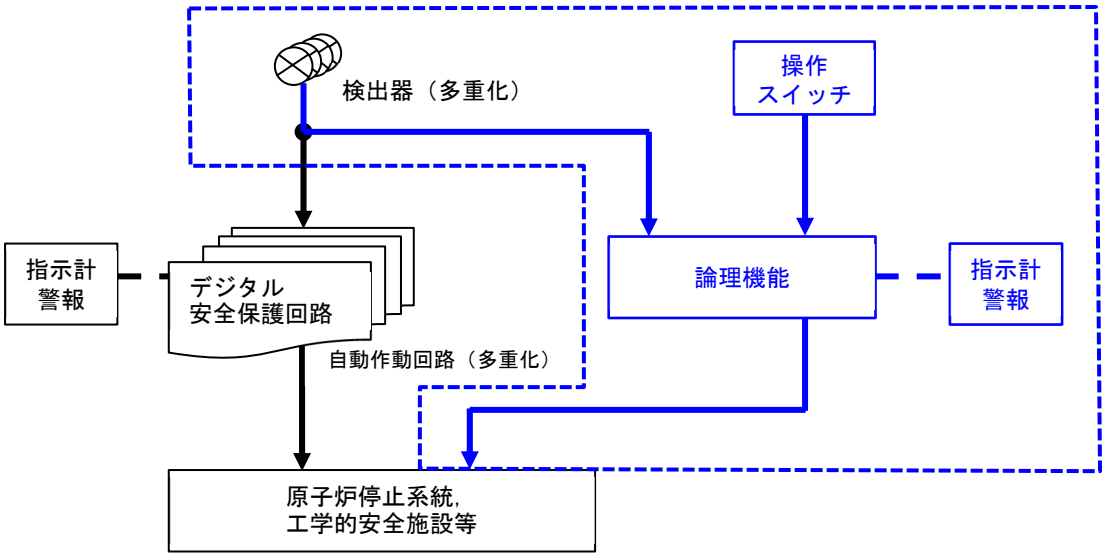
2.2.2 機能要求

多様化設備は、「運転時の異常な過渡変化」または「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または手動で作動させることができることとする。

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」または「設計基準事故」時に安全保護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ることとする。

2.2.3 多様化設備の範囲

多様化設備の範囲は、「2.2.2 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（図 2.2-1）。



（青点線は多様化設備の範囲の例を示す）

図 2.2-1　多様化設備の範囲

2.2.4　ソフトウェア CCF の影響評価と追加対策

「１．まえがき」にて述べたとおり、国内 PWR 事業者は、深層防護の観点でより一層の信頼性向上を図るため、デジタル安全保護回路のソフトウェアを介さずに原子炉停止系統や工学的安全施設を作動できる多様化設備を自主的に設置してきた。今般、ソフトウェア CCF に関する ATENA ガイドの発行を受け、設置変更許可申請書添付書類十で取り扱う「運転時の異常な過渡変化」及び「設計基準事故」の全事象に対し、ソフトウェア CCF の発生により安全保護機能が喪失する場合の影響を評価し、必要な追加対策を抽出した。

2.2.4.1　運転時の異常な過渡変化

現行措置の多様化設備は原子炉トリップ機能を備えているため、「運転時の異常な過渡変化」発生時にデジタル安全保護回路のソフトウェア CCF により原子炉トリップ機能が喪失する場合でも、原子炉トリップ可能である。

仮に、「運転時の異常な過渡変化」において原子炉トリップ機能が喪失すると、「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)」のシーケンスとなる。同評価において、原子炉冷却材圧力バウンダリの健全性確保の観点で厳しくなる「主給水流量喪失時に原子炉トリップ機能が喪失する事故」及び

「負荷の喪失時に原子炉トリップ機能が喪失する事故」を重要事故シーケンスとして選定し、原子炉トリップ機能が喪失する場合でも、ATWS 緩和設備（主蒸気隔離、補助給水）によって原子炉圧力バウンダリ及び燃料損傷の観点で問題なく、設計基準事故の判断基準を概ね満足していることを解析により確認している。したがって、「運転時の異常な過渡変化」発生時にソフトウェア CCF により原子炉トリップ機能が喪失する場合でも、現行措置の多様化設備により原子炉トリップするため、上述の ATWS のシーケンスよりも緩和されることから問題ない。

以上より、「運転時の異常な過渡変化」に対しては現行措置の多様化設備で対応可能であり、多様化設備の追設は不要である。

2.2.4.2　設計基準事故

評価結果を表 2.2-1 に示す。評価の結果、大中破断 LOCA 対策として以下の機能を追加設置することにより、現行措置と合わせ全ての設計基準事故に対応可能である。

・自動機能：高圧／低圧注入系（1 系列）の自動起動［追加措置］
・警報機能：原子炉圧力（異常）低［追加措置］

なお、本自動機能の追加措置にあわせて、現行措置の手動機能（高圧注入系（1 系列）の手動起動）に加えて以下の手動機能を設置する。

・手動機能：低圧注入系（1 系列）の手動起動

多様化設備の現行措置及び追加措置を整理して表 2.2-2 に示す。

表 2.2-1 ソフトウェア CCF の影響評価と追加対策（設計基準事故）

事象名	影響評価結果
原子炉冷却材喪失	・現行措置の手動による高圧注入では、炉心冷却不足のため大中破断 LOCA において判断基準を満足できず。 ・多様化設備（追設）として高圧／低圧注入系（1 系列）を自動作動させることにより、判断基準を概ね満足。 ・CV 健全性に関しては、現場で CV スプレイを手動作動（事故後 30 分以降）させることにより、判断基準を概ね満足。
原子炉冷却材流量の喪失	現行措置の多様化設備による原子炉トリップ、及び現実的な反応度帰還効果により、判断基準を概ね満足。
原子炉冷却材ポンプの軸固着	同上
主給水管破断	同上
主蒸気管破断	現行措置の多様化設備による主蒸気隔離、及び現実的な制御棒状態の想定により、判断基準を概ね満足。
制御棒飛び出し	現行措置の多様化設備による原子炉トリップ、及び現実的な事故想定により、判断基準を概ね満足。
蒸気発生器伝熱管破損	現行措置の多様化設備による原子炉トリップ、及び漏えい停止までの必要な手動操作を多様化設備等で対応することにより、漏えい量は添付書類十解析と同等となり、判断基準を概ね満足。

表 2.2-2 デジタル安全保護回路のソフトウェア CCF に対する多様化設備

項　目	機　能
自動機能	・原子炉トリップ （原子炉(加圧器)圧力低、原子炉(加圧器) 圧力高、蒸気発生器水位低） ・タービントリップ ・主給水隔離 ・主蒸気隔離 ・補助給水起動 ・高圧／低圧注入系起動　（原子炉(加圧器)圧力(異常)低）※
手動機能	・原子炉トリップ ・タービントリップ ・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※ ・原子炉格納容器隔離
警報機能	・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 ・原子炉(加圧器)圧力(異常)低（高圧／低圧注入系作動）
監視機能	・中間領域中性子束 ・加圧器圧力 ・１次冷却材圧力 ・１次冷却材低温側温度（広域） ・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 ・蒸気発生器２次側放射線 ・対象補機の状態

□：追加措置

※本自動機能の追加措置にあわせて、現行措置の手動機能（高圧注入系の手動起動）に加えて低圧注入系の手動起動を設置する。

３．ソフトウェア CCF 対策の有効性評価事象の選定について

3.1　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」または「設計基準事故」と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、デジタル安全保護回路の代替設備となる多様化設備が有効であることを確認するものであり、具体的には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。

3.2　事象選定の基本的考え

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、以下に挙げる「運転時の異常な過渡変化」及び「設計基準事故」の全事象を有効性評価の対象とする。

運転時の異常な過渡変化	設計基準事故
炉心内の反応度又は出力分布の異常な変化 ・原子炉起動時における制御棒の異常な引き抜き ・出力運転中の制御棒の異常な引き抜き ・制御棒の落下及び不整合 ・原子炉冷却材中のほう素の異常な希釈 炉心内の熱発生又は熱除去の異常な変化 ・原子炉冷却材流量の部分喪失 ・原子炉冷却材系の停止ループの誤起動 ・外部電源喪失 ・主給水流量喪失 ・蒸気負荷の異常な増加 ・２次冷却系の異常な減圧 ・蒸気発生器への過剰給水 原子炉冷却材圧力又は原子炉冷却材保有量の異常な変化 ・負荷の喪失 ・原子炉冷却材系の異常な減圧 ・出力運転中の非常用炉心冷却系の誤起動	原子炉冷却材の喪失又は炉心冷却状態の著しい変化 ・原子炉冷却材喪失 ・原子炉冷却材流量の喪失 ・原子炉冷却材ポンプの軸固着 ・主給水管破断 ・主蒸気管破断 反応度の異常な投入又は原子炉出力の急激な変化 ・制御棒飛び出し 環境への放射性物質の異常な放出 ・放射性気体廃棄物処理施設の破損 ・蒸気発生器伝熱管破損 ・燃料集合体の落下 ・原子炉冷却材喪失 ・制御棒飛び出し 原子炉格納容器内圧力、雰囲気等の異常な変化 ・原子炉冷却材喪失 ・可燃性ガスの発生

ただし、評価に際しては、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。さらに、判断基準に照らし合わせて影響の程度が軽微である事象、グルーピングしたグループ内の代表事象に包絡されることが定性的に評価できる事象、及びデジタル安全保護回路の動作を期待しない事象については解析を省略することができる。なお、本有効性評価において事象のグルーピングは実施しない。解析を省略する事象については、3.3 節にて述べる。

3.3 有効性評価事象

3.3.1 運転時の異常な過渡変化

「運転時の異常な過渡変化」については、2.2.4.1 にて述べたとおり、「重大事故等対策の有効性評価」として「原子炉停止機能喪失（ATWS)」の重要事故シーケンスの解析を実施し、原子炉トリップ機能が喪失する場合でも現行の ATWS 緩和設備によって原子炉圧力バウンダリ及び燃料損傷の観点で問題ないことを確認している。「運転時の異常な過渡変化」にソフトウェア CCF が重畳した場合、多様化設備の作動により原子炉トリップに至るため、ATWS の有効性評価よりも事象進展が緩和される。したがって、「運転時の異常な過渡変化」にソフトウェア CCF の重畳を考慮した事象は、判断基準に照らし合わせて影響の程度が軽微であり、解析を省略できると整理される。その上で、多様化設備による CCF 対策の有効性を確認し、判断基準に照らし合わせて影響の程度が軽微であることを示す観点から、ATWS の重要事故シーケンスの１つであり、より多くの多様化設備の機能に期待する「主給水流量喪失」を代表として有効性評価を実施する。

＜選定事象＞

(1)炉心内の熱発生又は熱除去の異常な変化

・主給水流量喪失

3.3.2 設計基準事故

「設計基準事故」については、以下の理由により、全事象を対象として有効性評価を実施する。

・多様化設備による原子炉トリップ及び ECCS の作動信号が限定的であり、かつ作

動のタイミングが本設より遅れるため、事象進展が厳しくなる。

・「運転時の異常な過渡変化」における ATWS のように、包絡させることができる既往の解析がない。

＜選定事象＞

(1)原子炉冷却材の喪失又は炉心冷却状態の著しい変化

・原子炉冷却材喪失(ECCS 性能評価)

・原子炉冷却材流量の喪失

・原子炉冷却材ポンプの軸固着

・主給水管破断

・主蒸気管破断

(2)反応度の異常な投入又は原子炉出力の急激な変化

・制御棒飛び出し

(3)環境への放射性物質の異常な放出

・蒸気発生器伝熱管破損

(4)原子炉格納容器内圧力、雰囲気等の異常な変化

・原子炉冷却材喪失(原子炉格納容器健全性評価)

なお、蒸気発生器伝熱管破損について、ソフトウェア CCF の重畳を考慮した場合における運転操作や操作時間が添付書類十解析と同等であり、判断基準に照らし合わせて影響の程度が軽微であるため解析を省略するが、当該事象に関する定性的な検討については 4.5.7 項にて述べる。また、「(4)原子炉格納容器内圧力、雰囲気等の異常な変化」のうち「可燃性ガスの発生」及び「(3)環境への放射性物質の異常な放出」に分類される事象の被ばく評価については、判断基準に照らし合わせて影響の程度が軽微であるため解析を省略するが、これら評価への影響については 4.6.2 項及び 4.6.3 項にて述べる。

４．ソフトウェア CCF 対策の有効性評価

３章にて選定した設計基準事象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、多様化設備等の対策により適切に対処可能であることを、ATENA が策定した ATENA ガイドに沿って評価する。その評価にあたっては、PWR プラントメーカが標準プラントとして解析入力値を整備している、以下に示す代表プラントを対象にソフトウェア CCF 対策の有効性を評価する。代表プラント以外の炉心条件等が異なるプラントに対する有効性については、4.6 節にて考察を行う。

＜代表プラント＞

・３ループプラント： 55GWd/t ウラン+MOX 炉心

・４ループプラント： 55GWd/t ウラン炉心

4.1 判断基準

有効性評価は、「運転時の異常な過渡変化」または「設計基準事故」とソフトウェア CCF が重畳するという設計基準を超える事象に対し、ソフトウェア CCF 影響緩和対策により、炉心損傷防止が可能になることを確認することが目的である。設計基準事象を超える事象であるが、安全保護回路に対して設けたソフトウェア CCF 影響緩和対策により、事象進展を設計基準対処設備が担う深層防護のレベルに留めることができる能力を確認することが目的であることから、設計基準事故の判断基準を基本とする。このため、「運転時の異常な過渡変化」及び「設計基準事故」のいずれに対しても、判断基準は設計基準事故において適用される判断基準（「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」第十三条第一項第二号）を準用し、その判断基準を概ね満足することを確認する。

なお、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℃）を適用する。

各事象に適用する具体的な判断基準については、4.4 節及び 4.5 節に記す。

4.2　解析に使用する計算プログラム

4.2.1　Non-LOCA

「運転時の異常な過渡変化」または「設計基準事故」とソフトウェア CCF が重畳する事象は設計基準を超える事象であるため、これら事象のプラント応答を評価するにあたっては、想定する事象を現実的に予測でき、設置変更許可申請書 添付書類十解析（重大事故等対策の有効性評価）に使用実績のある以下の最適評価コードを使用する。また、設計基準事象への適用性については、参考文献(2),(3)の SPARKLE-2 コードの DBA への適用に関する公開文献で示すとおり、最適評価コードの適用範囲に問題はないことを確認している。

・SPARKLE-2 コード[(2)(3)(4)]

4.2.2　LOCA

ATENA ガイドでは、“ソフトウェア CCF が重畳する場合においても、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最適評価を行わず保守的評価を採用してもよい。“と定めている。

解析対象とする LOCA 事象については、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。

LOCA 解析に使用する計算プログラムを表 4.2-1 に示す。計算プログラムは添付書類十解析（設計基準事故）の評価で使用する計算プログラムと同じである。

表4.2-1　LOCA解析に使用する計算プログラム

解析項目			計算プログラム	
			添付書類十解析 (設計基準事故)	CCF 対策 有効性評価
原子炉冷却材の喪失又は炉心冷却状態の著しい変化	原子炉冷却材喪失	大破断(5)	SATAN-M WREFLOOD BASH-M COCO LOCTA-M	同左
		小破断(6)	SATAN-M(Small LOCA) LOCTA-Ⅳ	同左
原子炉格納容器内圧力、雰囲気等の異常な変化	原子炉冷却材喪失(7)		SATAN-Ⅵ WREFLOOD COCO	同左

4.3　基本解析条件[1]

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」[8]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する。

各評価対象事象の解析条件を 4.4 節及び 4.5 節の主要解析条件に記載するとともに、代表３ループプラント及び代表４ループプラントの基本データを添付１に示す。

ソフトウェア CCF 発生時のデジタル安全保護回路、原子炉停止系統及び工学的安全施設を含む安全設備の作動状態、及び、ソフトウェア CCF 対策としての多様化設備については、以下を仮定する。

・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、自動起動信号また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。
・自動起動信号また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。
・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。

（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。）

ソフトウェア CCF 発生時の常用系設備の機能については、以下を仮定する。

・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。
・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。

・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。

解析にて自動起動を期待する多様化設備とその保護限界値、応答時間を表 4.3-1 と表 4.3-2 に示す。なお、多様化設備が作動させる設備に対するサポート系についての確認結果を添付 2 に示す。

ソフトウェア CCF 発生時の対応として、運転員による操作については、以下とする。

・運転員により事象が認知された後、整備される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、中央制御室、及び現場での運転員による手動操作を仮定する。
・運転員による操作の所要時間は、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た時間を仮定する。

ソフトウェア CCF 対策有効性評価で仮定する運転員操作条件を添付 1-3 に示す。

表4.3-1　自動起動を期待する多様化設備の保護限界値（代表３ループプラント）

自動起動を期待する多様化設備	保護限界値	応答時間（秒）	備考
原子炉圧力低信号による原子炉トリップ・タービントリップ・主給水隔離・主蒸気隔離	12.42MPa[gage]	12 秒	応答時間に、信号遅れ、多様化設備作動遅延タイマ（10 秒）を含む。主給水隔離、主蒸気隔離の弁作動時間は別途考慮する。
原子炉圧力高信号による原子炉トリップ・タービントリップ・主給水隔離・主蒸気隔離	16.90MPa[gage]	12 秒	
蒸気発生器水位低信号による原子炉トリップ・タービントリップ・主給水隔離・主蒸気隔離	7.0%	12 秒	
蒸気発生器水位低信号による補助給水起動	7.0%	60 秒	応答時間に、信号遅れ、多様化設備作動遅延タイマ（10 秒）、ポンプ起動時間等を含む。
原子炉圧力異常低による高圧／低圧注入系作動	11.03MPa[gage]	20 秒※	

※外部電源の喪失は仮定しないため、ディーゼル発電機の負荷投入シーケンスを介さずに、高圧注入ポンプ及び低圧注入ポンプは所定の遅れ時間（作動遅延タイマ、ポンプ起動時間等）で非常用母線から同時に給電されて作動する。

表4.3-2　自動起動を期待する多様化設備の保護限界値（代表４ループプラント）

自動起動を期待する多様化設備	保護限界値	応答時間（秒）	備考
原子炉圧力低信号による原子炉トリップ・タービントリップ・主給水隔離・主蒸気隔離	12.42MPa[gage]	12 秒	応答時間に、信号遅れ、多様化設備作動遅延タイマ（10 秒）を含む。主給水隔離、主蒸気隔離の弁作動時間は別途考慮する。
原子炉圧力高信号による原子炉トリップ・タービントリップ・主給水隔離・主蒸気隔離	16.90MPa[gage]	12 秒	
蒸気発生器水位低信号による原子炉トリップ・タービントリップ・主給水隔離・主蒸気隔離	7.0%	12 秒	
蒸気発生器水位低信号による補助給水起動	7.0%	60 秒	応答時間に、信号遅れ、多様化設備作動遅延タイマ（10 秒）、ポンプ起動時間等を含む
原子炉圧力低による高圧／低圧注入系作動	11.72MPa[gage]	20 秒※	

※外部電源の喪失は仮定しないため、ディーゼル発電機の負荷投入シーケンスを介さずに、高圧注入ポンプ及び低圧注入ポンプは所定の遅れ時間（作動遅延タイマ、ポンプ起動時間等）で非常用母線から同時に給電されて作動する。