2020年8月6日
四国電力株式会社

伊方３号機 デジタル安全保護系への変更工事に係る
発電用原子炉設置変更許可申請書への影響について

１．デジタル安全保護系への変更工事の概要

伊方３号機においては、設備の保守性向上の観点から安全保護系ロジック盤を取替えることに伴い、安全保護系の論理演算機能の一部について、既設のデジタル制御装置である安全保護系計器ラックのソフトウェアにて実現することにより、デジタル安全保護系への変更工事を実施する。

安全保護系ロジック盤の論理演算機能については、アナログ設備で実現する。また、安全保護系計器ラックと安全保護系ロジック盤間の信号取り合いの変更に伴い、安全保護系計器ラックのハードウェアの一部の改造（入力端子の増設）を行うが、計装設備の計測範囲、警報作動範囲の変更を伴うものではない。

（別紙－１）

２．当該行為と照会対象法令（条項）の規定との関係について

発電用原子炉設置者は、核原料物質、核燃料物質及び原子炉の規制に関する法律（以下、「法」という）第４３条の３の８第１項に基づき、法第４３条の３の５第２項第２号から第５号まで又は第８号から第１１号までに掲げる事項を変更しようとするときは、政令で定めるところにより、原子力規制委員会の許可を受けなければならない。

上記１．で実現しようとする行為は、発電用原子炉施設の位置、構造及び設備に係るものであり、法第４３条の３の５第２項第５号及び第１０号に関連するが、以下の理由により、法第４３条の３の５第２項第５号及び第１０号を変更する事項に該当しないものと考える。

（別紙－２）

（１）本文五号

デジタル安全保護系への変更工事において、新たに安全保護系の論理演算機能の一部について、既設のデジタル制御装置である安全保護系計器ラックのソフトウェアにて実現するが、新規制基準の審査時に安全保護系にデジタル制御装置を適用していたことから、新規制基準で新たに安全保護回路の電子計算機の要求事項として追加された、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２４条第１項第６号（不正アクセス行為等の被害の防止）について、発電用原子炉設置変更許可申請書に記載し、許可されている。なお、本内容については、工事計画段階において基本設計方針に記載し、認可（平成28年3月23日付）を受けている。

また、安全保護系計器ラックの改造及び安全保護系ロジック盤の取替えを実施するため、負荷容量に変更を伴うが、代替電源（直流）による給電に関する記載に影響はない。

以上から、当該行為は、伊方発電所３号炉の発電用原子炉設置変更許可申請書本文五号の記載事項の範囲内で実施するものである。

（2）本文十号

デジタル安全保護系への変更工事において、新たに安全保護系の論理演算機能の一部について、既設のデジタル制御装置である安全保護系計器ラックのソフトウェアにて実現し、また、安全保護系ロジック盤の取替えを実施するが、安全保護系の設定点の作動限界値及び応答時間の記載に影響はない。

また、安全保護系計器ラックの改造及び安全保護系ロジック盤の取替えに伴い負荷容量の増加が見込まれるが、蓄電池容量内に収まることから、負荷切離しの手順に変更はない。

このため、当該行為は、伊方発電所３号炉の発電用原子炉設置変更許可申請書本文十号の記載事項の範囲内で実施するものである。

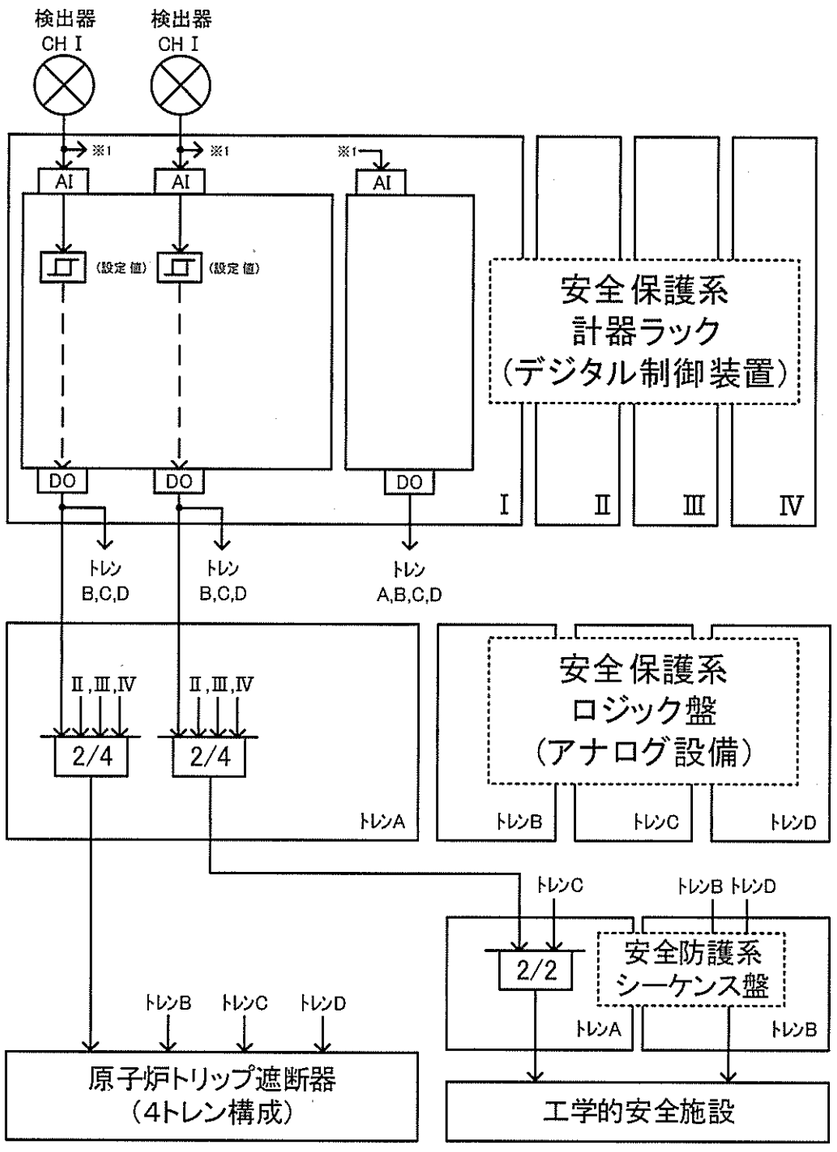
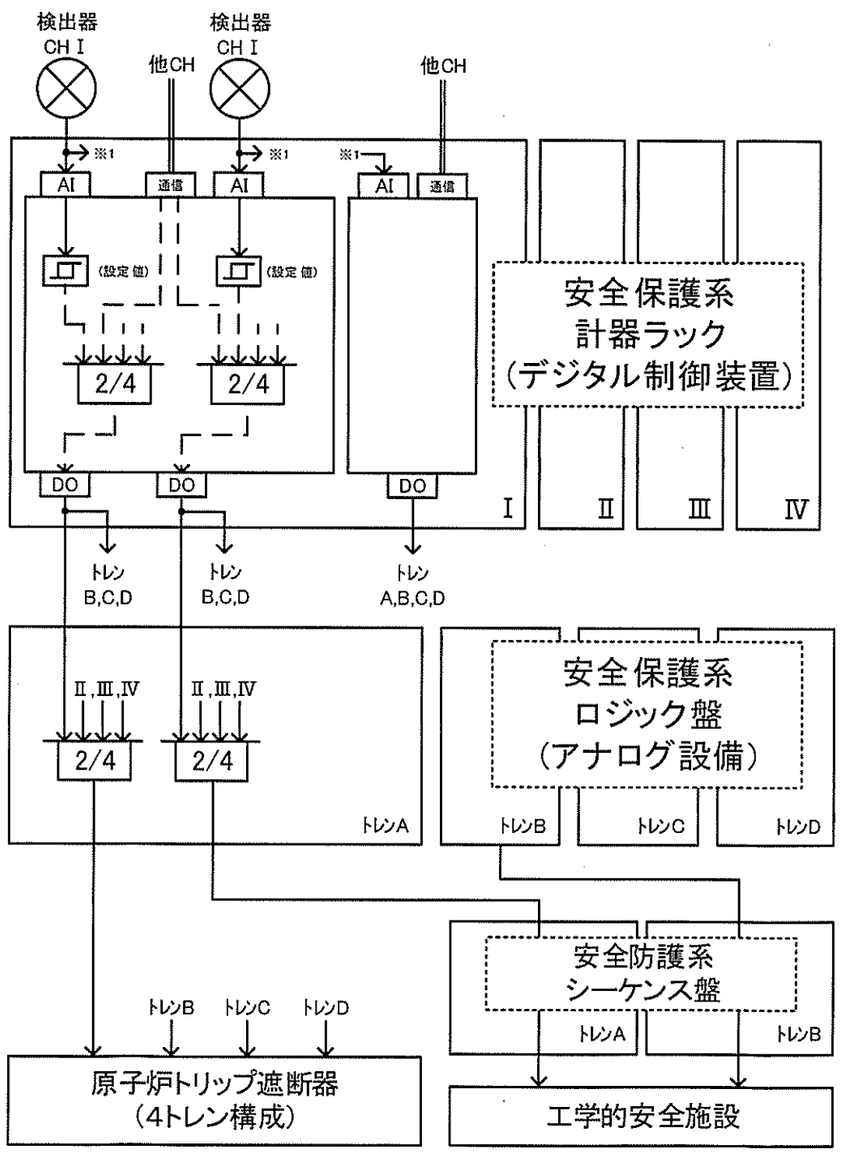
したがって、法第４３条の３の８第１項に基づく発電用原子炉設置変更許可申請は不要と考える。

別紙－１　伊方３号機デジタル安全保護系への変更工事の概要

別紙－２　伊方３号機デジタル安全保護系への変更工事に係る発電用原子炉設置変更許可申請書記載への影響評価

以上

伊方３号機デジタル安全保護系への変更工事の概要

変更前	変更後	変更内容
		デジタル制御装置である安全保護系計器ラックのソフトウェアにて、論理演算機能の一部を実現する。 安全保護系ロジック盤を取替える。

伊方３号機デジタル安全保護系への変更工事に係る発電用原子炉設置変更許可申請書記載への影響評価

許可申請書の記載	事業者の見解
五　発電用原子炉及びその附属施設の位置、構造及び設備	
へ　計測制御系統施設の構造及び設備 （２）安全保護回路 安全保護回路は，独立したチャンネルからなる多重チャンネル構成とし，測定変数に対して「２ out of ４」方式等の回路を形成し，原子炉停止回路及びその他の主要な安全保護回路（工学的安全施設作動回路）で構成される。 安全保護回路は，不正アクセス行為その他の電子計算機に使用目的に沿うべき動作をさせず，又は使用目的に反する動作をさせる行為による被害を防止する設計とする。 （ｉ）原子炉停止回路の種類 次に示す信号により発電用原子炉をトリップさせる原子炉停止回路を設ける。 ・中性子束高（線源領域及び中間領域） ・中性子束高（出力領域） ・中性子束変化率高（出力領域） ・非常用炉心冷却設備作動 ・過大温度ΔＴ高 ・過出力ΔＴ高 ・原子炉圧力高 ・原子炉圧力低 ・加圧器水位高 ・１次冷却材流量低 ・１次冷却材ポンプ電源電圧低 ・１次冷却材ポンプ電源周波数低 ・タービントリップ ・蒸気発生器水位低 ・地震加速度大 なお，手動操作で原子炉をトリップさせることができる。 （ⅱ）その他の主要な安全保護回路の種類 その他の主要な安全保護回路として，次の工学的安全施設作動回路を設ける。 ａ．原子炉圧力低と加圧器水位低の一致，原子炉圧力異常低，主蒸気ライン圧力低，原子炉格納容器圧力高のいずれかの信号による非常用炉心冷却設備の起動。 ｂ．原子炉格納容器圧力異常高信号による原子炉格納容器スプレイ設備の起動。 ｃ．原子炉格納容器圧力異常高，主蒸気ライン圧力低，主蒸気ライン圧力減少率高のいずれかの信号による主蒸気隔離弁の閉鎖。 ｄ．非常用炉心冷却設備作動信号又は原子炉格納容器スプレイ作動信号による主蒸気隔離弁以外の主要な原子炉格納容器隔離弁の閉鎖。 なお，手動操作で上記動作を行うことができる。	今回の工事において、新たに安全保護系の論理演算機能の一部について、既設のデジタル制御装置である安全保護系計器ラックのソフトウェアにて実現し、また安全保護系ロジック盤の取替えを実施するが、安全保護回路に係る多重チャンネル構成等に関する記載に変更はない。 また、安全保護系計器ラックは電子計算機を採用しており、安全保護系の論理演算機能の一部について、既設のデジタル制御装置である安全保護系計器ラックのソフトウェアにて実現する改造に際しても、不正アクセス行為等の防止に係る設計に変更はない。

許可申請書の記載	事業者の見解
(4)非常用制御設備 (iv)緊急停止失敗時に発電用原子炉を未臨界にするための設備 運転時の異常な過渡変化時において発電用原子炉の運転を緊急に停止することができない事象が発生するおそれがある場合又は当該事象が発生した場合においても炉心の著しい損傷を防止するため，原子炉冷却材圧力バウンダリ及び原子炉格納容器の健全性を維持するとともに，発電用原子炉を未臨界に移行するために必要な重大事故等対処設備を設置する。 緊急停止失敗時に発電用原子炉を未臨界に移行するための設備として以下の重大事故等対処設備（手動による原子炉緊急停止，原子炉出力抑制（自動），原子炉出力抑制（手動）及びほう酸水注入）を設ける。 a．フロントライン系故障時に用いる設備 (a) 手動による原子炉緊急停止 原子炉緊急停止が必要な原子炉トリップ設定値に到達した場合において，安全保護系ロジック盤の故障等により原子炉自動トリップに失敗した場合の重大事故等対処設備（手動による原子炉緊急停止）として，原子炉トリップスイッチは，手動による原子炉緊急停止ができる設計とする。 (b) 原子炉出力抑制（自動） 原子炉緊急停止が必要な原子炉トリップ設定値に到達した場合において，安全保護系ロジック盤又は原子炉トリップ遮断器の故障等により原子炉自動トリップに失敗した場合の重大事故等対処設備（原子炉出力抑制（自動））として，多様化自動作動盤（ATWS 緩和設備）は，発信する作動信号によるタービントリップ及び主蒸気隔離弁の閉止により，１次系から２次系への除熱を過渡的に悪化させることで原子炉冷却材温度を上昇させ，減速材温度上昇に伴う負の反応度帰還効果により原子炉出力を抑制できる設計とする。また，多様化自動作動盤（ATWS 緩和設備）は，補助給水タンクを水源とする電動補助給水ポンプ及びタービン動補助給水ポンプを自動起動させ，蒸気発生器水位の低下を抑制するとともに加圧器逃がし弁，加圧器安全弁，主蒸気逃がし弁及び主蒸気安全弁の作動により１次冷却系統の過圧を防止することで，原子炉冷却材圧力バウンダリ及び原子炉格納容器の健全性を維持できる設計とする。 (c) 原子炉出力抑制（手動） 多様化自動作動盤（ATWS 緩和設備）から自動信号が発信した場合において，原子炉の出力を抑制するために必要な機器等が自動作動しなかった場合の重大事故等対処設備（原子炉出力抑制（手動））として，中央制御室での操作により，手動で主蒸気隔離弁を閉止することで原子炉出力を抑制するとともに，補助給水タンクを水源とする電動補助給水ポンプ及びタービン動補助給水ポンプを手動で起動し，補助給水を確保することで蒸気発生器水位の低下を抑制し，加圧器逃がし弁，加圧器安全弁，主蒸気逃がし弁及び主蒸気安全弁の作動により１次冷却系統の過圧を防止できる設計とする。 (d) ほう酸水注入 制御棒クラスタ，原子炉トリップ遮断器又は安全保護系ロジック盤の故障等により原子炉トリップに失敗した場合の重大事故等対処設備（ほう酸水注入）として，ほう酸タンクを水源としたほう酸ポンプは，緊急ほう酸注入系統を介して充てんポンプにより炉心に十分な量のほう酸水を注入できる設計とする。 ほう酸ポンプが故障により使用できない場合の重大事故等対処設備（ほう酸水注入）として，燃料取替用水タンクを水源とした充てんポンプは，化学体積制御系統により炉心に十分な量のほう酸水を注入できる設計とする。	今回の工事において、安全保護系ロジック盤については取替えを実施するが、取替え後における安全保護系ロジック盤の故障時の影響に関する記載に変更はない。

許可申請書の記載	事業者の見解
ヌ．その他発電用原子炉の附属施設の構造及び設備 （２）非常用電源設備の構造 （ⅳ）代替電源設備 設計基準事故対処設備の電源が喪失したことにより重大事故等が発生した場合において，炉心の著しい損傷，原子炉格納容器の破損，使用済燃料貯蔵槽内燃料体等の著しい損傷及び運転停止中原子炉内燃料体の著しい損傷を防止するため，必要な電力を確保するために必要な重大事故等対処設備を設置及び保管する。 重大事故等の対応に必要な電力を供給するための設備として以下の非常用電源設備，代替電源設備，所内常設蓄電式直流電源設備，所内常設直流電源設備（３系統目），可搬型直流電源設備及び代替所内電気設備を設ける。 c．非常用電源（直流）による給電に用いる設備 (a) 蓄電池（非常用）による非常用電源（直流）からの給電 設計基準事故対処設備の電源が喪失（全交流動力電源喪失）した場合に，重大事故等の対応に必要な設備に直流電力を供給する所内常設蓄電式直流電源設備として，蓄電池（非常用）を使用する。 蓄電池（非常用）は，中央制御室に隣接する計装盤室において簡易な操作で必要な負荷以外を切り離すことにより８時間にわたり電力の供給を行うことが可能な設計とする。また，蓄電池（重大事故等対処用）と組み合わせることにより事象発生から 24 時間にわたり電力の供給を行うことが可能な設計とする。 d．代替電源（直流）による給電に用いる設備 (a) 蓄電池（重大事故等対処用）による代替電源（直流）からの給電 設計基準事故対処設備の電源が喪失（全交流動力電源喪失）した場合に，重大事故等の対応に必要な設備に直流電力を供給する所内常設蓄電式直流電源設備として，蓄電池（重大事故等対処用）を使用する。 蓄電池（重大事故等対処用）は，蓄電池（非常用）により８時間にわたり電力の供給を行った後，中央制御室に隣接する計装盤室以外の場所で必要な負荷以外を切り離して 16 時間にわたり電力の供給を行うことが可能な設計とする。また，蓄電池（非常用）と組み合わせることにより 24 時間にわたり電力の供給を行うことが可能な設計とする。 (b) 蓄電池（３系統目）による代替電源（直流）からの給電 更なる信頼性を向上するため，設計基準事故対処設備の電源が喪失（全交流動力電源喪失）した場合に，重大事故等の対応に必要な設備に直流電力を供給するため，特に高い信頼性を有する所内常設直流電源設備（３系統目）として，蓄電池（３系統目）を使用する。 蓄電池（３系統目）は，中央制御室に隣接する計装盤室において簡易な操作で必要な負荷以外を切り離すことにより８時間，その後，必要な負荷以外を切り離して残り 16 時間の合計 24 時間にわたり，電力の供給を行うことが可能な設計とする。	今回の工事において、新たに安全保護系の論理演算機能の一部について、既設のデジタル制御装置である安全保護系計器ラックのソフトウェアにて実現し、また安全保護系ロジック盤の取替えを実施することに伴い、負荷容量が変更になるが、代替電源（直流）による給電に関する記載に変更はない。

許可申請書の記載	影響評価
十　発電用原子炉の炉心の著しい損傷その他の事故が発生した場合における当該事故に対処するために必要な施設及び体制の整備に関する事項	
イ　運転時の異常な過渡変化 (2)解析条件 (i)主要な解析条件 a．初期定常運転条件 原子炉出力の初期値として，定格値（2,660MWt）に定常運転出力決定に際して生じる熱校正の誤差（定格値の±２％）を考慮した値を用いる。また，１次冷却材平均温度の初期値は，定格値（302.3℃）に定常運転時の誤差（±2.2℃）を考慮した値，原子炉圧力の初期値は，定格値（15.41MPa[gage]）に定常運転時の誤差（±0.21MPa）を考慮した値を用いる。 これらの初期値の選定に際しては，判断基準に照らして解析結果が最も厳しくなるように定常誤差の符号を選択するが，ＤＮＢＲの評価では改良統計的熱設計手法を使用するため，初期定常運転状態の誤差の効果は最小ＤＮＢＲの許容限界値に含まれており，初期値として定格値を用いる。 b．安全保護系の設定点の作動限界値及び応答時間 原子炉トリップ限界値及び応答時間を以下に示す。 出力領域中性子束高(高設定) 118%(定格出力値に対して)（応答時間0.5秒） 出力領域中性子束高(低設定) 35%(定格出力値に対して)（応答時間0.5秒） 過大温度ΔＴ高 １次冷却材平均温度等の関数（第１図参照） （応答時間6.0秒） 過出力ΔＴ高 １次冷却材平均温度等の関数（第１図参照） （応答時間6.0秒） 原子炉圧力高 16.61MPa[gage]（応答時間2.0秒） 原子炉圧力低 12.73MPa[gage]（応答時間2.0秒） １次冷却材流量低 87%(定格流量に対して)（応答時間1.0秒） １次冷却材ポンプ電源電圧低 65%(定格値に対して)（応答時間1.2秒） 蒸気発生器水位低 狭域水位検出器下端水位（応答時間2.0秒） タービントリップ －　（応答時間1.0秒） 工学的安全施設作動信号の作動限界値及び応答時間を以下に示す。 (a) 非常用炉心冷却設備作動信号 原子炉圧力低と加圧器水位低の一致 12.04MPa[gage](圧力)と水位検出器下端水位(水位)（応答時間2.0秒）	今回の工事において、新たに安全保護系の論理演算機能の一部について、既設のデジタル制御装置である安全保護系計器ラックのソフトウェアにて実現するが、作動限界値及び応答時間の記載に変更はない。

許可申請書の記載	影響評価
原子炉圧力異常低 11.36MPa[gage]（応答時間2.0秒） 主蒸気ライン圧力低 3.35MPa[gage]（応答時間2.0秒） 原子炉格納容器圧力高 0.034MPa[gage]（応答時間2.0秒） (b) 主蒸気ライン隔離信号 主蒸気ライン圧力低 3.35MPa[gage]（応答時間2.0秒） (c) 原子炉格納容器スプレイ作動信号 原子炉格納容器圧力異常高 0.136MPa[gage]（応答時間2.0秒） ロ 設計基準事故 (2)有効性評価 (b) 共通評価条件 (ii)評価条件 a．主要な解析条件 (b-1) 運転中の原子炉における重大事故に至るおそれがある事故 (b-1-3) 重大事故等対策に関連する機器条件 ・原子炉自動停止時の制御棒クラスタ落下による反応度の添加は，余裕を考慮した値を使用する。制御棒クラスタ落下開始から全ストロークの85%落下までの時間を2.2 秒とする。 ・安全保護系の設定点の作動限界値及び応答時間 原子炉トリップ限界値及び応答時間として以下の値を用いるものとする。 過大温度ΔT高 1次冷却材平均温度等の関数（応答時間6.0 秒） 原子炉圧力低 12.73MPa[gage]（応答時間2.0 秒） 1次冷却材ポンプ電源電圧低 65%（定格値に対して）（応答時間1.2 秒） 蒸気発生器水位低 蒸気発生器狭域水位11%（応答時間2.0 秒） また，工学的安全施設作動信号のうち，ＥＣＣＳの作動限界値及び応答時間として以下の値を用いるものとする。 原子炉圧力低と加圧器水位低の一致 12.04MPa[gage]（圧力）と水位検出器下端水位（水位）の一致（応答時間2.0 秒） 原子炉圧力異常低 11.36MPa[gage]（応答時間2.0 秒） （ただし，事故シーケンスグループ「原子炉格納容器の除熱機能喪失」及び「ＥＣＣＳ再循環機能喪失」を除く）	今回の工事において、新たに安全保護系の論理演算機能の一部について、既設のデジタル制御装置である安全保護系計器ラックのソフトウェアにて実現するが、作動限界値及び応答時間の記載に変更はない。

許可申請書の記載	影響評価

第 10.1 表　重大事故等対策における手順書の概要（１／１９）（その１）

1.14　電源の確保に関する手順等		
目的		電源が喪失したことにより重大事故等が発生した場合，炉心の著しい損傷，原子炉格納容器の破損，使用済燃料ピット内燃料体等の著しい損傷及び運転停止中における原子炉内の燃料体の著しい損傷を防止するため非常用電源（交流），代替電源（交流），非常用電源（直流），代替電源（直流），代替所内電気設備から給電するための手順等を整備する。
対応手順等	非常用電源（交流）からの給電	外部電源喪失及び所内単独運転に失敗した場合は，非常用高圧母線へディーゼル発電機による給電を行い，給電状態を母線電圧により確認する。
	代替電源（交流）からの給電	全交流動力電源が喪失した場合は，以下の手段により非常用高圧母線又は非常用低圧母線へ代替電源（交流）から給電し，母線電圧により受電確認する。 ・非常用ガスタービン発電機又は空冷式非常用発電装置からの受電準備を行ったのち非常用ガスタービン発電機又は空冷式非常用発電装置を起動し非常用高圧母線へ給電する。 ・300kVA電源車からの受電準備を行ったのち300kVA電源車を起動し非常用低圧母線へ給電する。 代替電源（交流）による給電手段の優先順位は，非常用ガスタービン発電機，空冷式非常用発電装置，300kVA電源車の順で使用する。
	非常用電源（直流）からの給電	全交流動力電源が喪失した場合は，非常用直流母線へ蓄電池（非常用）により給電し，給電状態を母線電圧により確認する。
	代替電源（直流）からの給電	交流動力電源が復旧する見込みがない場合，24時間以上にわたり必要な負荷へ給電するため，蓄電池（重大事故等対処用）により非常用直流母線へ給電する。全交流動力電源喪失発生後，２時間以内に中央制御室に隣接する計装盤室で不要な直流負荷の切離しを行い，８時間以内に現場で不要な直流負荷の切離しを行う。また，蓄電池（重大事故等対処用）からの給電にて母線電圧が低下する前までに蓄電池（３系統目）により非常用直流母線へ給電する。蓄電池（重大事故等対処用）又は蓄電池（３系統目）からの給電にて母線電圧が低下する前に，可搬型直流電源装置により非常用直流母線へ給電する。

今回の工事において、新たに安全保護系の論理演算機能の一部について、既設のデジタル制御装置である安全保護系計器ラックのソフトウェアにて実現し、また安全保護系ロジック盤の取替えを実施することに伴い、負荷容量が変更になるが、代替電源（直流）による給電に関する記載に変更はない。

別紙-3

資料２－１－１

伊方発電所３号炉

誤操作の防止について
安全避難通路等について
全交流動力電源喪失対策設備について
安全保護回路について

平成２５年１２月　３日
四国電力株式会社

目　次

Ⅳ　安全保護回路について

1．概要

安全保護回路に対しては、「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」第二十四条第１項第六号にておいて「不正アクセス行為その他の電子計算機に使用目的に沿うべき動作をさせず、又は使用目的に反する動作をさせる行為による被害を防止することができるものとすること。」が要求されており、以下の対策を実施している。

●外部ネットワークからの不正アクセス及びコンピュータウイルス等の侵入防止対策

安全保護回路は外部ネットワークに直接接続せず、外部ネットワークからの不正アクセス及びコンピュータウィルス等の侵入防止を図る。

●物理的、電気的アクセス制限に係る管理

発電所の入域制限、安全保護回路を構成する制御盤の設置区画及び盤扉の施錠管理及び安全保護系に適用したデジタル計算機のソフトウェア変更に使用する保守ツールのパスワード管理により、不正行為の防止を図る。

なお、安全保護系に適用したデジタル計算機に対しては、「ディジタル安全保護系の検証及び妥当性確認に関する指針」(JEAG4609-2008)に基づき、設備の設計、製作、試験、変更管理の各段階において、上流仕様と下流仕様の整合性確認を主体とする検証及び妥当性確認を行うことにより、安全保護上要求される機能が正しく確実に実現されていることを保証する活動を行っている。

2．外部ネットワークからの不正アクセス防止

- 安全保護系は、原子炉計装あるいは安全保護系のプロセス計装からの信号を受信し、原子炉停止回路を作動させ、原子炉を自動停止させる原子炉保護設備と、安全保護系のプロセス計装からの信号を受信し、工学的安全施設を作動させる工学的安全施設作動設備で構成される。
- 安全保護系では計器ラックにデジタル計算機を適用しているが、プラントデータを収集するプラント計算機に対してアナログ信号の形式で信号を伝送しており、直接外部ネットワークに接続していないことから、外部ネットワークからの遠隔操作及びウィルス等の侵入による被害を受けることはない。

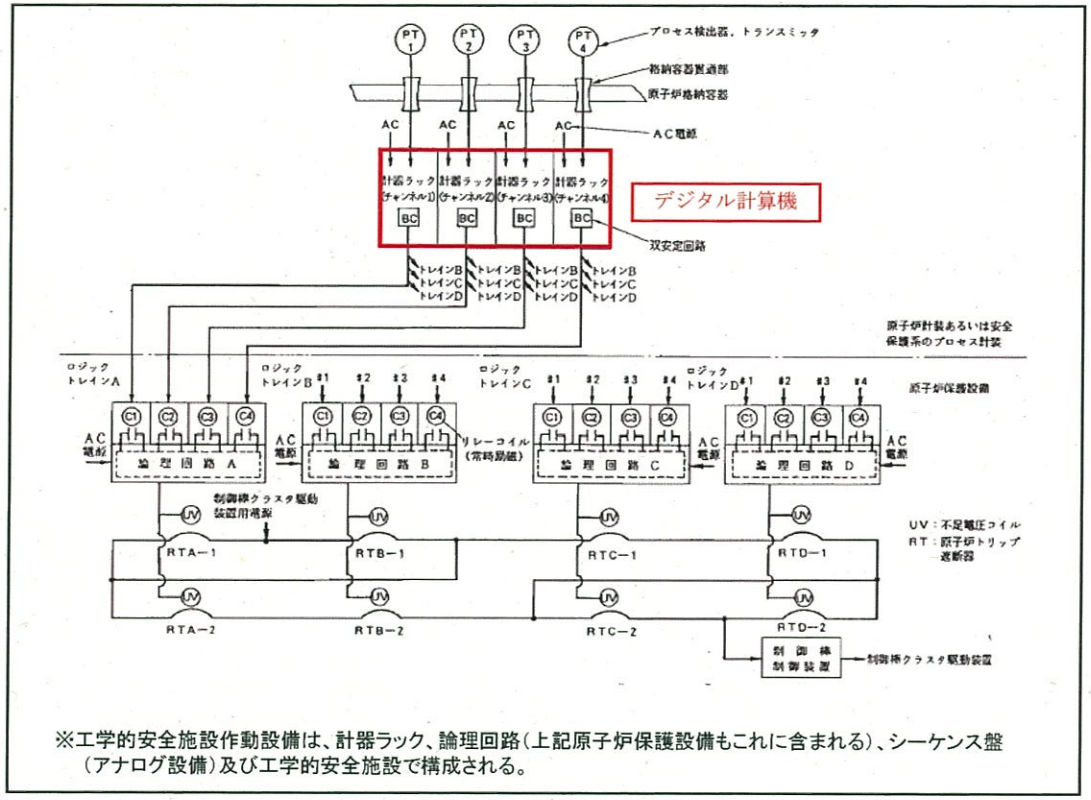


図１　原子炉保護設備の構成

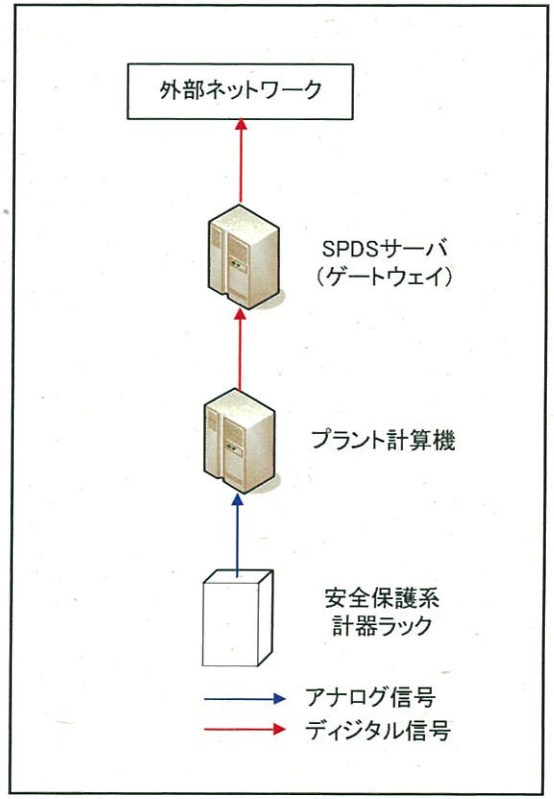


図２　外部ネットワークとの接続構成

3. 物理的、電気的アクセス制限に係る管理

物理的、電気的アクセスの制限対策として、以下の管理を行っている。

●発電所への入域に対しては、出入管理等により入域を制限している。また、安全保護系に対しては、安全保護回路を構成する制御盤を設置している区画及び盤扉の施錠管理を当直長が実施している。

●デジタル計算機のソフトウェアを変更する際に使用する専用の保守ツールに対しては、デジタル計算機のソフトウェア管理責任者が、操作権限に応じたパスワードを設定するとともにパスワードは定期的に見直しを行い、関係者以外の不正な変更等を防止している。

●デジタル計算機を適用した安全保護系のソフトウェアを変更する場合は、工事の主管箇所が変更理由、変更箇所等を文書化し、変更の影響範囲を明確にした上で作業を実施する。また、ソフトウェアの変更作業を行う場合は、工事の主管箇所が承認した作業手順に基づき作業を行い、作業者及び当社がソフトウェアインストール前後に行うソフトウェア照合の結果により、意図した箇所以外の変更がないことを確認する。

4. デジタル計算機の検証及び妥当性確認

- 安全保護系にデジタル計算機を適用するに当たり、安全保護上要求される機能が正しく確実に実現されていることを保証するため、設計、製作、試験、変更管理の各段階において、「安全保護系へのディジタル計算機の適用に関する規定」(JEAC4620-2008)及び「ディジタル安全保護系の検証及び妥当性確認に関する指針」(JEAG4609-2008)に基づき、検証及び妥当性確認(V&V)を実施している。
- 検証及び妥当性確認がなされたソフトウェアを使用することにより、デジタル計算機の導入時及び導入後のソフトウェア変更において、安全保護上の要求を満足する機能を確実に実現することができ、意図しない動作を防止することができる。

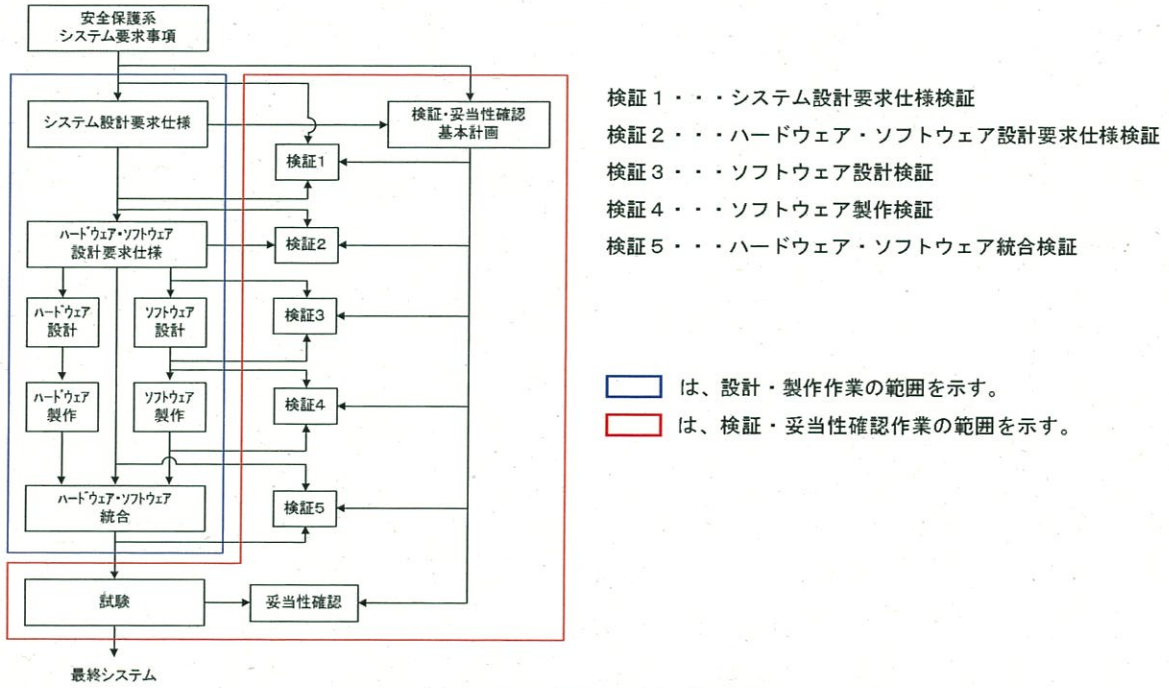


図　検証及び妥当性確認概要

別紙-1②

本資料のうち、枠囲みの内容は核物質防護にかかる情報のため、公開できません。

資料２－１－２

伊方発電所３号炉
誤操作の防止について
安全避難通路等について
全交流動力電源喪失対策設備について
安全保護回路について
補足説明資料

平成２５年１２月　３日

四国電力株式会社

Ⅳ．安全保護回路について

１．新規制基準への適合状況

実用発電用原子炉及びその付属施設の位置、構造及び設備の基準に関する規則　第二十四条（安全保護回路）

新規制基準の項目	適合状況
発電用原子炉施設には、次に掲げるところにより、安全保護回路（安全施設に属するものに限る。以下この条において同じ。）を設けなければならない。	
一　運転時の異常な過渡変化が発生する場合において、その異常な状態を検知し、及び原子炉停止系統その他系統と併せて機能することにより、燃料要素の許容損傷限界を超えないようにできるものとすること。	【規制要求変更なし】 安全保護回路には、予想される各種の運転時の異常な過渡変化に対処し得る複数の原子炉トリップ信号及び工学的安全施設作動信号を設け、運転時の異常な過渡変化時に、原子炉の過出力状態や出力の急激な上昇等の異常状態を検知した場合には、原子炉停止系を作動させて原子炉を自動的に停止させるとともに、必要に応じて工学的安全施設作動設備により非常用炉心冷却設備を自動的に作動させ、燃料の許容設計限界を超えることがないようにできる。
二　設計基準事故が発生する場合において、その異常な状態を検知し、原子炉停止系統及び工学的安全施設を自動的に作動させるものとすること。	【規制要求変更なし】 安全保護回路は、事故時に異常状態を検知し、原子炉保護設備の動作により原子炉を自動的に停止させる。また、自動的に非常用炉心冷却設備の起動、格納容器隔離弁の閉鎖、原子炉格納容器スプレイ設備の起動を行なわせること等ができる。
三　安全保護回路を構成する機械若しくは器具又はチャンネルは、単一故障が起きた場合又は使用状態からの単一の取り外しを行った場合において、安全保護機能を失わないよう、多重性を確保するものとすること。	【規制要求変更なし】 安全保護回路は、使用状態からの単一の取り外し、あるいは運転時の異常な過渡変化時及び事故時においてチャンネルの単一故障を想定しても、安全保護機能を失うことがなく、かつ、誤信号発生等による誤動作を防止するため原則として“2 out of 4”構成としている。 プラント起動等、その安全機能を必要とする期間が短時間に限られる場合は、その短期間でのチャンネルの故障確率が小さいことか

新規制基準の項目	適合状況
	ら、“1 out of 2”構成としている。
四　安全保護回路を構成するチャンネルは、それぞれ互いに分離し、それぞれのチャンネル間において安全保護機能を失わないように独立性を確保するものとすること。	【規制要求変更なし】 安全保護回路を構成するチャンネルに対しては、以下の設計により、各チャンネル相互を実用上可能な限り物理的、電気的に分離し独立性を図っている。 （1）計装用配管は、格納容器貫通部を含めて可能な限りチャンネルごとに分離、独立している。 （2）各チャンネルごとに専用のケーブルトレイ、計器ラック等を設置している。 （3）各チャンネルの電源は、無停電電源4母線から独立に供給する設計としている。
五　駆動源の喪失、系統の遮断その他の不利な状況が発生した場合においても、発電用原子炉施設をより安全な状態に移行するか、又は当該状態を維持することにより、発電用原子炉施設の安全上支障がない状態を維持できるものとすること。	【規制要求変更なし】 安全保護回路のうち原子炉保護系を自動的に作動させる設備の双安定回路、原子炉トリップ遮断器の不足電圧コイル等は、駆動源の喪失、系の遮断に対して、原子炉をトリップさせる方向に作動する。 その他の安全保護回路は、駆動源の喪失、系の遮断に対して安全保護動作が作動するか又はそのまま現在の状態を維持する。この現状維持の場合でも多重化されたほかの回路が保護動作を行うことから、安全上支障がない。
六　不正アクセス行為その他の電子計算機に使用目的に沿うべき動作をさせず、又は使用目的に反する動作をさせる行為による被害を防止することができるものとすること。	【新規要求事項】 安全保護回路は，不正アクセス行為又は電子計算機の使用目的と異なる動作をさせる行為による被害を防止するため，電気通信回線を通じて妨害行為又は破壊行為を受けることがないように，電気通信回線を通じた当該情報システムに対する外部からの不正なアクセスを遮断することができる。

新規制基準の項目	適合状況
七　計測制御系統施設の一部を安全保護回路と共用する場合には、その安全保護機能を失わないよう、計測制御系統施設から機能的に分離されたものとすること。	物理的及び電気的アクセスの制限対策として、発電所への入域に対しては、出入管理等により入域を制限している。また、安全保護、安全保護回路を設置している部屋および盤の施錠管理を実施している。 デジタル計算機を適用した安全保護系のソフトウェア変更に使用する専用の保守ツールに対しては、操作権限に応じたパスワードを設定するとともにパスワードは定期的に見直しを行い、関係者以外の不正な変更等を防止している。 【規制要求変更なし】 安全保護回路は、計測制御系統施設から分離した設計としている。安全保護回路の一部から計測制御系統施設への信号を取り出す場合には、絶縁増幅器を使用し、出力側（計測制御系統施設）で回路の短絡、開放等の故障が生じても入力側（安全保護回路）へ影響を与えない設計としている。

新規制基準の項目	適合状況
（解釈） 1　第１号について、安全保護回路の運転時の異常な過渡変化時の機能の具体例としては、原子炉の過出力状態や出力の急激な上昇を防止するために、異常な状態を検知し、原子炉停止系統を含む適切な系統を作動させ、緊急停止の動作を開始させること等をいう。	【規制要求変更なし】 第１項第一号と同じ。
2　第３号に規定する「チャンネル」とは、安全保護動作に必要な単一の信号を発生させるために必要な構成要素（抵抗器、コンデンサ、トランジスタ、スイッチ及び導線等）及びモジュール（内部連絡された構成要素の集合体）の配列であって、検出器から論理回路入口までをいう。	【規制要求変更なし】 第１項第三号と同じ。
3　第４号に規定する「それぞれ互いに分離し」とは、独立性を有するようなチャンネル間の物理的分離及び電気的分離等をいう。	【規制要求変更なし】 第１項第四号と同じ。
4　第５号に規定する「駆動源の喪失、系統の遮断その他の不利な状況」とは、電力若しくは計装用空気の喪失又は何らかの原因により安全保護回路の論理回路が遮断される等の状況をいう。なお、不利な状況には、環境条件も含むが、どのような状況を考慮するかは、個々の設計に応じて判断する。	【規制要求変更なし】 第１項第五号と同じ。

新規制基準の項目	適合状況
5　第５号に規定する「発電用原子炉施設をより安全な状態に移行するか、又は当該状態を維持することにより、発電用原子炉施設の安全上支障がない状態を維持できるもの」とは、安全保護回路が単一故障した場合においても、発電用原子炉施設をより安全な状態に移行することにより、最終的に発電用原子炉施設が安全側の状態を維持するか、又は安全保護回路が単一故障してそのままの状態にとどまっても発電用原子炉施設の安全上支障がない状態を維持できることをいう。	【規制要求変更なし】 第１項第五号と同じ。
6　第６号に規定する「不正アクセス行為その他の電子計算機に使用目的に沿うべき動作をさせず、又は使用目的に反する動作をさせる行為による被害を防止すること」とは、ハードウェアの物理的分離、機能的分離に加え、システムの導入段階、更新段階又は試験段階でコンピュータウイルスが混入することを防止する等、承認されていない動作や変更を防ぐ設計のことをいう。	【新規要求事項】 第１項第六号と同じ。
7　第７号に規定する「安全保護機能を失わない」とは、接続された計測制御系統施設の機器又はチャンネルに単一故障、誤操作若しくは使用状態からの単一の取り外しが生じた場合においても、これにより悪影響を受けない部分の安全保護回路が第１号から第６号を満たすことをいう。	（規制要求変更なし（第６号を除く）） 解釈第１号から第６号と同じ。

実用発電用原子炉及びその付属施設の技術基準に関する規則　第三十五条（安全保護装置）

新規制基準の項目	適合状況
発電用原子炉施設には、安全保護装置を次に定めるところにより施設しなければならない。	
一　運転時の異常な過渡変化が発生する場合又は地震の発生により発電用原子炉の運転に支障が生ずる場合において、原子炉停止系統その他系統と併せて機能することにより、燃料要素の許容損傷限界を超えないようにできるものであること。	【規制要求変更なし】 「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」第二十四条第１項第一号と同じ。
二　系統を構成する機械若しくは器具又はチャンネルは、単一故障が起きた場合又は使用状態からの単一の取り外しを行った場合において、安全保護機能を失わないよう、多重性を確保すること。	【規制要求変更なし】 「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」第二十四条第１項第三号と同じ。
三　系統を構成するチャンネルは、それぞれ互いに分離し、それぞれのチャンネル間において安全保護機能を失わないように独立性を確保すること。	【規制要求変更なし】 「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」第二十四条第１項第四号と同じ。
四　駆動源の喪失、系統の遮断その他の不利な状況が生じた場合においても、発電用原子炉施設をより安全な状態に移行するか、又は当該状態を維持することにより、発電用原子炉施設の安全上支障がない状態を維持できること。	【規制要求変更なし】 「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」第二十四条第１項第五号と同じ。
五　不正アクセス行為その他の電子計算機に使用目的に沿うべき動作をさせず、又は使用目的に反する動作をさせる行為による被害を防止するために必要な措置が講じられているものであること。	【新規要求事項】 「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」第二十四条第１項第六号と同じ。

新規制基準の項目	適合状況
六　計測制御系の一部を安全保護装置と共用する場合には、その安全保護機能を失わないよう、計測制御系から機能的に分離されたものであること。 七　発電用原子炉の運転中に、その能力を確認するための必要な試験ができるものであること。	【規制要求変更なし】 「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」第二十四条第１項第七号と同じ。 【規制要求変更なし】 （１）　安全保護回路のプロセス計装は原則として、４チャンネルで構成し、運転中、任意の１チャンネルについて検出器の出力信号回路に模擬入力を印加し、設定値確認を行うことができる。 この場合、残りのチャンネルの信号により論理回路を作動し、保護機能（原子炉トリップ、非常用炉心冷却設備作動等）を作動させることができる。 （２）　原子炉保護設備は４トレインで構成し、運転中、任意の１トレインについてテストスイッチ操作により論理回路の作動確認を行うことができる。 この場合、残りのトレインの信号により保護機能（原子炉トリップ）を作動させることができる。 （３）　原子炉トリップ遮断器は４トレインで構成し、運転中、任意の１トレインについてテストスイッチ操作により遮断器が開放することを確認することができる。 この場合、残りのトレインの遮断器により保護機能（原子炉トリップ）を作動させることができる。 （４）　工学的安全施設作動回路は、２トレインで構成し、運転中、任意の１トレインについてテストスイッチ操作により論理回路の作動確認を行うことができる。 この場合、残りのトレインの信号により保護機能（非常用炉心冷却設備作動等）を作動させることができる。

新規制基準の項目	適合状況
八　運転条件に応じて作動設定値を変更できるものであること。	【規制要求変更なし】 安全保護回路は、運転条件に応じて作動設定値を変更できるものである。
（解釈） 1　第１号の安全保護装置の機能の確認については、設置許可申請書の添付書類八の設備仕様及び設置許可申請書において評価した運転時の異常な過渡変化の評価の条件に非保守的な変更がないことを確認すること。	【規制要求変更なし】 第１号の安全保護装置の機能の確認については、設置許可申請書の添付書類八の設備仕様及び設置許可申請書において評価した運転時の異常な過渡変化の評価の条件に非保守的な変更がないことを確認している。
2　第３号に規定する「独立性を確保すること」とは、チャンネル間の距離、バリア、電気的隔離装置等により、相互を分離することをいう。	【規制要求変更なし】 「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」第二十四条第１項第四号と同じ。
3　第５号に規定する「必要な措置が講じられているものであること」とは、外部ネットワークと物理的な分離又は機能的な分離を行うこと、有線又は無線による外部ネットワークからの遠隔操作及びウイルス等の侵入を防止すること、物理的及び電気的アクセスの制限を設けることにより、システムの据付、更新、試験、保守等で、承認されていない者の操作及びウイルス等の侵入を防止すること等の措置を講じることをいう。なお、ソフトウェアの内部管理を強化するために、ウイルス等によるシステムの異常動作を検出させる場合には以下の機能を有すること。	【新規要求事項】 「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」第二十四条第１項第六号と同じ。 なお、ウイルス等によるシステムの異常動作を検知する機能については、安全保護設備では汎用ではない言語及びプログラムを使用しており、また、外部ネットワークと直接接続していないことから、設けていない。

新規制基準の項目	適合状況
（１）ウイルス等によるシステムの異常動作を検出する機能を設ける場合には、ウイルス等を検知した場合に運転員等へ告知すること。	前項のとおり
（２）ウイルス等によるシステムの異常動作を検出する機能は、安全保護装置の機能に悪影響を及ぼさないこと。	前項のとおり
４　デジタル安全保護系の適用に当たっては、日本電気協会「安全保護系へのディジタル計算機の適用に関する規程」（JEAC 4620-2008）（以下「JEAC4620」という。）５．留意事項を除く本文、解説－４から６まで、解説－８及び解説－１１から１８まで並びに「ディジタル安全保護系の検証及び妥当性確認に関する指針」（JEAG 4609-2008）本文及び解説－９に以下の要件を付したものによること。ただし、「ディジタル」は「デジタル」と読み替えること。	【規制要求変更なし】 安全保護回路にはデジタル計算機を適用していない。 なお、安全保護回路ではないが、安全保護系にデジタル計算機を適用した安全保護系計器ラックについては、JEAC 4620、JEAG 4609の要求事項を満足したものとなっている。本事項以降の適合性は、安全保護計器ラックについて、新規制基準への適合状況を記す。
（１）JEAC4620の４．１の適用当たっては、運転時の異常な過渡変化が生じる場合又は地震の発生等により原子炉の運転に支障が生じる場合において、原子炉停止系統及び工学的安全施設と併せて機能することにより、燃料許容損傷限界を超えないよう安全保護系の設定値を決定すること。	【規制要求変更なし】 安全保護系計器ラックは、プラントでの異常な状態を検知し、適切な系統を自動的に作動させ、燃料が許容設計限界を超えない設計としている。
（２）JEAC4620の４．１８．３において検証及び妥当性確認の実施に際して作成された文書は、４．１８．２の構成管理計画の中に文書の保存を定め、適切に管理すること。	【規制要求変更なし】 安全保護系計器ラックの検証と妥当性確認の実施に際して作成された文書は、デジタル安全保護系管理手順書の構成管理対象に含めている。

新規制基準の項目	適合状況
（３）JEAC4620の４．８における「想定される電源擾乱、電磁波等の外部からの外乱・ノイズの環境条件を考慮した設計とすること」を「想定される電源擾乱、サージ電圧、電磁波等の外部からの外乱・ノイズの環境条件を考慮して設計し、その設計による対策の妥当性が十分であることを確証すること」と読み替えること。	【規制要求変更なし】 安全保護系計器ラックは、インバータとの協調により、想定される電源撹乱が発生した場合においても安全保護系に影響を与えない設計としている。また、サージ電圧（雷サージ）による擾乱に対しては、建屋内に設置するとともに、規格に基づいたサージに対する耐力を有する設計としている。また、外部からの外乱・ノイズの環境条件を設計としており、その設計による対策の妥当性を確認している。
（４）JEAC4620の４．５及び解説－６の適用に当たっては、デジタル安全保護系は、試験時を除き、計測制御系からの情報を受けないこと。試験時に、計測制御系からの情報を受ける場合には、計測制御系の故障により、デジタル安全保護系が影響を受けないように措置を講じること。デジタル安全保護系及び計測制御系の伝送ラインを共有する場合、通信をつかさどる制御装置は発信側システムの装置とすること。	【規制要求変更なし】 安全保護系計器ラックは、計測制御系とは分離した設計とする。 計測制御系へ信号を取り出す場合には、計測制御系に故障が生じても、安全保護系計器ラックへ影響を与えない設計としている。
（５）JEAC4620の４．１６の「外部からの影響を防止し得る設計」を「外部影響の防止された設備」と読み替えること。	【規制要求変更なし】 安全保護系計器ラックは、外部のネットワークに直接接続しない設計としている。

新規制基準の項目	適合状況
（６）JEAC4620の４．における安全保護機能に相応した高い信頼性を有するとは、デジタル安全保護系のトリップ失敗確率及び誤トリップする頻度を評価し、従来型のものと比較して同等以下とすること。また、デジタル安全保護系の信頼性評価において、ハードウェア構成要素に異常の検出、検出信号の伝送、入出力信号の処理、演算処理、トリップ信号の伝送、トリップの作動等、評価に必要な構成要素を含むこと。	【規制要求変更なし】 デジタル計算機を適用した安全保護系計器ラックを含む安全保護系のトリップが失敗する確率及び誤トリップする頻度は、必要なハードウェア構成要素について評価を行い、従来設備に比べて同等以下であることを確認している。
（７）安全保護系に用いられるデジタル計算機の健全性を実証できない場合、安全保護機能の遂行を担保するための原理の異なる手段を別途用意すること。（「日本電気協会「安全保護系へのディジタル計算機の適用に関する規程（JEAC 4620-2008）」及び「ディジタル安全保護系の検証及び妥当性確認に関する指針（JEAG 4609-2008）」に関する技術評価書」（平成２３年１月原子力安全・保安院、原子力安全基盤機構取りまとめ））	【規制要求変更なし】 安全保護系計器ラックは、JEAC 4620に基づき品質を確保しており、健全性は実証されている。

2．安全保護系に適用するデジタル計算機の検証及び妥当性確認について

（1）検証及び妥当性確認の概要

安全保護系へのデジタル計算機の適用に当たっては、ソフトウェアの品質を確保することが重要であり、安全保護系としての機能を実現するソフトウェアに対して、設計、製作、試験、変更の各段階において、安全保護上要求される機能が正しく確実に実現されていることを保証する活動として検証及び妥当性確認（V＆V）を行う。

検証は、設計、製作過程のステップごとに上位仕様と下位仕様の整合性チェックを主体として、以下の観点から検証作業を行う。

a．安全保護系システム要求事項がシステム設計要求仕様に正しく反映されていること。

b．システム設計要求仕様がハードウェア、ソフトウェアの設計要求仕様に正しく反映されていること。

c．上記設計要求仕様に基づいてソフトウェアが製作されていること。

d．検証及び妥当性確認が可能なソフトウェアとなっていること。

必要な検証を経て製作されたソフトウェアをハードウェアと統合した後の全体システムについて、最終的に安全保護系システム要求事項が正しく実現されていることの確認をするために、妥当性確認を行う。

（2）検証と妥当性確認の手順と内容

以下に、検証と妥当性確認の手順と内容を示し、第1図に安全保護系に適用するデジタル計算機の設計・製作及び検証と妥当性確認の流れを示す。

検　証　1：安全保護系システム要求事項が正しくシステム設計要求仕様に反映されていることを検証する。

検　証　2：システム設計要求仕様が正しくハードウェア・ソフトウェア設計要求仕様に反映されていることを検証する。

検証3，4：ソフトウェア設計要求仕様どおりに正しくソフトウェアが製作されていることを検証する。ソフトウェア設計要求仕様図書から自動的にソフトウェアを製作するツールを適用し、ソフトウェアの設計と製作を一体化するため、検証3と検証4は統合する。

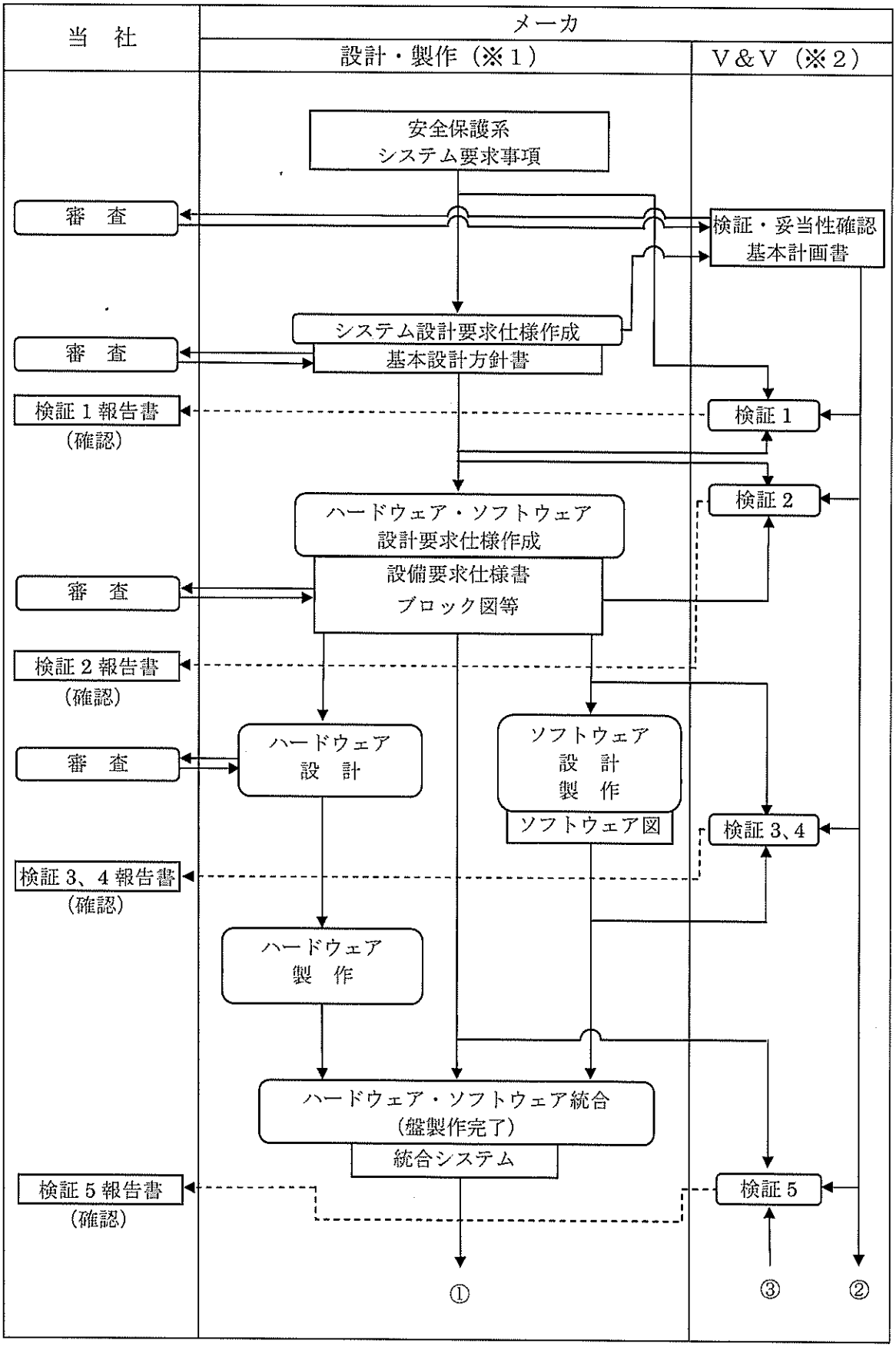
検　証　5：ハードウェアとソフトウェアを統合してハードウェア・ソフトウェア設計要求仕様どおりのシステムとなっていることを検証する。

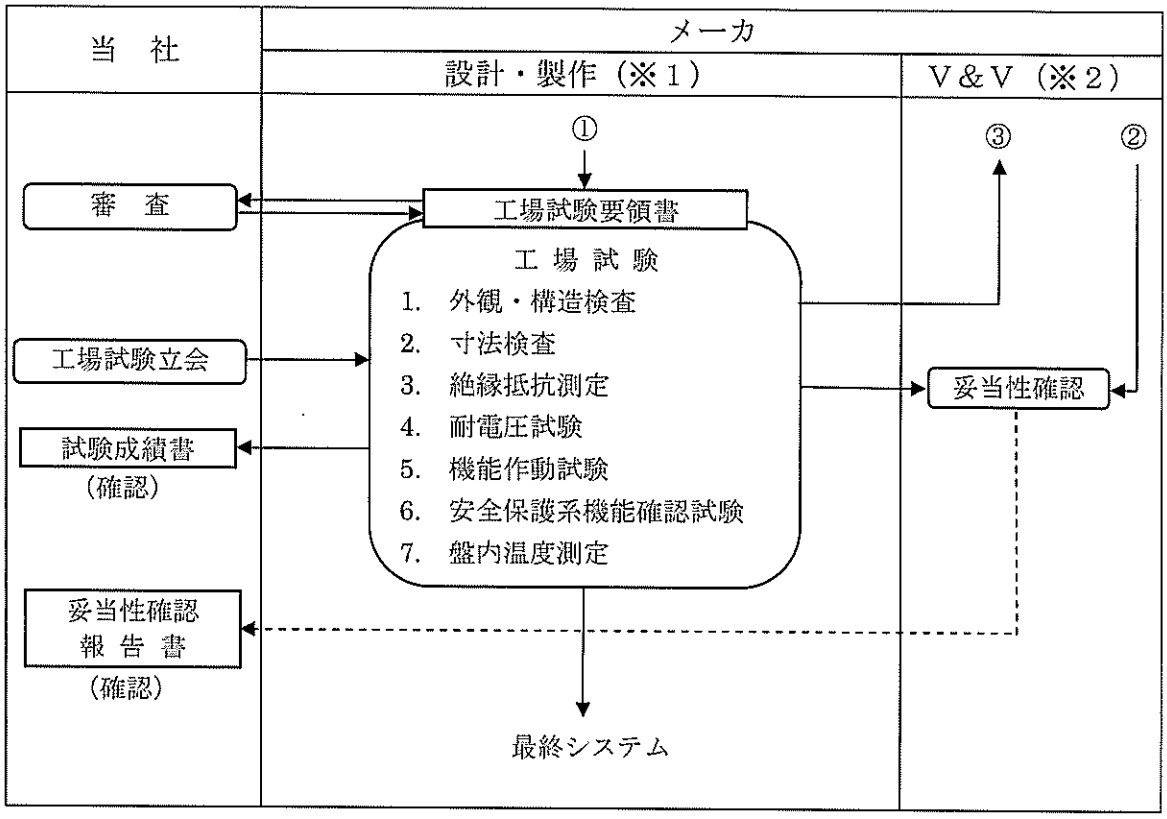
妥当性確認：ハードウェアとソフトウェアを統合して検証されたシステムが、安全保護系システム要求事項を満足していることを確認する。

（3）変更管理

設計要求仕様の変更及びソフトウェアの変更に関する管理方法は手順に定めており、適切な管理のもとに変更を行う。変更を行う場合は、変更理由、変更箇所を文書化し、変更の影響範囲を明確にした上で、変更を実施する。必要に応じ、変更箇所及び変更を受ける部分について検証及び妥当性確認作業を再度実施する。

第１図　安全保護系に適用するデジタル計算機の設計・製作及び検証と妥当性確認の流れ





（※１）設計・製作は「原子力発電所における安全のための品質保証規程」（JEAC 4111）に準拠して、品質保証活動を行う。

（※２）安全保護系に適用するデジタル計算機のソフトウェアの検証及び妥当性確認（Ｖ＆Ｖ）は、「ディジタル安全保護系の検証及び妥当性確認に関する指針」（JEAG 4609）に準拠して行う。