資料1

伊方発電所3号機
安全保護系ロジック盤の取替えに伴う
デジタル安全保護系への変更工事に係る
設計及び工事計画認可申請の概要について

令和２年１０月２０日

四国電力株式会社

本資料のうち、枠囲みの内容は、商業機密あるいは防護上の観点から公開できません。

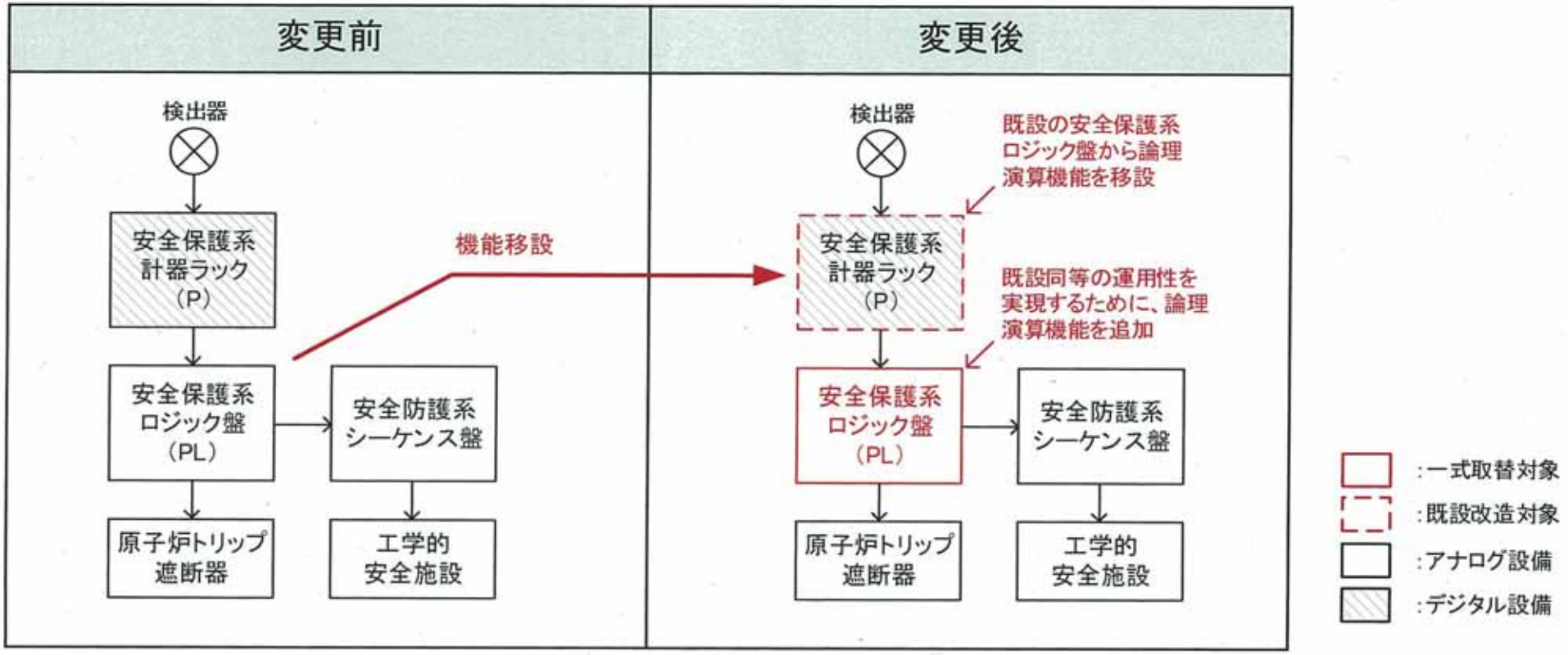
目 次

1. デジタル安全保護系への変更工事の概要(1／11)

(1)目的

伊方3号機において、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とし、現在、安全保護系ロジック盤が担っている、パラメータに対する論理演算機能について、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。

また、変更後においても既設同等の運用性を実現するために、原子炉トリップ遮断器の誤動作、及び工学的安全施設作動設備の不動作を防止するための論理演算機能を有する安全保護系ロジック盤を設ける。



1. デジタル安全保護系への変更工事の概要(2／11)

(2)工事概要

- ✓ 既設の安全保護系ロジック盤は、安全保護系計器ラックにおけるパラメータの設定値比較結果を入力信号とし、2 out of 4などの論理演算を実施し、原子炉トリップ信号及び工学的安全施設作動信号を出力する。

- ✓ 既設の安全保護系ロジック盤には、アナログ集積回路等の電子部品が使用されているが、現在、これら電子部品が入手困難となっていることから、安全保護系ロジック盤が有する論理演算機能について、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で実現する。

- ✓ 変更前において、設定値比較機能のみを有している安全保護系計器ラックは、既設の安全保護系ロジック盤の機能を移設することによって、設定値比較機能及び論理演算機能を有することになり、安全保護系計器ラックが担う機能の範囲が拡大する。

- ✓ 変更前では、安全保護系計器ラックの1チャンネルの誤動作故障時においても、原子炉トリップ遮断器は動作(開放)せず、また、1チャンネルの不動作故障時においても、工学的安全施設作動設備は不動作にならない。

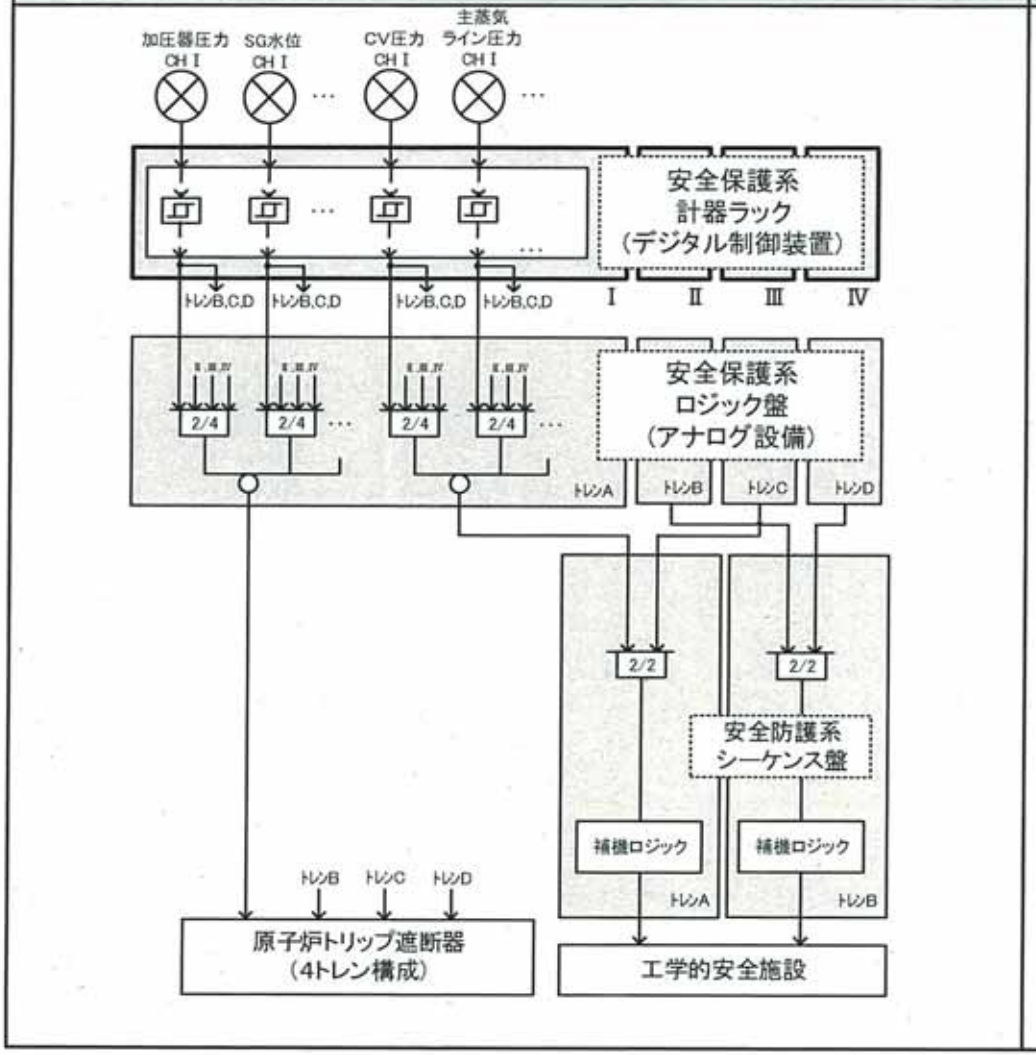
- ✓ 変更後において、安全保護系計器ラックの1チャンネルの誤動作故障及び不動作故障時においても、既設と同じ動作(原子炉トリップ遮断器の誤動作防止、工学的安全施設作動設備の不動作防止)するために、新たに簡素なアナログ部品で構成される安全保護系ロジック盤を設置し、4つある安全保護系計器ラックのうち2チャンネル以上からこれら信号が発信されていることを判定する論理演算を行う必要がある。

変更後の設備構成について、それぞれ説明を行う。
(3)原子炉保護設備　6 ～ 8　、(4)工学的安全施設作動設備　9 ～ 11

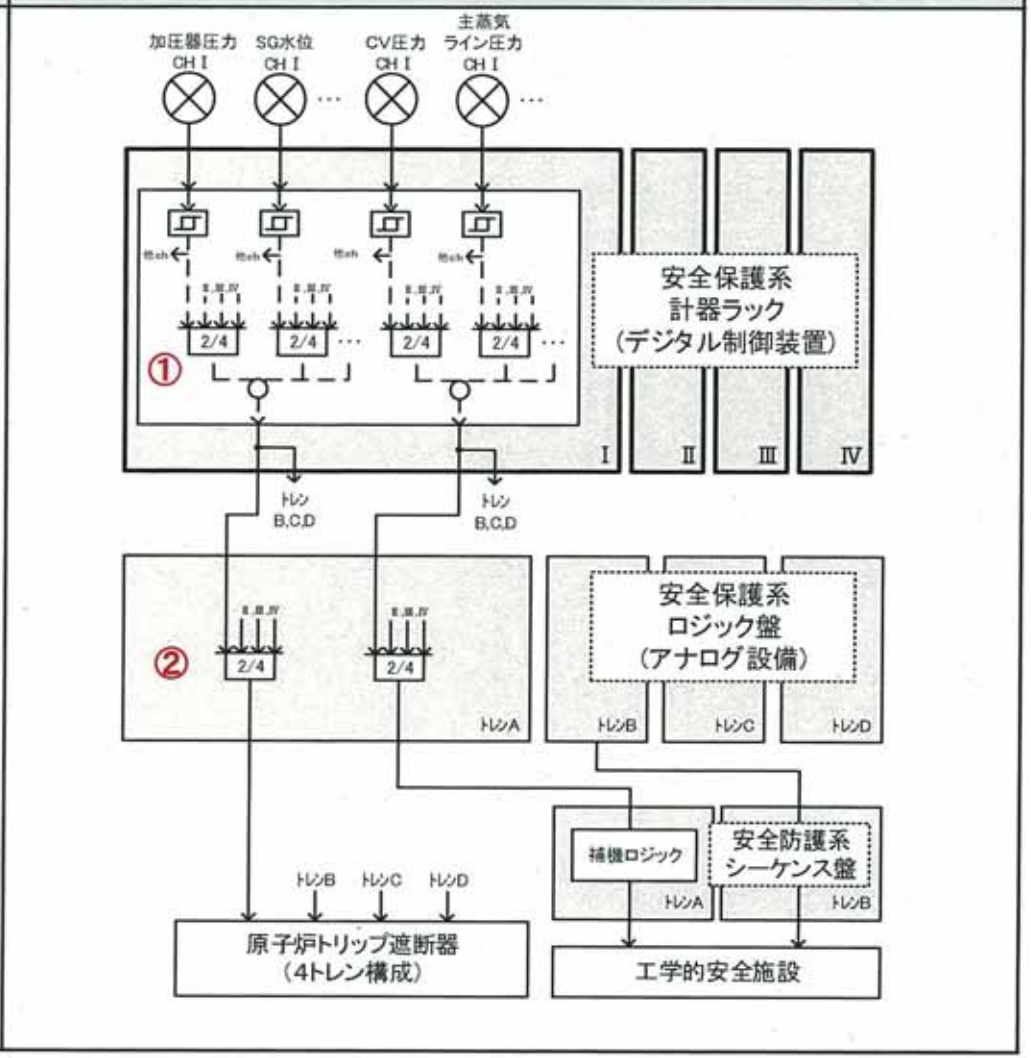
1. デジタル安全保護系への変更工事の概要(3／11)

(3)全体システム構成の概略

変更前



変更後



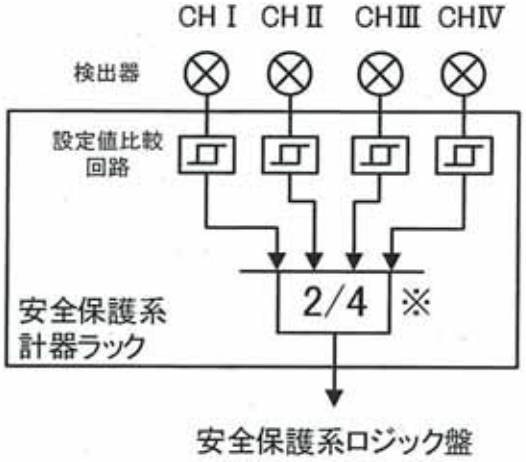
--- : CPU内または通信
—— : ハードワイヤード
[◻] : 設定値比較回路
[2/4] : 論理回路 (2 out of 4 の例)
▭ : デジタル制御装置
▭ : ハードウェア回路

1. デジタル安全保護系への変更工事の概要(4／11)

(4)各部の論理演算機能

【安全保護系計器ラックの論理演算機能】 前頁①

4つの検出器のうち、2つ以上が原子炉トリップ信号又は工学的安全施設作動信号の設定値に達しているかの判定を行う。

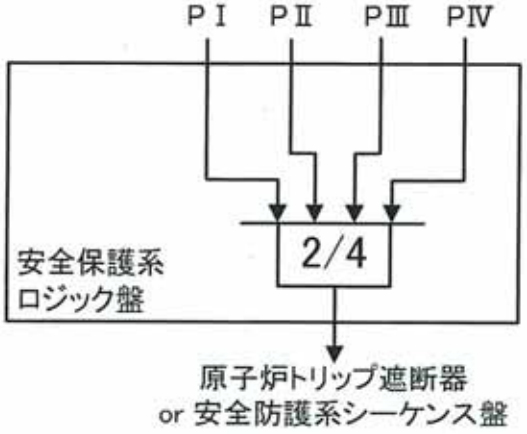


CH:チャンネル

※ 論理回路は、パラメータ毎に設けられ、パラメータにより、2/4以外のロジックもある。

【安全保護系ロジック盤の論理演算機能】 前頁②

全4チャンネルの安全保護系計器ラックのうち、2つ以上から原子炉トリップ信号又は工学的安全施設作動信号が発信されているかの判定を行う。

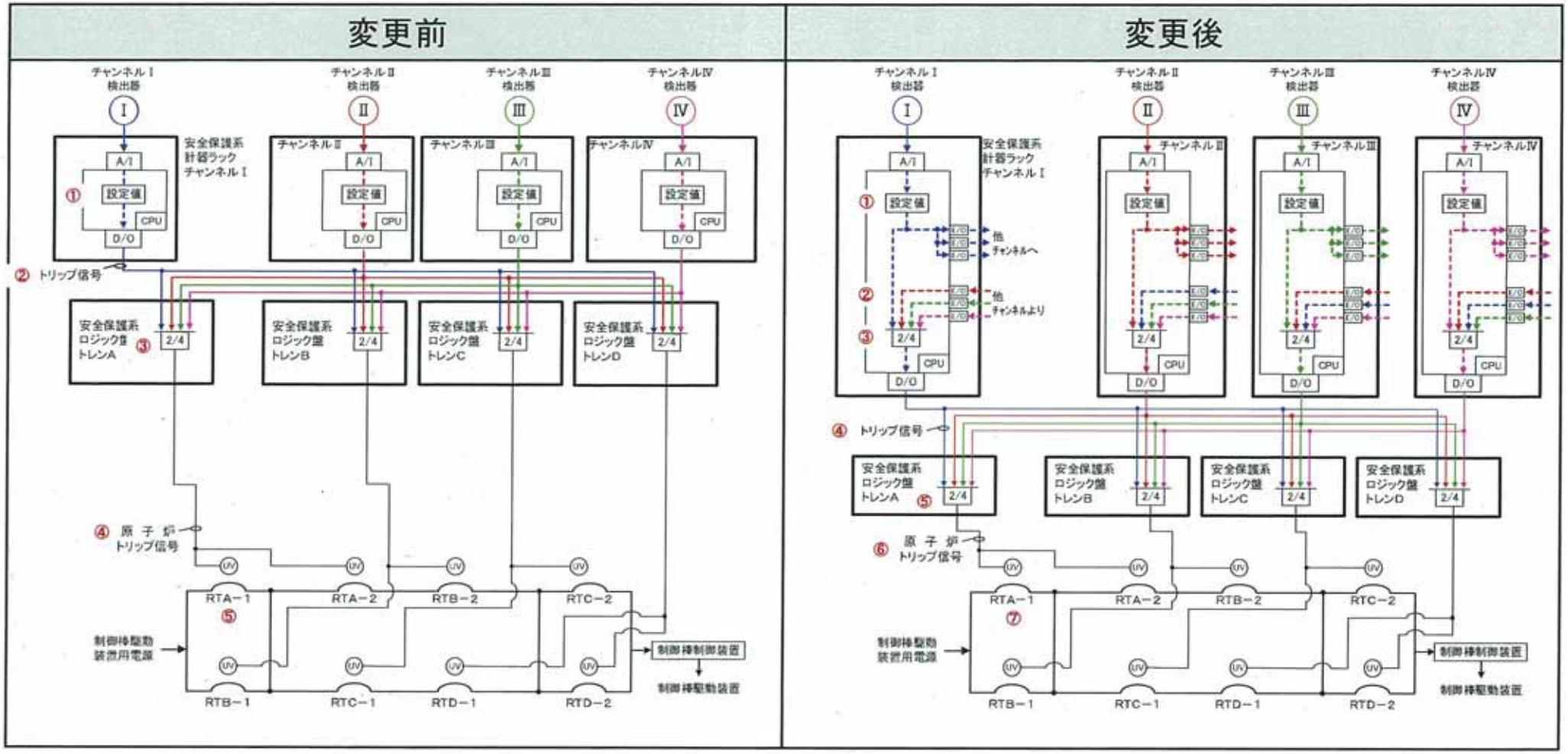


P:安全保護系計器ラック

1. デジタル安全保護系への変更工事の概要(5／11)

(5)原子炉保護設備

○システム構成比較



A/I：アナログ信号入力部
CPU：マイクロプロセッサ部
D/O：接点信号出力部
E/O：電気/光変換部
－－：CPU内または通信
——：ハードワイヤード
UV：不足電圧コイル
RTA, RTB, RTC, RTD：原子炉トリップ遮断器

：デジタル制御装置
：ハードウェア回路

1. デジタル安全保護系への変更工事の概要(6／11)

(5)原子炉保護設備(続き)

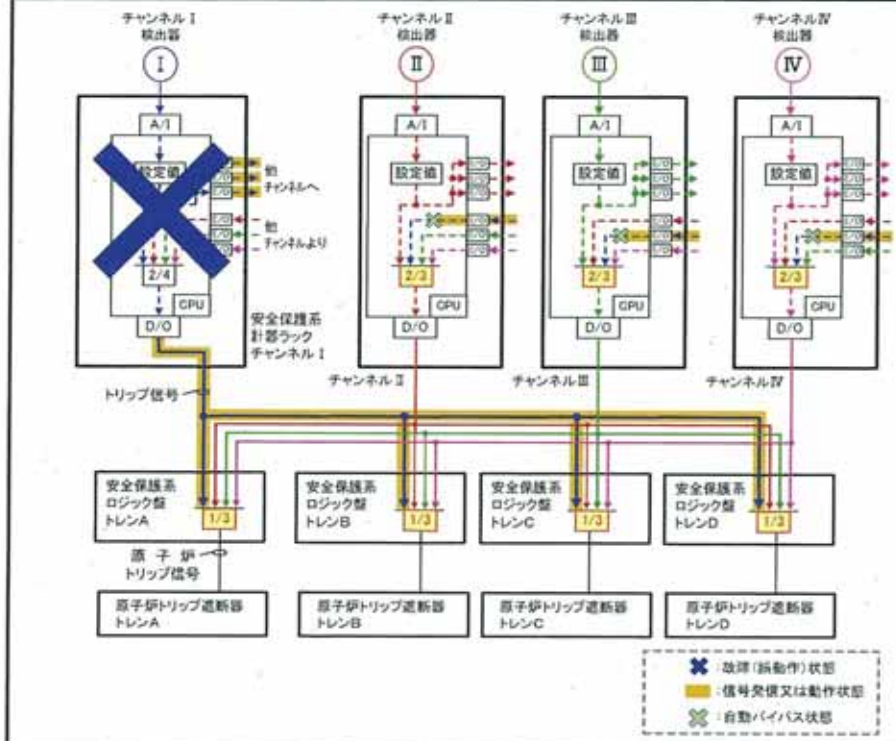
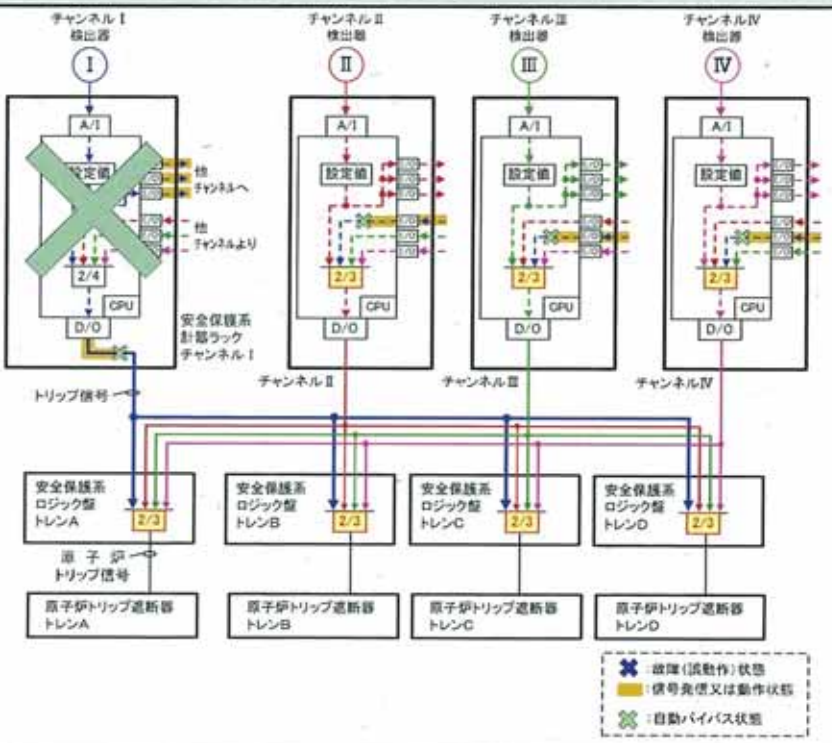
○機能比較

変更前		変更後	
制御盤	機　能	制御盤	機　能
安全保護系計器ラック Ⅰ～Ⅳ (4チャンネル)	①プロセス信号を受け、作動設定値との比較演算を行う。 ②作動設定値の比較演算の結果、作動設定値に達したチャンネルは、安全保護系ロジック盤にトリップ信号を発信する。	安全保護系計器ラック Ⅰ～Ⅳ (4チャンネル)	①プロセス信号を受け、作動設定値との比較演算を行う。 ②作動設定値の比較演算の結果、作動設定値に達したチャンネルは、4チャンネルすべてにトリップ信号を発信する。
安全保護系ロジック盤 A～D (4トレン)	**③安全保護系計器ラックからのトリップ信号を集約し、論理演算(2/4等)を行う。** ④論理演算の結果、作動条件が成立した場合に、原子炉トリップ遮断器に原子炉トリップ信号を発信する。		**③チャンネルからのトリップ信号を受け、論理演算(2/4等)を行う。** ④論理演算の結果、作動条件が成立した場合には、安全保護系ロジック盤にトリップ信号を発信する。
		安全保護系ロジック盤 A～D (4トレン)	**⑤安全保護系計器ラックからトリップ信号を集約し、論理演算(2/4)を行う。** ⑥論理演算の結果、作動条件が成立した場合には、原子炉トリップ遮断器に原子炉トリップ信号を発信する。
原子炉トリップ遮断器 (4トレン)	⑤原子炉トリップ信号を受け、原子炉トリップ遮断器を開放する。	原子炉トリップ遮断器 (4トレン)	⑦原子炉トリップ信号を受け、原子炉トリップ遮断器を開放する。

1. デジタル安全保護系への変更工事の概要(7／11)

(5)原子炉保護設備(続き)

○誤動作故障に対する運用性向上

故障時(誤動作)	バイパス時
	
原子炉トリップ信号の信号状態： 1／3	原子炉トリップ信号の信号状態： 2／3
安全保護系計器ラックのマイクロプロセッサ等の故障に伴う誤動作時に、故障したチャンネルからトリップ信号が発信され、すべての安全保護系ロジック盤の論理回路の状態が1/3となる。	故障した安全保護系計器ラックを系統から除外(バイパス)することによって、残りの健全な安全保護系計器ラック及びすべての安全保護系ロジック盤の論理回路の状態は2/3になり、2チャンネルのトリップ信号によって、原子炉トリップ信号を発信する状態に復帰する。

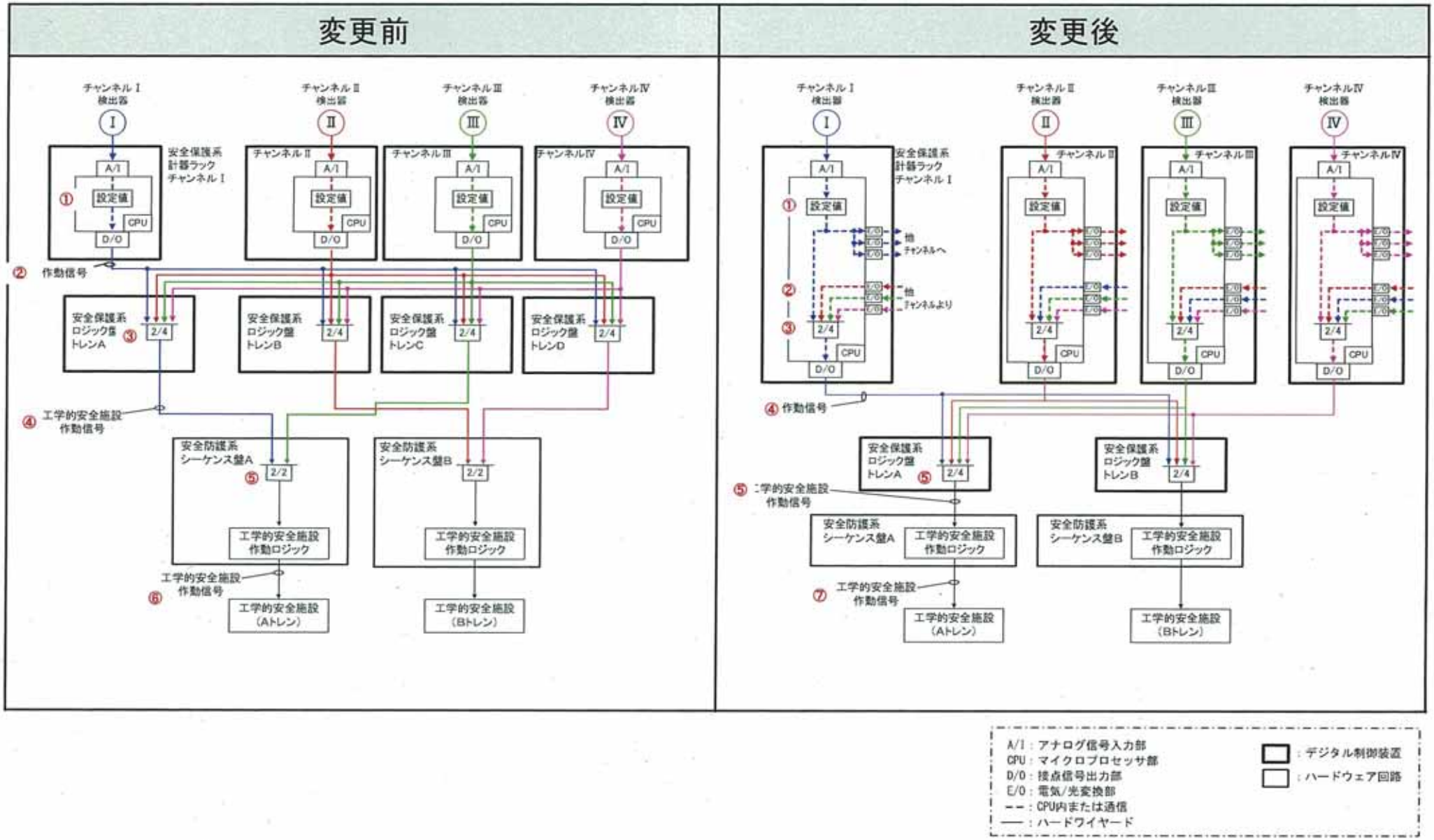
バイパス

安全保護系ロジック盤を設けることで、原子炉トリップ遮断器は動作(開放)しない。また、故障チャンネルのバイパスにより、2チャンネル以上の信号で原子炉トリップする通常状態に復帰できる。

1. デジタル安全保護系への変更工事の概要(8／11)

(6)工学的安全施設作動設備

○システム構成比較



1. デジタル安全保護系への変更工事の概要(9／11)

(6)工学的安全施設作動設備(続き)

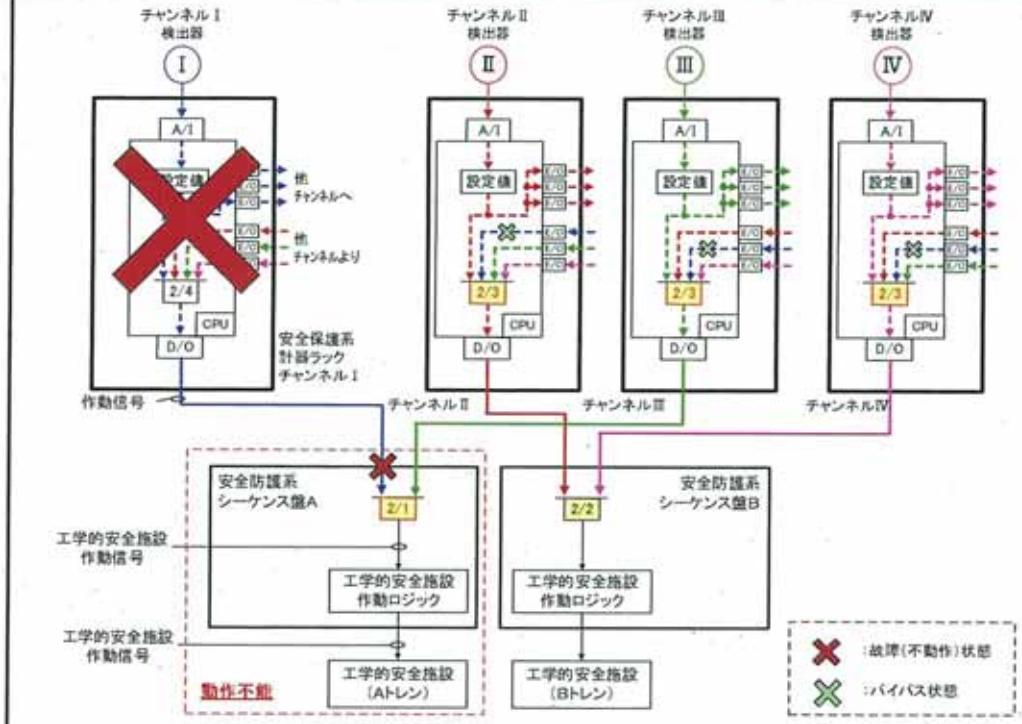
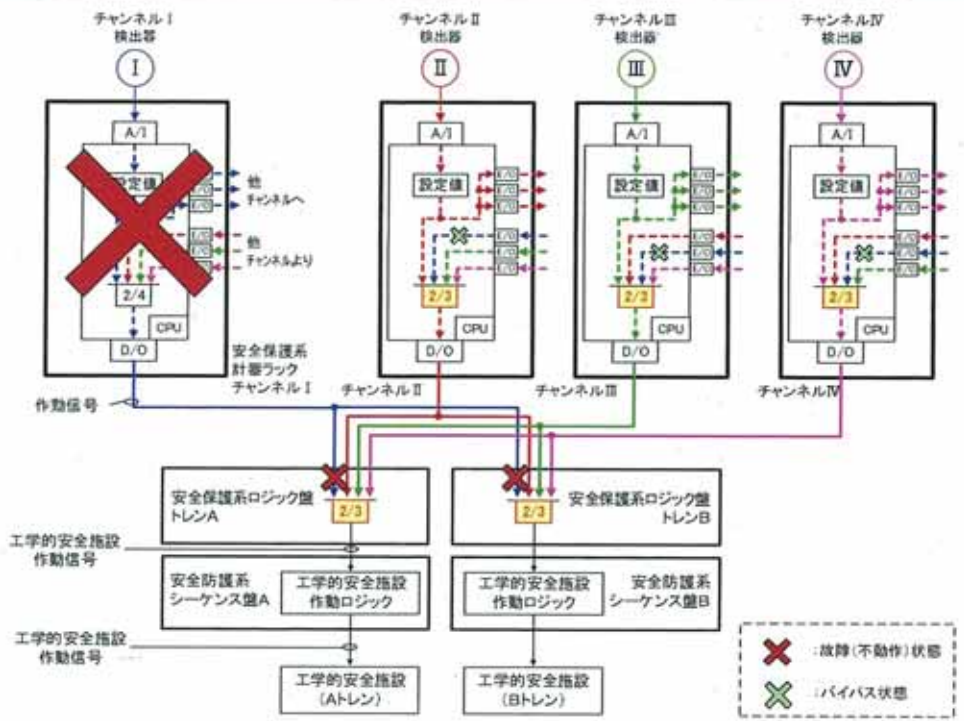
○機能比較

変更前		変更後	
制御盤	機　能	制御盤	機　能
安全保護系計器ラック Ⅰ～Ⅳ (4チャンネル)	①プロセス信号を受け、作動設定値との比較演算を行う。 ②作動設定値の比較演算の結果、作動設定値に達したチャンネルは、安全保護系ロジック盤にトリップ信号を発信する。	安全保護系計器ラック Ⅰ～Ⅳ (4チャンネル)	①プロセス信号を受け、作動設定値との比較演算を行う。 ②作動設定値の比較演算の結果、作動設定値に達したチャンネルは、4チャンネルすべてにトリップ信号を発信する。
安全保護系ロジック盤 A～D (4トレン)	**③安全保護系計器ラックからの作動信号を集約し、論理演算(2/4等)を行う。** ④論理演算の結果、作動条件が成立した場合に、安全防護系シーケンス盤に工学的安全施設作動信号を発信する。		**③チャンネルからの作動信号を受け、論理演算(2/4等)を行う。** ④論理演算の結果、作動条件が成立した場合には、安全保護系ロジック盤に作動信号を発信する。
安全防護系シーケンス盤 A,B(2トレン)	**⑤トレン毎の安全保護系ロジック盤からの作動信号を集約し、論理演算(2/2)を行う。**	安全保護系ロジック盤 A～D (4トレン)	**⑤安全保護系計器ラックから作動信号を集約し、論理演算(2/4)を行う。** ⑥論理演算の結果、作動条件が成立した場合に、安全防護系シーケンス盤に工学的安全施設作動信号を発信する。
	⑥論理演算の結果、作動条件が成立した場合には、工学的安全施設の作動ロジックに従い、工学的安全施設作動信号を発信する。	安全防護系シーケンス盤 A,B(2トレン)	⑦工学的安全施設の作動ロジックに従い、工学的安全施設作動信号を発信する。

1. デジタル安全保護系への変更工事の概要（10／11）

（6）工学的安全施設作動設備（続き）

○不動作故障に対する運用性向上

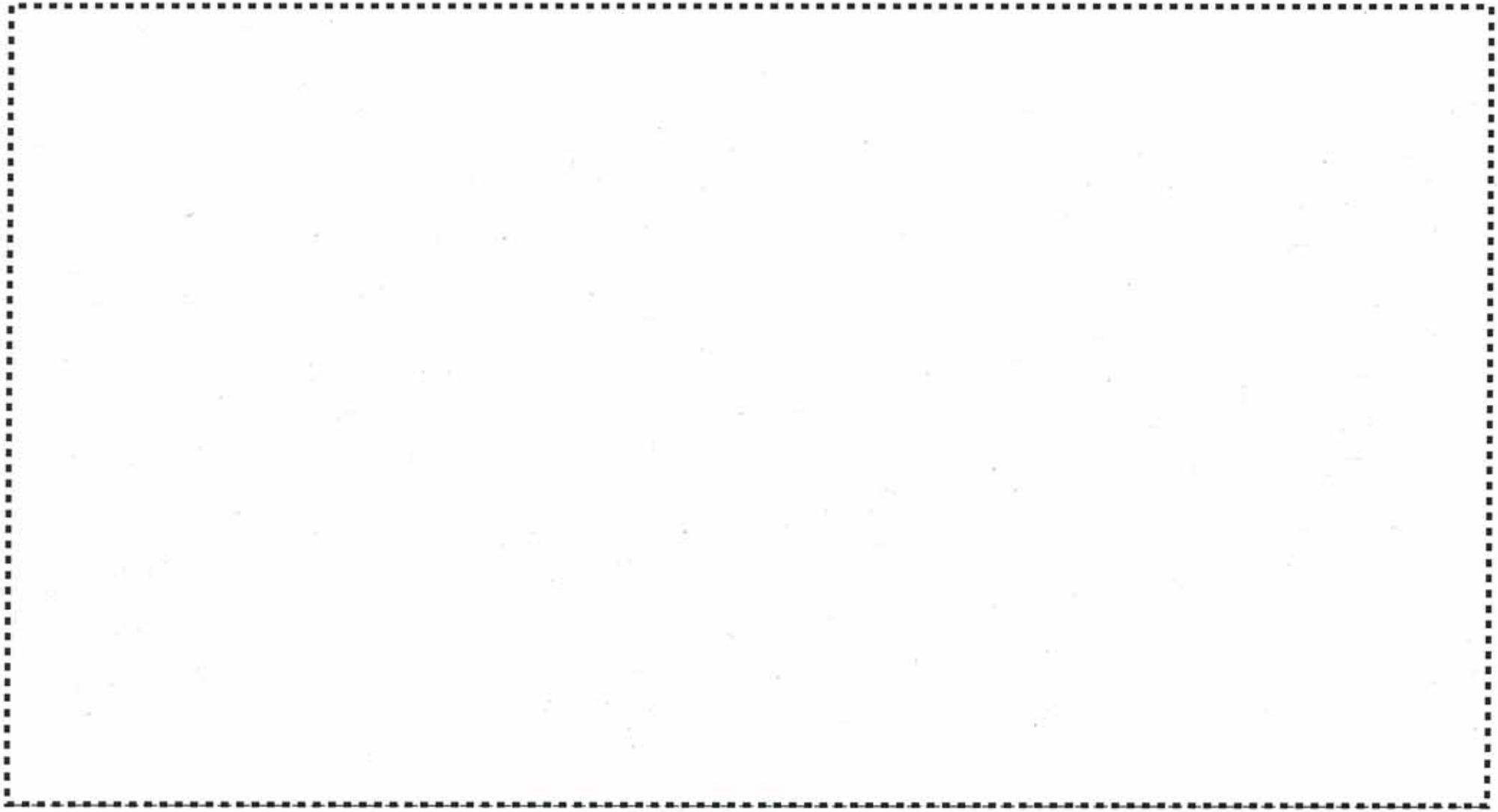
安全保護系ロジック盤を設けない（2/2ロジックの）場合	安全保護系ロジック盤を設けた（2/4ロジックに変更した）場合
	
安全保護系計器ラックの故障により1つのチャンネルが不動作となった場合、安全防護系シーケンス盤の2/2ロジックが実質2/1ロジックとなり、残りの健全なチャンネル（図ではチャンネルⅢ）が動作してもロジックが成立しなくなることから、片トレンの工学的安全施設作動設備が動作不能となる。	安全保護系計器ラックの故障により1つのチャンネルが不動作となった場合、安全防護系シーケンス盤の2/4ロジックが実質2/3ロジックとなり、残りの健全なチャンネルのうち2チャンネルが動作すれば、安全防護系ロジック盤のロジックが成立することから、**両トレンの工学的安全施設作動設備を維持することができる。**

安全保護系ロジック盤を設けた場合、安全防護系シーケンス盤にて実現していた2/2ロジックを2/4ロジックに変更することができる。変更後は、安全保護系計器ラックの単一故障（不動作故障）を想定した場合、両トレンの工学的安全施設作動設備を維持することができる。

1. デジタル安全保護系への変更工事の概要(11／11)

(7)設置場所

本工事において、取替えを行う安全保護系ロジック盤、及び改造を行う安全保護系計器ラックの設置場所に変更はない。



原子炉補助建屋　EL.17.0m

2. 設計及び工事計画認可申請の概要(1／7)

(1)設計及び工事計画認可申請書 本文の変更事項(1/4)

安全保護系について、デジタル制御装置を適用したデジタル安全保護系への変更を行うことで、安全保護系の論理演算機能のうち、原子炉非常停止信号及び工学的安全施設作動信号の論理回路のデジタル化を実施することから、以下の対応を行う。

① 計測制御系統施設の要目表
1．制御方式及び制御方法
(2)発電用原子炉の制御方法
ｄ． 安全保護系等の制御方法
について、「(a)安全保護系の制御方法」に、マイクロプロセッサを用いたデジタル制御装置を用いる記載を追加する。

② 計測制御系統施設の基本設計方針
基本設計方針のうち、安全保護系の論理演算機能に係る記載について、アナログ回路に加えてデジタル回路を用いる記載を追加する。

2. 設計及び工事計画認可申請の概要(2／7)

(1)設計及び工事計画認可申請書 本文の変更事項(2/4)

計測制御系統施設

1 制御方式及び制御方法

(2) 発電用原子炉の制御方法

d 安全保護系等の制御方法

(a)安全保護系の制御方法

イ 原子炉非常停止信号による原子炉非常停止機能

原子炉非常停止信号の作動回路は多重チャンネル構成で"2 out of 4"方式などの論理回路及び原子炉トリップ遮断器で構成され、原子炉非常停止を行う。

原子炉非常停止信号の検出部及び論理回路部は、検出部又は論理回路部の駆動源喪失等が生じた場合において、原子炉非常停止信号を発信するとともに、警報を中央制御室に表示する。

原子炉非常停止信号の論理回路は、マイクロプロセッサを用いたデジタル制御装置を適用し、検証及びハードウェアと統合されたシステムに対する妥当性確認を行ったソフトウェアを使用する。

原子炉非常停止信号の作動回路		
種　　類		マイクロプロセッサを用いたデジタル制御装置
演算処理方式		シングルタスク方式
デジタル制御装置の個数		論理回路：4
自己診断		マイクロプロセッサの停止、通信の遮断等を早期に検知し、警報を発信するとともに、保護機能喪失の場合は当該チャンネルをトリップ状態とする
環境条件	温　　度	0～50℃
	湿　　度	10～95%RH
	放射線量	放射線の影響のないこと（非管理区域に設置）
応答時間		[redacted]秒以下 プロセス信号がデジタル制御装置に入力されてから、原子炉非常停止信号が原子炉トリップ遮断器へ出力されるまで。ただし、チャンネル間データ通信を行わない原子炉非常停止信号は、[redacted]秒以下
データ通信		計測制御系と電気的及び機能的に分離
外部ネットワークとの遮断		外部ネットワークへの直接接続なし

※下線部及び表は、今回の設工認可申請で変更(追記)する箇所

2. 設計及び工事計画認可申請の概要(3／7)

(1)設計及び工事計画認可申請書 本文の変更事項(3/4)

計測制御系統施設

1 制御方式及び制御方法

(2) 発電用原子炉の制御方法

d 安全保護系等の制御方法

(a)安全保護系の制御方法

ロ 工学的安全施設作動信号による工学的安全施設の作動機能

工学的安全施設作動信号の作動回路は多重チャンネル構成で"2 out of 4"方式などの論理回路及び作動装置で構成され、工学的安全施設を起動させる。

工学的安全施設作動信号の検出部は駆動源の喪失が生じた場合において、フェイル・セーフとなり、工学的安全施設作動信号が発信する。ただし、一部の検出部※及び論理回路部は、駆動源の喪失が生じた場合において、工学的安全施設作動信号を作動させず原子炉施設への安全上の支障がない状態を維持する設計(フェイル・アズ・イズ)とし、駆動源が喪失したことを運転員が確実に認知できるよう中央制御室に警報を表示する。なお、単一チャンネルの駆動源が喪失した場合においても、残りのチャンネルによって安全保護系の機能は確保される。

工学的安全施設作動信号の論理回路は、マイクロプロセッサを用いたデジタル制御装置を適用し、検証及びハードウェアと統合されたシステムに対する妥当性確認を行ったソフトウェアを使用する。

※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)を指す。

工学的安全施設作動信号の作動回路		
種　　類		マイクロプロセッサを用いたデジタル制御装置
演算処理方式		シングルタスク方式
デジタル制御装置の個数		論理回路：4
自己診断		マイクロプロセッサの停止、通信の遮断等を早期に検知し、警報を発信するとともに、異常な信号を出力しないようにする
環境条件	温　　度	0～50℃
	湿　　度	10～95%RH
	放射線量	放射線の影響のないこと（非管理区域に設置）
応答時間		[redacted]秒以下 （プロセス信号がデジタル制御装置に入力されてから、工学的安全施設作動信号が出力されるまで）
データ通信		計測制御系と電気的及び機能的に分離
外部ネットワークとの遮断		外部ネットワークへの直接接続なし

※下線部及び表は、今回の設工認可申請で変更(追記)する箇所

2. 設計及び工事計画認可申請の概要(4／7)

(1)設計及び工事計画認可申請書 本文の変更事項(4/4)

計測制御系統施設

10 計測制御系統施設(発電用原子炉の運転を管理するための制御装置を除く。)の基本設計方針、適用基準及び適用規格

(1) 基本設計方針

1.3 安全保護装置等
1.3.1 安全保護装置
(1) 安全保護装置の機能及び構成

(2) 安全保護装置の不正アクセス行為等の被害の防止

安全保護装置は、外部ネットワークと物理的分離及び機能的分離、外部ネットワークからの遠隔操作の防止、ソフトウェアの内部管理の強化によるウイルス等の侵入の防止、物理的及び電気的アクセスの制限、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で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できる設計とするとともに安全保護装置の論理演算機能(作動(起動)回路)については、デジタル回路及びアナログ回路で構成する設計とする。

安全保護装置が収納された盤の施錠等により、ハードウェアを直接接続させない措置を実施すること及び安全保護装置のソフトウェアは設計、製作、試験及び変更管理の各段階で検証と妥当性の確認を適切に行うことで不正アクセスを防止する。

※下線部は、今回の設工認可申請で変更(追記)する箇所

2. 設計及び工事計画認可申請の概要(5／7)

(1)設計及び工事計画認可申請書 添付資料

実用炉規則 別表第二 に基づく添付資料は以下のとおりである。

資料名称	説明概要
発電用原子炉の設置の許可との整合性に関する説明書	本工事が設置許可に従ったものであることを示す。
安全設備及び重大事故等対処設備が使用される条件の下における健全性に関する説明書	本工事で改造を行う安全保護系計器ラック及び取替えを行う安全保護系ロジック盤が使用される条件の下における健全性について示す。
発電用原子炉施設の火災防護に関する説明書	本工事で取替えを行う安全保護系ロジック盤が火災区域及び火災区画に対して、火災発生防止を考慮した火災防護対策を講じることを示す。
発電用原子炉施設の溢水防護に関する説明書	本工事で取替えを行う安全保護系ロジック盤が溢水防護に係る評価について影響を及ぼさないことを示す。
耐震性に関する説明書	本工事で取替えを行う安全保護系ロジック盤が耐震Sクラス設備として耐震機能を有することを示す。
計測装置の構成に関する説明書並びに計測範囲及び警報動作範囲に関する説明書	本工事で改造を行う安全保護系計器ラック及び取替えを行う安全保護系ロジック盤が安全保護装置として不正アクセス等の被害防止に必要な措置を講じるものであることを示す。
デジタル制御方式を使用する安全保護系等の適用に関する説明書	本工事で適用するデジタル安全保護系について、原子炉保護設備及び工学的安全施設作動設備の構成及び設計方針が安全保護装置として適合していることを示す。
設計及び工事に係る品質マネジメントシステムに関する説明書	本工事計画に係る設計等の品質管理の実績・計画について説明し、「実用発電用原子炉に係る発電用原子炉設置者の設計及び工事に係る品質管理の方法及びその検査のための組織の技術基準に関する規則」に適合していることを示す。

2. 設計及び工事計画認可申請の概要(6／7)

(3)設計方針の概要

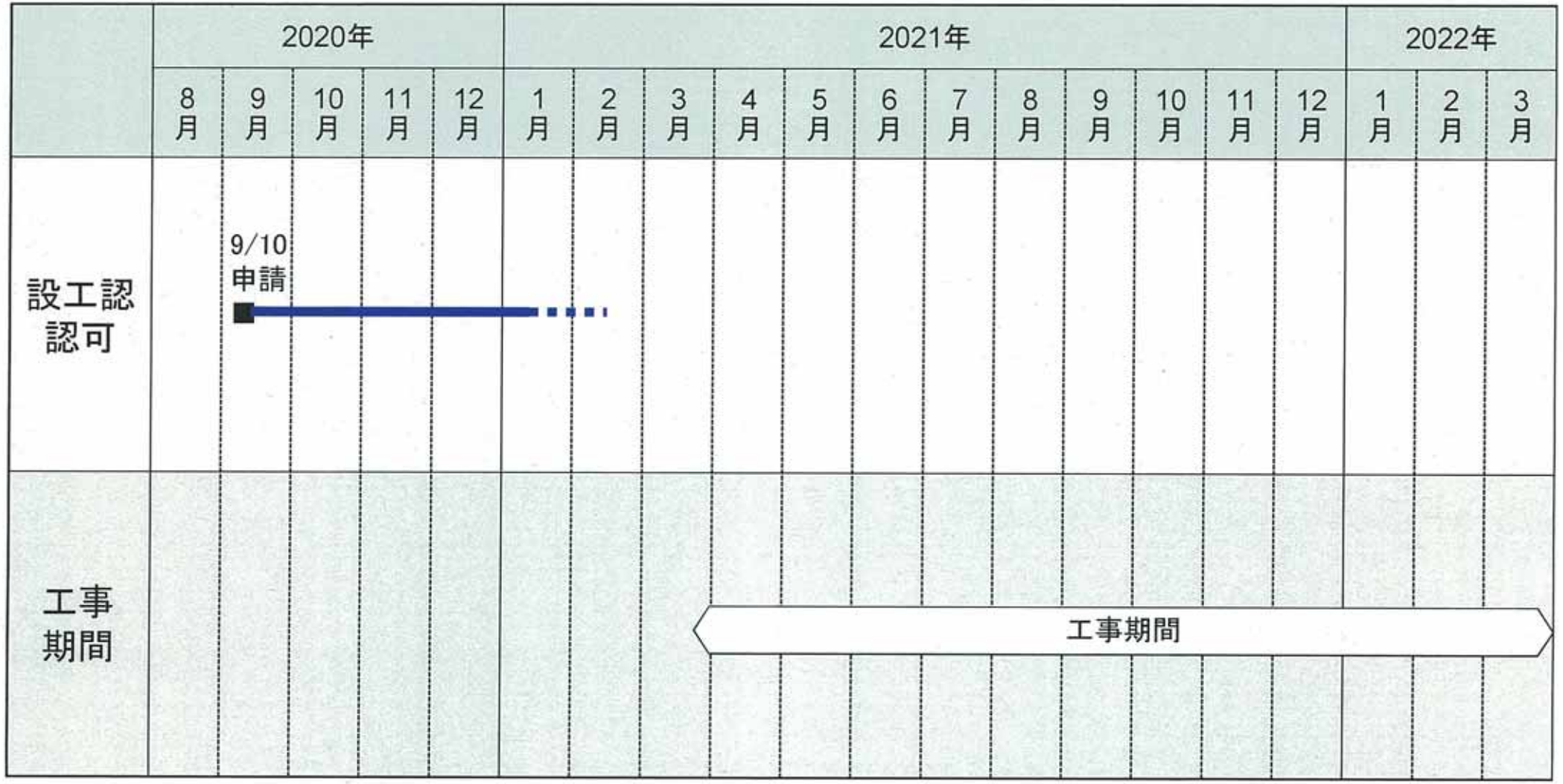
技術基準規則(解釈含む)への適合のための設計方針を下表に示す。

条　文	適合するための設計方針	添付資料
第5条　地震による損傷の防止 第11条　火災による損傷の防止 第12条　溢水等による損傷の防止 第14条　安全設備 第15条　設計基準対象施設の機能	既工事計画における基本方針に変更はなく、各条文に適合するよう設計する。	耐震性に関する説明書 発電用原子炉施設の火災防護に関する説明書 発電用原子炉施設の溢水防護に関する説明書 安全設備及び重大事故等対処設備が使用される条件の下における健全性に関する説明書
第35条　安全保護装置	**⇒12頁以降に、技術基準規則への適合性を図るための設計方針を示す。**	計測装置の構成に関する説明書並びに計測範囲及び警報動作範囲に関する説明書 デジタル制御方式を使用する安全保護系等の適用に関する説明書

2. 設計及び工事計画認可申請の概要(7／7)

(4)工程表

本工事は、2021年3月からを実施する計画としている。



3. 技術基準規則への適合性（1／13）

技術基準規則第35条（安全保護装置）及びその解釈に適合するための設計方針を示す。

技術基準規則	技術基準規則の解釈	設計方針
第1項 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。	第1項 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。	✓ デジタル安全保護系は、運転時の異常な過渡変化時に、その異常な状態を検知し、原子炉トリップを含む適切な系統を自動的に作動させ、燃料が許容損傷限界を超えない設計とする。 **⇒次頁にて説明する。** ✓ デジタル安全保護系は、制御棒クラスタの偶発的な連続引き抜きのような反応度制御設備のいかなる単一の誤動作に起因する急激な反応度投入が生じた場合でも、その異常な状態を検知し、原子炉トリップを含む適切な系統を自動的に作動させ、燃料が許容損傷限界を超えない設計とする。 ✓ また、デジタル安全保護系は、地震時に、その異常な状態を検知し、原子炉トリップを自動的に作動させる設計とする。

3. 技術基準規則への適合性（2／13）

デジタル制御装置を用いたデジタル安全保護系への変更後も、設置許可の安全解析で使用している安全保護設備の応答時間を満足する設計とする。

○ 原子炉トリップ信号の応答時間

信号処理回路の遅れ時間（T_2）が**最も厳しい**1次冷却材流量低及び出力領域中性子束高（高設定及び低設定）の遅れ時間を満足する設計とする。

[sec]

	検出遅れ時間（T_1）	**信号処理回路遅れ時間（T_2）**	原子炉トリップ遮断器の開放時間（T_3）	制御棒切り離し時間（T_4）	安全解析使用値（$T_1+T_2+T_3+T_4$）
1次冷却材流量低					1.0
出力領域中性子束高（高設定）					0.5
出力領域中性子束高（低設定）					0.5

○ 工学的安全施設作動信号の応答時間

信号処理回路の遅れ時間（T_2）が**最も厳しい**加圧器圧力低と加圧器水位低の一致、格納容器圧力高及び格納容器圧力異常高の遅れ時間を満足する設計とする。

[sec]

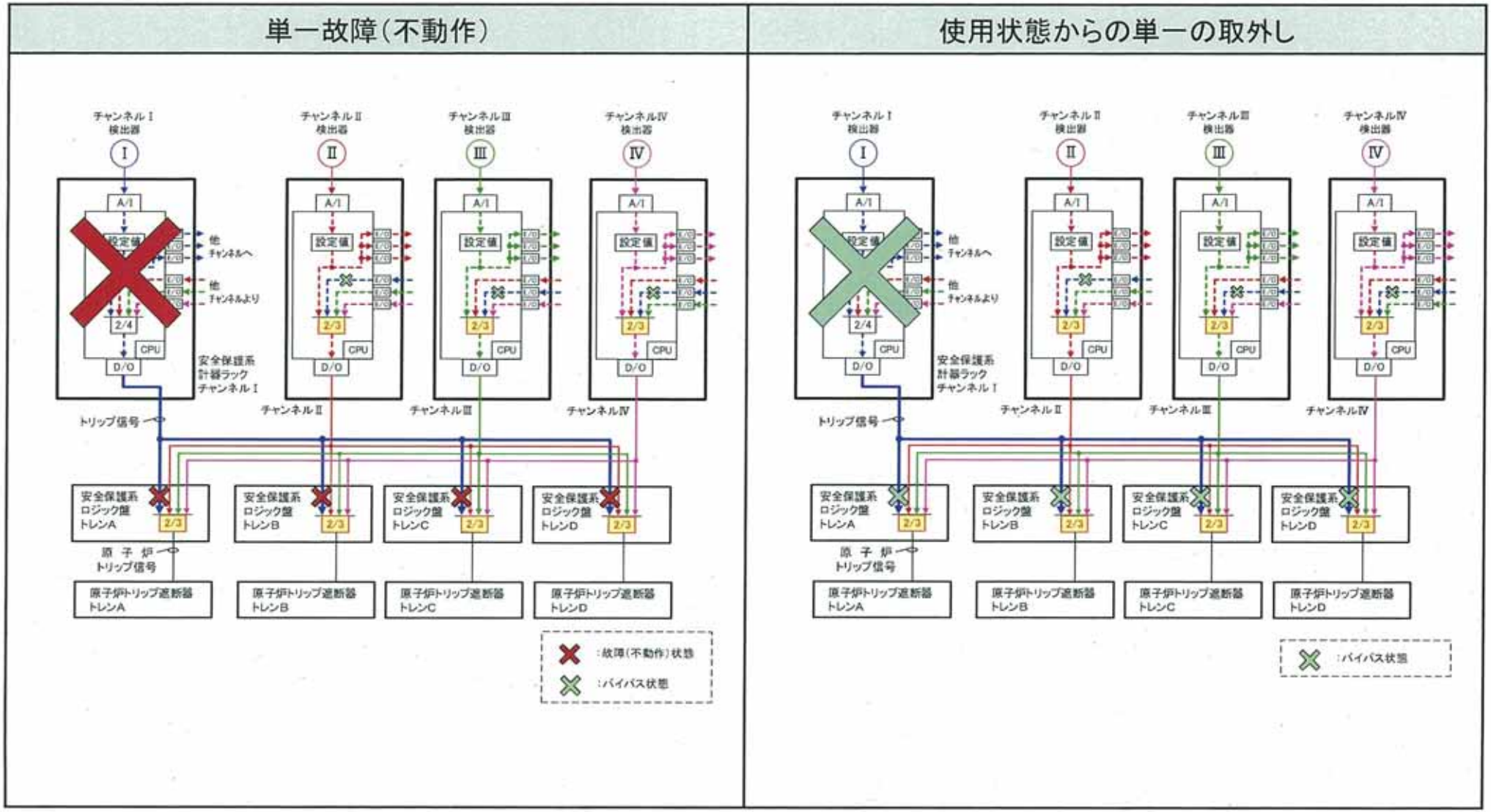
	検出遅れ時間（T_1）	**信号処理回路遅れ時間（T_2）**	安全解析使用値（T_1+T_2）
原子炉圧力低と加圧器水位低の一致			2.0
原子炉格納容器圧力高			2.0
原子炉格納容器圧力異常高			2.0

3. 技術基準規則への適合性（3／13）

技術基準規則	技術基準規則の解釈	設計方針
第2項 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。	—	✓ デジタル安全保護系は、その系統を構成する機器若しくはチャンネルに単一故障が起きた場合、又は使用状態からの単一の取外しを行った場合においても、その安全保護機能を失わないように、多重性を備えた設計とする。 **⇒次頁にて説明する。**

3. 技術基準規則への適合性(4／13)

例えば、下図のとおり、安全保護系計器ラックの単一故障又は使用状態からの単一の取り外しの場合においても、他の設備によって安全保護機能が動作できるよう、多重性を有する設計とする。



3. 技術基準規則への適合性（5／13）

技術基準規則	技術基準規則の解釈	設計方針
第3項 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。	第2項 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。	✓ デジタル安全保護系は、通常運転時、保修時、試験時、運転時の異常な過渡変化時及び設計基準事故時において、その安全保護機能を失わないように、その系統を構成するチャンネル相互を分離し、それぞれのチャンネル間の独立性を実用上可能な限り考慮した設計とする。 ✓ 具体的には、デジタル安全保護系はチャンネル毎に個別の筐体に収納することにより物理的分離を図り、チャンネル相互でデータ通信を行う場合は、光伝送方式を用いることにより電気的分離を図るとともに、通信専用のコントローラ及びメモリを介することにより他チャンネル又はデータ通信機能の異常がマイクロプロセッサ部に影響を及ぼさない設計とする。 **⇒次頁にて説明する。**

3. 技術基準規則への適合性（6／13）

下図のとおり、チャンネル間は、物理的、電気的、機能的な独立性を有する。

3. 技術基準規則への適合性(7／13)

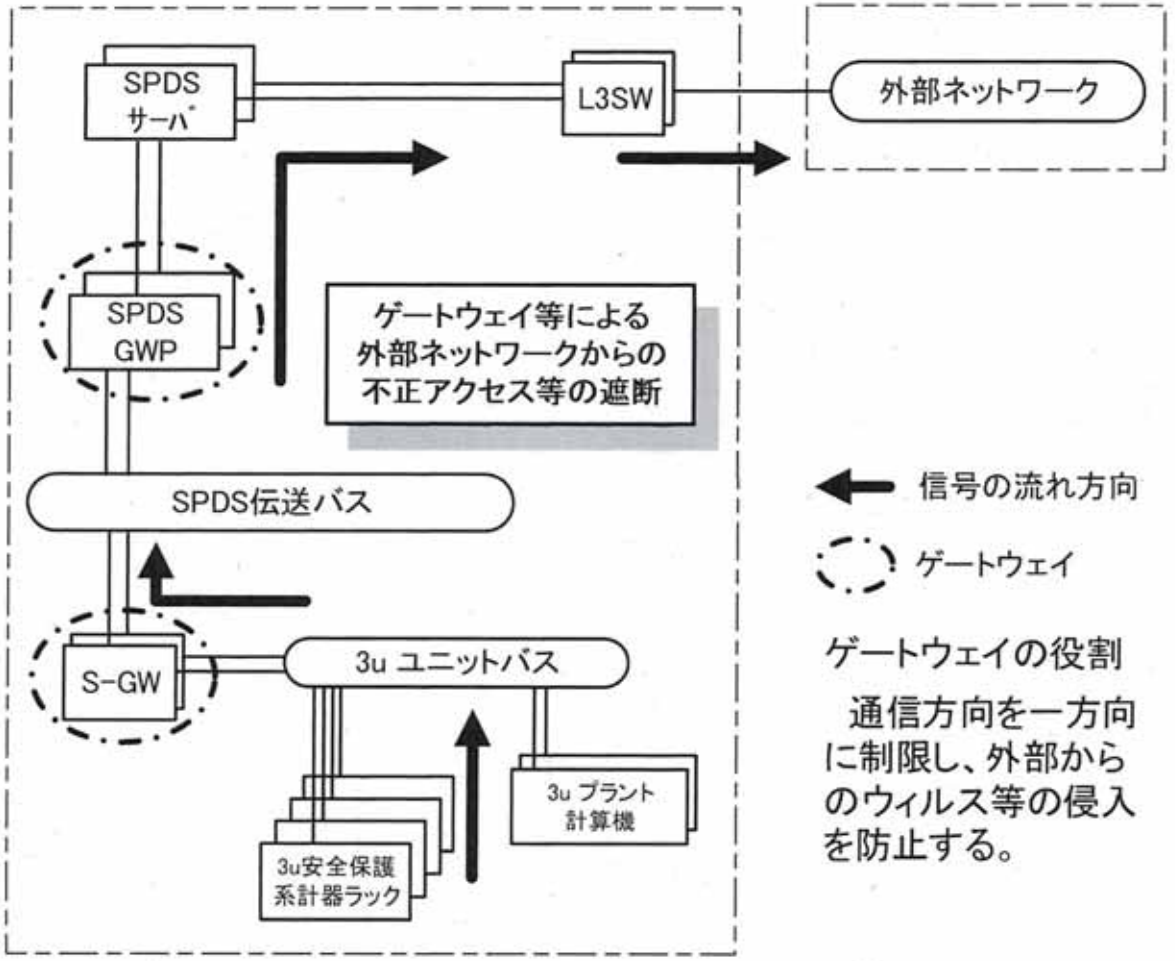
技術基準規則	技術基準規則の解釈	設計方針
第4項 駆動源の喪失、系統の遮断その他の不利な状況が生じた場合においても、発電用原子炉施設をより安全な状態に移行するか、又は当該状態を維持することにより、発電用原子炉施設の安全上支障がない状態を維持できること。	—	✓ 原子炉保護設備は、駆動源の喪失、系統の遮断等が生じた場合においてもフェイル・セーフとなり、最終的に原子炉施設が安全な状態に落ち着く設計とする。また、マイクロプロセッサ部の安全保護機能を喪失するような故障に対して原子炉トリップ信号を発信する設計とする。 ✓ 工学的安全施設作動設備は、駆動源の喪失、系統の遮断、及びマイクロプロセッサ部の安全保護機能を喪失するような故障等が生じた場合においてもフェイル・セーフとなるか、又は現状維持(フェイル・アズ・イズ)となり、この場合でも、多重化された他の装置によって安全保護動作を行うことができる設計とする。

3. 技術基準規則への適合性（8／13）

技術基準規則	技術基準規則の解釈	設計方針
第5項 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。	第3項 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。 （以下省略）	✓ 外部ネットワークと物理的な分離 〇デジタル安全保護系は、盤に対する施錠によりハードウェアを直接接続させないことにより物理的に分離する設計とする。 ✓ 外部ネットワークと機能的な分離 〇デジタル安全保護系は、外部ネットワークに直接接続しない設計とする。 〇デジタル安全保護系は、外部ネットワークである原子力防災用ネットワークに接続されている安全パラメータ表示システム等からの侵入に対して、ゲートウェイを介して信号の流れを送信のみに制限することにより機能的に分離する設計とする。 **⇒次頁にて説明する。** ✓ 物理的及び電気的アクセスの制限 〇人的侵入や不正行為が発生しないように、発電所への入域の出入管理による物理的アクセスを制限するとともに、デジタル安全保護系のデジタル計算機（ソフトウェアを変更するツール）のパスワード管理により電気的アクセスを制限する設計とする。

3. 技術基準規則への適合性(9／13)

下図のとおり、外部ネットワークに直接接続せず、外部ネットワークである原子力防災用ネットワークに接続されている安全パラメータ表示システム(SPDS)等からの侵入に対して、ゲートウェイを介して信号の流れを送信のみに制限することにより機能的に分離する設計としている。



3. 技術基準規則への適合性（10／13）

技術基準規則	技術基準規則の解釈	設計方針
第6項 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。	—	✓ デジタル安全保護系は、計測制御系とは機能的に分離した設計とする。デジタル安全保護系から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、デジタル安全保護系へ影響を与えない設計とする。 ✓ 具体的には、デジタル安全保護系と計測制御系は、個別の筐体に収納することにより物理的分離を図り、デジタル安全保護系と計測制御系とでデータ通信を行う場合は、光伝送方式を用いることにより電気的分離を図るとともに、通信専用のコントローラ及びメモリを介する等により計測制御系の故障がデジタル安全保護系に影響を及ぼさない設計とする。（17頁の図と同様）

3. 技術基準規則への適合性（11／13）

技術基準規則	技術基準規則の解釈	設計方針
第7項 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。	—	✓ デジタル安全保護系は、その健全性及び多重性の維持を確認するため、原子炉の運転中に多重性のある安全保護系のプロセス計装からの信号の監視や論理回路の動作等により、各チャンネルが独立して試験及び検査ができる設計とする。この場合、残りのチャンネルにより、安全保護機能を維持することができる。
第8項 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。	—	✓ デジタル安全保護系の設定値は、プラントの運転状態に合わせて、ソフトウェアの変更により、変更可能な設計とする。

3. 技術基準規則への適合性（12／13）

技術基準規則	技術基準規則の解釈	設計方針
—	第4項 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。（以下、省略）	✓ デジタル安全保護系のトリップが失敗する確率（アンアベイラビリティ）及び誤トリップする頻度（誤動作率）は、従来設備に比べて同等以下とする。 **⇒次頁にて説明する。** ✓ デジタル安全保護系のマイクロプロセッサ部にはサンプリング周期ごとに実施される自己診断機能を設け、故障の早期発見が可能な設計とし、運転中に常時、装置の健全性を確認する設計とする。 ✓ デジタル安全保護系のソフトウェアの品質を確保するために、「安全保護系へのディジタル計算機の適用に関する規程」（JEAC4620-2008）に基づき以下の品質保証活動を実施する。 〇ソフトウェアライフサイクル 〇ソフトウェア構成管理 〇検証および妥当性確認

3. 技術基準規則への適合性（13／13）

以下のとおり、デジタル安全保護系のトリップが失敗する確率（アンアベイラビリティ）及び誤トリップする頻度（誤動作率）は、デジタル制御装置を用いたデジタル安全保護系への取替え後、従来型の設備に比べて同等以下とする。

	変更前 ※ （従来アナログ設備）	変更後 （デジタル安全保護系）
トリップが失敗する確率 （アンアベイラベリティ）		
誤トリップする頻度 （誤動作率）		

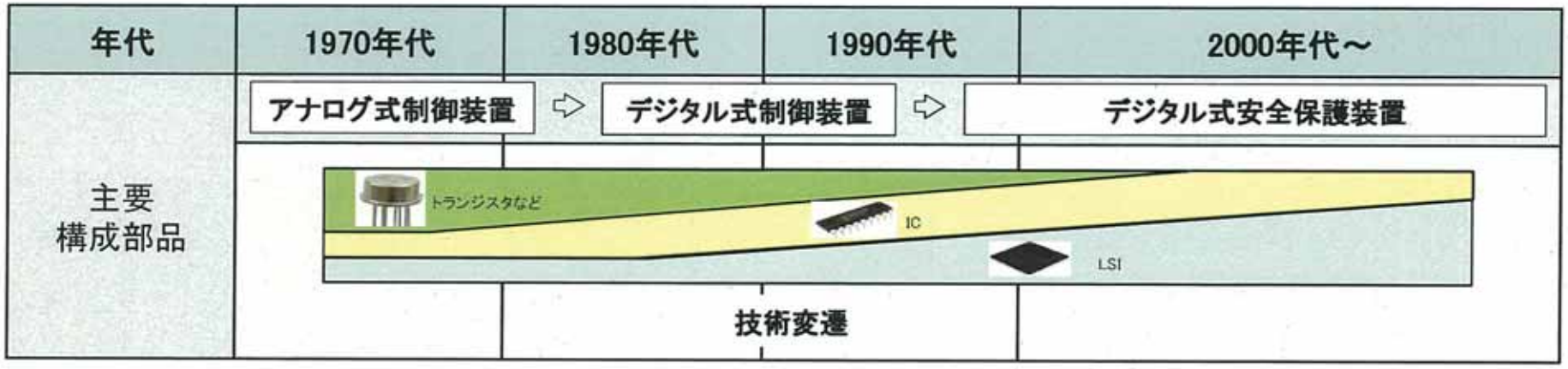
※建設時安全審査メモの記載値。デジタル安全保護系と同じ評価手法により再評価した場合は、
アンアベイラビリティ：［　　］/demand、 誤動作率：［　　］/hとなる。

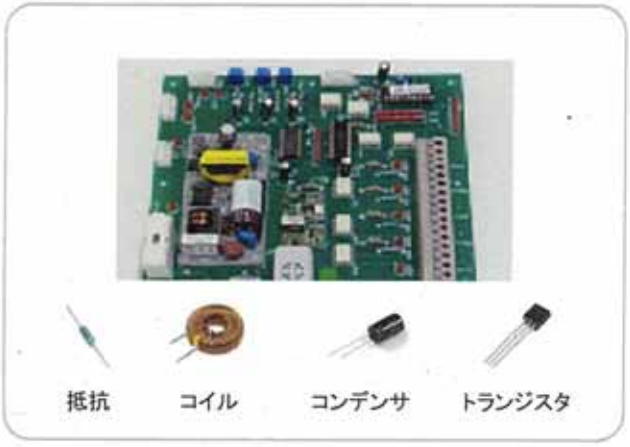
参考資料

参考① デジタル化の必要性

アナログ制御装置は、技術の進歩・変遷による部品の生産中止や減少による保守性の低下や拡張性の限界が課題になりつつあったことから、1980年代半ば以降、原子力分野への保守性向上を目的としてデジタル制御装置の適用が進められてきた。

【計測制御装置のデジタル化への変遷】





置き換え

マイクロプロセッサ

参考② 変更前後における安全保護系ロジック盤の構成

安全保護系ロジック盤は、変更前後ともにアナログ設備であるが、変更後では、汎用的な接点リレーを用いた簡素な構成のアナログ設備で構成する。

変更前	変更後

参考③ 発電用原子炉施設の設計及び工事の計画に係る手続ガイド

【発電用原子炉施設の設計及び工事の計画に係る手続ガイド（抜粋）】

I. 制御方式及び制御方法

安全保護系にデジタル安全保護系を適用する場合には、デジタル安全保護系を適用することを記載することとする。なお、ここでいうデジタル安全保護系とは、安全保護系の論理演算機能（作動（起動）回路）※がデジタル化されている設備をいう。

※「論理演算機能（作動（起動）回路）」とは、「論理回路」および「作動装置」からなる。

	変更前		変更後	
	論理回路	作動装置	論理回路	作動装置
原子炉非常停止信号	安全保護系ロジック盤	－	安全保護系計器ラック ＋ 安全保護系ロジック盤	－
工学的安全施設作動信号	安全保護系ロジック盤	安全防護系シーケンス盤	安全保護系計器ラック ＋ 安全保護系ロジック盤	安全防護系シーケンス盤

※赤字下線部は、デジタル制御装置を指す。

参考④ デジタル安全保護系の応答時間(1／2)

原子炉トリップ信号の応答時間（一覧）

[sec]

	検出遅れ時間(T_1)	信号処理回路遅れ時間(T_2)	原子炉トリップ遮断器の開放時間(T_3)	制御棒切り離し時間(T_4)	$T_1+T_2+T_3+T_4$
出力領域中性子束高（高設定）					0.5
出力領域中性子束高（低設定）					0.5
過大温度ΔT高					6.0
過出力ΔT高					6.0
原子炉圧力高					2.0
原子炉圧力低					2.0
1次冷却材流量低					1.0
1次冷却材ポンプ電源電圧低					1.2
蒸気発生器水位低					2.0
タービントリップ					1.0

安全解析使用値

参考④ デジタル安全保護系の応答時間（2／2）

工学的安全施設作動信号の応答時間（一覧）

[sec]

		検出遅れ時間 (T_1)	信号処理回路遅れ時間 (T_2)	T_1+T_2
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			2.0
	原子炉圧力異常低			2.0
	主蒸気ライン圧力低			2.0
	原子炉格納容器圧力高			2.0
主蒸気ライン隔離信号	主蒸気ライン圧力低			2.0
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			2.0

安全解析使用値

参考⑤ 設置許可申請書の記載（不正アクセス行為等の防止に係る箇所）

伊方3号機においては、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、新規制基準で新たな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」（設置許可基準規則）第24条第1項第6号（不正アクセス行為等の被害の防止）については、新規制基準への適合性を確認する審査において、要求を満足する設計とすることをご確認いただいており、許可済みの発電用原子炉設置変更許可申請書に反映されている。

○ 不正アクセス行為等の被害の防止について、平成27年7月15日発電用原子炉設置変更許可

五 発電用原子炉及びその附属施設の位置、構造及び設備
ロ．発電用原子炉施設の一般構造 (3)その他の主要な構造 （ｉ）本発電用原子炉施設は，「(1)耐震構造」，「(2)耐津波構造」に加え，以下の基本的方針のもとに安全設計を行う。 a．設計基準対象施設 (s)安全保護回路 安全保護回路を構成するデジタル計算機は、不正アクセス行為に対する安全保護回路の物理的分離及び機能的分離を行うとともに，ソフトウェアは設計、製作，試験及び変更管理の各段階で検証と妥当性の確認を適切に行うことで，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設計とする。 ヘ 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。

参考⑥ 設置許可申請書の記載（蓄電池による給電に係る箇所）（1／2）

伊方3号機においては、新規制基準の審査時に、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、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、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時間にわたって、電力の供給を行う設計としている。

その後、更なる信頼性の向上のため、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）を使用し、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している。

これらの蓄電池による給電について、本工事後においても給電時間への影響はない。

○ 蓄電池（非常用）及び蓄電池（重大事故等対処用）による給電について、平成27年7月15日発電用原子炉設置変更許可

○ 蓄電池（3系統目）による給電について、令和2年8月6日発電用原子炉設置変更許可

参考⑥ 設置許可申請書の記載（蓄電池による給電に係る箇所）（2／2）

ヌ. その他発電用原子炉の附属施設の構造及び設備

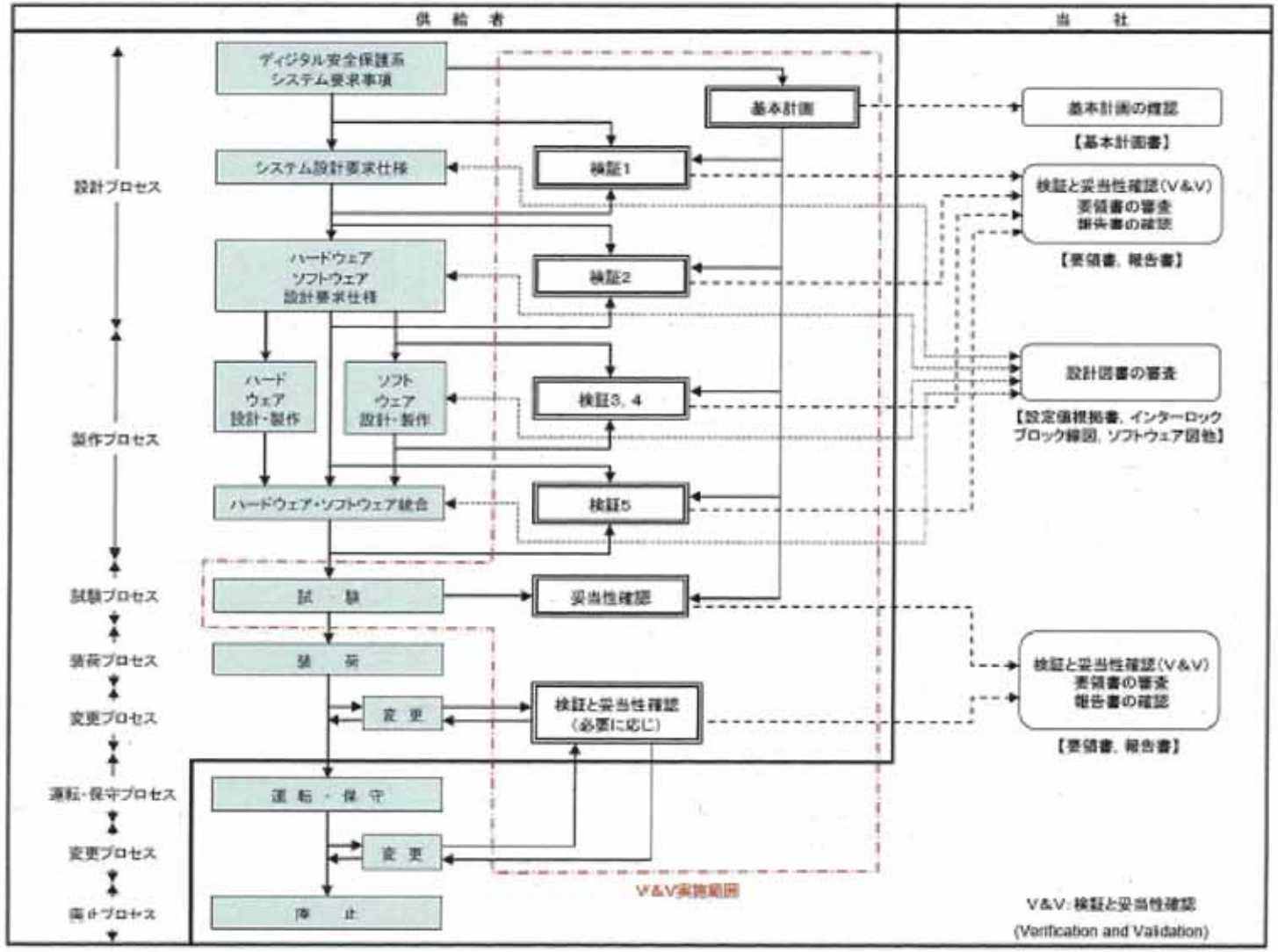
(2)非常用電源設備の構造
(ⅳ)代替電源設備
c. 非常用電源（直流）による給電に用いる設備
(a) 蓄電池（非常用）による非常用電源（直流）からの給電
設計基準事故対処設備の電源が喪失（全交流動力電源喪失）した場合に，重大事故等の対応に必要な設備に直流電力を供給する所内常設蓄電式直流電源設備として，蓄電池（非常用）を使用する。
蓄電池（非常用）は，中央制御室に隣接する計装盤室において簡易な操作で必要な負荷以外を切り離すことにより8時間にわたり電力の供給を行うことが可能な設計とする。また，蓄電池（重大事故等対処用）と組み合わせることにより事象発生から24時間にわたり電力の供給を行うことが可能な設計とする。

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。

参考⑦ ソフトウェアに対する検証及び妥当性確認

ディジタル安全保護系は，JEAC-4620／JEAG4609に基づいたV&Vを実施している。

【ディジタル安全保護系のソフトウェアに対する検証及び妥当性確認の流れ】



参考⑧ バックアップ設備

- ✓ 安全保護系計器ラックのソフトウェアについては、原子力発電所における安全のための品質保証活動に加え、「安全保護系へのディジタル計算機の適用に関する規程」（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）に基づく品質保証活動を実施することによって、多重化された設備が共通要因で同時に故障（以下「共通要因故障」という。）を生じる可能性は十分に小さいと考えられるが、より一層の信頼性向上を目的として、ハードウェアを用いて「止める」「冷やす」「閉じ込める」の安全機能を合理的にバックアップする設備（以下「バックアップ設備」という。）を自主的に設置している。

- ✓ 具体的には、早期の作動を要求する原子炉トリップ、タービントリップ、主給水隔離、補助給水起動について、バックアップ設備から自動作動させる。

- ✓ バックアップ設備の構成品については、デジタル安全保護系の設備に対する多様性並びに十分な品質、信頼性及び実績を考慮して、アナログのハードウェア（アナログ信号処理回路、リレー回路など）を用いる設計とし、デジタル安全保護系のソフトウェアを介さない構成とする。

- ✓ バックアップ設備の悪影響防止については、安全保護系を構成する設備とは別盤とすることによって、物理的分離及び絶縁回路の設置による電気的分離を図り、バックアップ設備の故障による安全保護系への悪影響を防止する設計とする。

- ✓ バックアップ設備の耐震性については、Sクラスの地震動においても誤動作のない設計とするとともに、安全保護系の設備と接続する回路については、耐震Sクラスとし、安全保護系の機能を阻害しない設計とする。