

泊発電所3号炉審査資料	
資料番号	DB24-9 r. 5. 0
提出年月日	令和4年10月7日

泊発電所3号炉

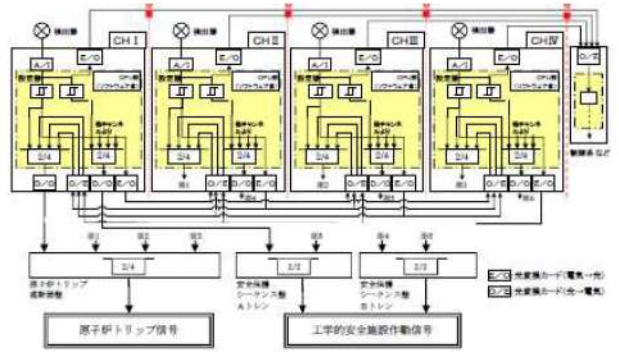
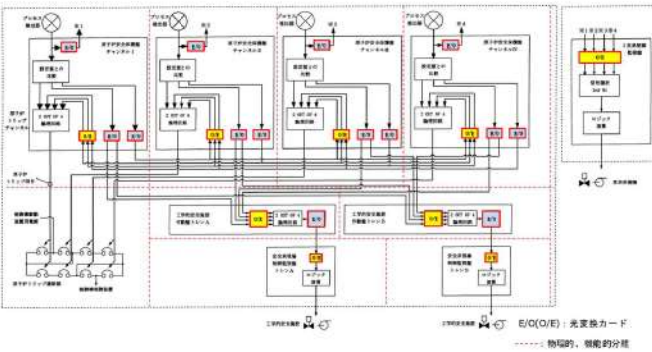
設置許可基準規則等への適合状況について (設計基準対象施設等) 比較表

第24条 安全保護回路

令和4年10月
北海道電力株式会社

枠囲みの内容は機密情報に属しますので公開できません。

大飯発電所3/4号炉	女川原子力発電所2号炉	泊発電所3号炉	相違理由
比較結果等を取りまとめた資料			
1. 先行審査実績等を踏まえた泊3号炉まとめ資料の変更状況(2017年3月以降)			
1-1) 設計方針・運用・体制などを変更し、まとめ資料を修正した箇所と理由			
a. 大飯3/4号炉まとめ資料と比較した結果、変更したもの : なし			
b. 女川2号炉まとめ資料と比較した結果、変更したもの : なし			
c. 他社審査会合の指摘事項を確認した結果、変更したもの : なし			
d. 当社が自主的に変更したもの : なし			
1-2) 設計方針・運用・体制を変更するものではないが、まとめ資料の記載の充実を行った箇所と理由			
a. 大飯3/4号炉まとめ資料と比較した結果、変更したもの : あり（比較表相違理由欄参照）			
b. 女川2号炉まとめ資料と比較した結果、変更したもの : あり（比較表相違理由欄参照）			
c. 他社審査会合の指摘事項を確認した結果、変更したもの : なし			
d. 当社が自主的に変更したもの : なし			
1-3) バックフィット関連事項			
なし			
2. まとめ資料との比較結果の概要			
2-1) 既許可に係る記載の相違			
<p>安全保護回路について、設置許可基準規則第24条及び技術基準規則第35条における追加要求事項は下表1のとおりであり、その他の要求事項に変更はない。したがって、以下の追加要求事項への適合性に係る記載を除いては既許可時から設計に変更がないため、記載の相違があっても既許可に係る記載の相違である。</p>			
表1：設置許可基準規則第24条及び技術基準規則第35条における追加要求事項			
設置許可基準規則第24条（安全保護回路）		技術基準規則第35条（安全保護回路）	
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。		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。	

大飯発電所3/4号炉	女川原子力発電所2号炉	泊発電所3号炉	相違理由														
<p>2-2) 設備構成の相違</p> <p>大飯3/4号炉と泊3号炉とで、下表2のとおり安全保護回路の機能を果たす安全保護系の構成が異なるため、上表1に示す追加要求事項に適合すべき対象(安全保護系のデジタル計算機)に差異がある。ただし、各対象設備において、上表1に示す追加要求事項に適合するための対策内容に、差異はない。</p>																	
<p>表2：安全保護回路の機能を果たす安全保護系の構成</p>																	
<p>項目</p>	<p>大飯3/4号炉</p> 	<p>泊3号炉</p> 	<p>差異理由</p> <p style="text-align: center;">—</p>														
<p>安全保護系の構成</p>	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 50%;">対象設備</th> <th style="width: 50%;">主な機能</th> </tr> </thead> <tbody> <tr> <td>原子炉安全保護計装盤</td> <td>原子炉トリップロジックおよび工学的安全施設作動ロジック</td> </tr> <tr> <td style="text-align: center;">—</td> <td style="text-align: center;">—</td> </tr> </tbody> </table>	対象設備	主な機能	原子炉安全保護計装盤	原子炉トリップロジックおよび工学的安全施設作動ロジック	—	—	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 50%;">対象設備</th> <th style="width: 50%;">主な機能</th> </tr> </thead> <tbody> <tr> <td>原子炉安全保護盤</td> <td>原子炉トリップロジック</td> </tr> <tr> <td>工学的安全施設作動盤</td> <td>工学的安全施設作動ロジック</td> </tr> <tr> <td>安全系現場制御監視盤</td> <td>工学的安全施設作動信号と各補機とのインターフェイス</td> </tr> </tbody> </table>	対象設備	主な機能	原子炉安全保護盤	原子炉トリップロジック	工学的安全施設作動盤	工学的安全施設作動ロジック	安全系現場制御監視盤	工学的安全施設作動信号と各補機とのインターフェイス	<p style="text-align: center;">—</p> <p>大飯3/4号炉は、原子炉安全保護計装盤が原子炉トリップロジックおよび工学的安全施設作動ロジックの機能を兼ねているが、泊3号炉はそれぞれの機能を別の盤にて実現している。</p> <p>泊3号炉は総合デジタルプラントであり、工学的安全施設作動信号と各補機とのインターフェイス機能を有する設備もデジタル計算機である。一方、大飯3/4号炉はアナログ設備(安全保護シーケンス盤)であり、デジタル計算機に該当しない。</p>
対象設備	主な機能																
原子炉安全保護計装盤	原子炉トリップロジックおよび工学的安全施設作動ロジック																
—	—																
対象設備	主な機能																
原子炉安全保護盤	原子炉トリップロジック																
工学的安全施設作動盤	工学的安全施設作動ロジック																
安全系現場制御監視盤	工学的安全施設作動信号と各補機とのインターフェイス																
<p>安全保護系のデジタル計算機</p>	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 50%;">対象設備</th> <th style="width: 50%;">主な機能</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;">—</td> <td style="text-align: center;">—</td> </tr> </tbody> </table>	対象設備	主な機能	—	—	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 50%;">対象設備</th> <th style="width: 50%;">主な機能</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;">—</td> <td style="text-align: center;">—</td> </tr> </tbody> </table>	対象設備	主な機能	—	—	<p style="text-align: center;">—</p>						
対象設備	主な機能																
—	—																
対象設備	主な機能																
—	—																

大飯発電所3/4号炉	女川原子力発電所2号炉	泊発電所3号炉	相違理由
<p>2-3) セキュリティ対策に係る運用の相違</p>			
<p>大飯3/4号炉と泊3号炉とで、安全保護系のデジタル計算機について、セキュリティ対策に係る運用の相違が下表3のとおり抽出された。ただし、セキュリティ対策に係る基本的な考え方は同じであり、対策の実効性に差異はない。</p>			
<p>表3：安全保護系のデジタル計算機におけるセキュリティ対策の運用</p>			
項目	大飯3/4号炉	泊3号炉	相違理由
ソフトウェア変更に用いる専用保守ツールのパスワード変更	定期的（1年に1回以上）	定期的（定期保安工事毎等）	<ul style="list-style-type: none"> 大飯3/4号炉および泊3号炉ともに、セキュリティ対策における基本的な考え方は、「パスワードは、セキュリティ責任者の管理のもと、必要最小限の者に付与すること」である。 具体的な運用として、大飯3/4号炉は、少なくとも1年に1回以上パスワードを変更することとしている。 一方、泊3号炉は、定期保安工事や人事異動により、セキュリティ責任者やパスワードを付与すべき対象者が変更となる都度、パスワードを変更することとしている。 結果として、大飯3/4号炉にて定期保安工事の際にパスワードを変更することもあれば、泊3号炉にて1年に1回以上パスワードを変更することもあり、対策の実効性に差異はない。
ソフトウェアのバックアップ	定期的	ソフトウェアの改造工事毎	<ul style="list-style-type: none"> 大飯3/4号炉および泊3号炉ともに、セキュリティ対策における基本的な考え方は、「実際に現場の設備にインストールされている最新版のソフトウェアについて、バックアップを保管しておくこと」である。 具体的な運用として、大飯3/4号炉は、定期的にバックアップを取得することとしている。 一方、泊3号炉は、ソフトウェアの改造工事の都度、最新版のソフトウェアについてバックアップを取得し、保管する運用としている。 結果として、大飯3/4号炉にてソフトウェアの改造工事の際にバックアップを取得することもあり、対策の実効性に差異はない。

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

第24条 安全保護回路

大飯発電所3/4号炉（リファレンスプラント）	女川原子力発電所2号炉	泊発電所3号炉	相違理由
<p>第24条：安全保護回路</p> <p><目次></p> <p>1. 基本方針</p> <p>1.1 要求事項の整理</p> <p>1.2 追加要求事項に対する適合性</p> <p>(1) 位置、構造及び設備</p> <p>(2) 安全設計方針</p> <p>(3) 適合性説明</p> <p>1.3 気象等</p> <p>1.4 設備等（手順等含む）</p> <p>2. 安全保護回路</p> <p>2.1 概要</p> <p>2.2 原子炉安全保護計装盤の物理的分離</p> <p>2.3 原子炉安全保護計装盤の機能的分離</p> <p>2.4 コンピュータウィルスによる被害の防止</p> <p>2.5 設計、製作、試験及び変更管理の各段階における検証及び妥当性確認</p> <p>2.6 物理的及び電氣的アクセスの制限</p> <p>2.7 原子炉安全保護計装盤の概要</p> <p>2.8 原子炉安全保護計装盤のソフトウェア変更管理</p> <p>2.9 耐ノイズ・サージ対策</p>	<p>第24条：安全保護回路</p> <p><目次></p> <p>1. 基本方針</p> <p>1.1 要求事項の整理</p> <p>1.2 追加要求事項に対する適合性</p> <p>(1) 位置、構造及び設備</p> <p>(2) 安全設計方針</p> <p>(3) 適合性説明</p> <p>1.3 気象等</p> <p>1.4 設備等（手順等含む）</p> <p>2. 追加要求事項に対する適合方針</p> <p>2.1 安全保護回路の不正アクセス行為防止のための措置について</p> <p>2.3 安全保護回路の物理的分離対策</p> <p>2.5 安全保護系の検証及び妥当性確認について</p> <p>2.6 想定脅威に対する対策について</p> <p>2.4 外部からの不正アクセス行為の防止について</p> <p>2.2 安全保護回路の概要</p> <p>2.7 物理的分離及び電氣的分離について</p> <p>3. 別紙</p> <p>別紙1 安全保護回路について、承認されていない動作や変更を防ぐための設計方針</p> <p>別紙2 今回の設置許可申請に関し、安全保護回路に変更を施している場合の基準適合性</p> <p>別紙3 安全保護系の過去のトラブル（落雷によるスクラム動作事象等）の反映事項</p> <p>別紙4 現場据付以降の作業時における、インサイダー等に対するセキュリティ対策</p> <p>別紙5 安全保護回路のうちデジタル処理部のある機器のシステムへ接続可能なアクセスについて</p> <p>別紙6 安全保護系のセキュリティ対策に関する当社及び受注者の対応について</p> <p>別紙7 安全保護回路のうちデジタル部分について、システム設計と実際のデバイスが具備している機能との差（未使用機能等）によ</p>	<p>第24条：安全保護回路</p> <p><目次></p> <p>1. 基本方針</p> <p>1.1 要求事項の整理</p> <p>1.2 追加要求事項に対する適合性</p> <p>(1) 位置、構造及び設備</p> <p>(2) 安全設計方針</p> <p>(3) 適合性説明</p> <p>1.3 気象等</p> <p>1.4 設備等（手順等含む）</p> <p>2. 追加要求事項に対する適合方針</p> <p>2.1 安全保護回路の不正アクセス行為防止のための措置について</p> <p>2.2 概要</p> <p>2.3 安全保護設備の物理的分離</p> <p>2.4 安全保護設備の機能的分離</p> <p>2.5 コンピュータウィルスによる被害の防止</p> <p>2.6 設計、製作、試験及び変更管理の各段階における検証及び妥当性確認</p> <p>2.7 物理的及び電氣的アクセスの制限</p> <p>2.8 安全保護設備の概要</p> <p>2.9 安全保護設備のソフトウェア変更管理</p> <p>2.10 耐ノイズ・サージ対策</p> <p>3. 別紙</p> <p>別紙1 安全保護設備について、承認されていない動作や変更を防ぐための設計方針</p> <p>別紙2 今回の設置許可申請に関し、安全保護設備に変更を施している場合の基準適合性</p> <p>別紙3 安全保護系の過去のトラブル（落雷によるスクラム動作事象等）の反映事項</p> <p>別紙4 現場据付以降の作業時における、インサイダー等に対するセキュリティ対策</p> <p>別紙5 安全保護設備のシステムへ接続可能なアクセスについて</p> <p>別紙6 安全保護設備のセキュリティ対策に関する当社及び受注者の対応について</p> <p>別紙7 安全保護設備について、システム設計と実際のデバイスが具備している機能との差（未使用機能等）による影響の有無</p>	<p>相違理由</p> <p>項目名称の相違</p> <p>・以下 2.1 の追加に併せ、2. の項目名称も女川を参照。</p> <p>記載内容の相違(女川実績の反映)</p> <p>・大飯をリファレンスプラントとしつつも、女川の審査実績を踏まえ、記載を拡充するもの。</p> <p>資料番号の相違</p> <p>・以降、同様の相違は、相違理由の記載を省略する。</p> <p>記載内容の相違(女川実績の反映)</p>

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

第24条 安全保護回路

大飯発電所3/4号炉（リファレンスプラント）	女川原子力発電所2号炉	泊発電所3号炉	相違理由
<p>3. 技術的能力説明資料 （別添資料）安全保護回路</p>	<p>る影響の有無 別紙8 安全保護回路のうち一部デジタル演算処理を行う機器の検証及び妥当性確認について</p> <p>4. 別添 別添 女川原子力発電所2号炉 運用、手順説明資料 安全保護回路</p>	<p>別紙8 安全保護設備の検証及び妥当性確認について</p> <p>4. 技術的能力説明資料 （別添資料）安全保護回路</p>	

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

第24条 安全保護回路

大飯発電所3/4号炉（リファレンスプラント）	女川原子力発電所2号炉	泊発電所3号炉	相違理由
<p style="text-align: center;">＜概要＞</p> <p>1. において、設計基準事故対処設備の設置許可基準規則、技術基準規則の追加要求事項を明確化するとともに、それら要求に対する大飯発電所3号炉及び4号炉における適合性を示す。</p> <p>2. において、設計基準事故対処設備について、追加要求事項に適合するために必要となる機能を達成するための設備又は運用等について説明する。</p> <p>3. において、追加要求事項に適合するための技術的能力（手順等）を抽出し、必要となる運用対策等を整理する。</p>		<p style="text-align: center;">＜概要＞</p> <p>1. において、設計基準事故対処設備の設置許可基準規則、技術基準規則の追加要求事項を明確化するとともに、それら要求に対する泊発電所3号炉における適合性を示す。</p> <p>2. において、設計基準事故対処設備について、追加要求事項に適合するために必要となる機能を達成するための設備又は運用等について説明する。</p> <p>3. において、追加要求事項に適合するための技術的能力（手順等）を抽出し、必要となる運用対策等を整理する。</p>	<p>名称の相違（申請ブラント）</p> <p>以降、同様の相違は、相違理由の記載を省略する。</p>

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

第24条 安全保護回路

大阪発電所3/4号炉（リファレンスプラント）

1. 基本方針
 1.1 要求事項の整理
 安全保護回路について、設置許可基準規則第24条及び技術基準規則第35条における追加要求事項を明確化する（表1）。

表1 設置許可基準規則第24条及び技術基準規則第35条 要求事項

設置許可基準規則 第24条（安全保護回路）	技術基準規則 第35条（安全保護装置）	備考
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。 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。 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。 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。	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。 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、多重性を確保するものとする。 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。	変更なし

設置許可基準規則 第24条（安全保護回路）	技術基準規則 第35条（安全保護装置）	備考
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。	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。	変更なし
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。	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。	追加要求事項
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。	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。 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。	変更なし

女川原子力発電所2号炉

1. 基本方針
 1.1 要求事項の整理
 安全保護回路について、設置許可基準規則第二十四条及び技術基準規則第三十五条における追加要求事項を明確化する（第1.1表）。

第1.1表 設置許可基準規則第二十四条及び技術基準規則第三十五条 要求事項

設置許可基準規則 第二十四条（安全保護回路）	技術基準規則 第三十五条（安全保護装置）	備考
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。 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。 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。	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。 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。	変更なし
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。	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。	変更なし
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。	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。	変更なし

設置許可基準規則 第二十四条（安全保護回路）	技術基準規則 第三十五条（安全保護装置）	備考
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。	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。	追加要求事項
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。	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。	変更なし
—	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。	変更なし
—	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。	変更なし

泊発電所3号炉

1. 基本方針
 1.1 要求事項の整理
 安全保護回路について、設置許可基準規則第24条及び技術基準規則第35条における追加要求事項を明確化する（表1）。

表1 設置許可基準規則第24条及び技術基準規則第35条 要求事項

設置許可基準規則 第24条（安全保護回路）	技術基準規則 第35条（安全保護装置）	備考
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。 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。 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。 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。	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。 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。 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。	変更なし 変更なし 変更なし 変更なし

設置許可基準規則 第24条（安全保護回路）	技術基準規則 第35条（安全保護装置）	備考
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。	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。	変更なし
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。	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。	変更なし
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。	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。	追加要求事項
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。	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。	変更なし 変更なし
設置許可基準規則 第24条（安全保護回路）	技術基準規則 第35条（安全保護装置）	備考
—	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。	変更なし

相違理由

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

第24条 安全保護回路

大飯発電所3/4号炉（リファレンスプラント）	女川原子力発電所2号炉	泊発電所3号炉	相違理由
<p>1.2 追加要求事項に対する適合性</p> <p>(1) 位置、構造及び設備</p> <p>(3) その他の主要な構造</p> <p>(i) 本原子炉施設は、(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。</p> <p>a. 設計基準対象施設</p> <p>(s) 安全保護回路</p> <p>安全保護回路は、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とともに、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設計とする。</p> <p>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、多重性を確保する設計とする。</p> <p>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独立性を確保する設計とする。</p> <p>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、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、原子炉施設の安全上支障がない状態を維持できる設計とする。</p> <p>安全保護系のデジタル計算機は、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。</p>	<p>1.2 追加要求事項に対する適合性</p> <p>(1) 位置、構造及び設備</p> <p>ロ 発電用原子炉施設の一般構造</p> <p>(3) その他の主要な構造</p> <p>(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。</p> <p>a. 設計基準対象施設</p> <p>(s) 安全保護回路</p> <p>安全保護回路は、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保護系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とともに、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、原子炉保護系及び工学的安全施設を自動的に作動させる設計とする。</p> <p>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、多重性を確保する設計とする。</p> <p>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独立性を確保する設計とする。</p> <p>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設計とする。</p> <p>安全保護回路のうち一部デジタル演算処理を行う機器は、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、ソフトウェア及びハードウェア回路は設計、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。</p>	<p>1.2 追加要求事項に対する適合性</p> <p>(1)位置、構造及び設備</p> <p>ロ. 発電用原子炉施設の一般構造</p> <p>(3)その他の主要な構造</p> <p>(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。</p> <p>a. 設計基準対象施設</p> <p>(s) 安全保護回路</p> <p>安全保護回路は、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とともに、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設計とする。</p> <p>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、多重性を確保する設計とする。</p> <p>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独立性を確保する設計とする。</p> <p>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設計とする。</p> <p>安全保護回路の機能を果たす安全保護系のデジタル計算機は、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。</p>	<p>既許可構成の相違</p> <p>記載表現の相違(発電用原子炉施設)</p> <p>・以降、同様の相違は、相違理由の記載を省略する。</p> <p>記載表現の相違(安全保護回路/系)</p> <p>・泊は「安全保護回路：機能を指す言葉」「安全保護系：設備を指す言葉」と定義している。</p> <p>記載表現の相違(デジタル/デジタル)</p> <p>・泊は、建設時より「TEAG4609」における用語の定義に基づき、記載をデジタルとしている。</p> <p>・以降、同様の相違は、相違理由の記載を省略する。</p> <p>【女川】 設備の相違(ハードウェア回路)</p> <p>・ハードウェア回路とは、アナログのロ</p>

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

第24条 安全保護回路

大阪発電所3/4号炉（リファレンスプラント）	女川原子力発電所2号炉	泊発電所3号炉	相違理由
<p>計測制御系統施設の一部を共用する場合には、その安全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した設計とする。</p> <p>【説明資料（2.1、2.2、2.3、2.4、2.5、2.6）】</p> <p>【まとめ資料作成範囲外のため。設置許可(令和3年5月)より引用】↓</p> <p>へ、計測制御系統施設の構造及び設備</p> <p>A. 3号炉</p> <p>(1) 計装</p> <p>(i) 核計装の種類</p> <p>原子炉容器外周に設置した炉外核計装の中性子束検出器により次の3領域に分けて中性子束を測定する。</p> <p>中性子源領域 2チャンネル 中間領域 2チャンネル 出力領域 4チャンネル</p> <p>(ii) その他の主要な計装の種類</p> <p>原子炉施設のプロセス計装制御のため、原子炉圧力、加圧器水位、1次冷却材流量及び温度、蒸気発生器水位、制御棒クラスタ位置、反応度停止余裕等の計測装置を設ける。</p> <p>原子炉格納容器内の温度、圧力、水位、水素濃度及び放射線量率等想定される重大事故等の対応に必要な重要な監視パラメータ及び重要代替パラメータが計測又は監視及び記録ができる設計とする。</p>	<p>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した設計とする。</p> <p>【説明資料（2.1：P24条-27,28）（2.2：P24条28-31）（2.3：P24条-32）（2.4：P24条-33）（2.5：P24条-34,35）（2.6：P24条-36）（2.7：P24条-37,38）】</p> <p>へ 計測制御系統施設の構造及び設備</p> <p>(1) 計装</p> <p>(i) 核計装の種類</p> <p>中性子束は以下のように二つの領域に分けて発電用原子炉内で計測する。</p> <p>起動領域：核分裂電離箱方式モニタ 8チャンネル （中性子源領域及び中間領域） 出力領域：小形核分裂電離箱方式モニタ 124チャンネル</p> <p>(ii) その他の主要な計装の種類</p> <p>発電用原子炉施設のプロセス計測制御のため、原子炉水位、原子炉圧力、原子炉再循環流量、給水流量、主蒸気流量、制御棒駆動水圧等の計測装置を設ける。</p>	<p>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した設計とする。</p> <p>【説明資料（2.1：P24条-30,31）（2.2：P24条31）（2.3：P24条-31,32）（2.4：P24条-33）（2.5：P24条-33）（2.6：P24条-34-36）（2.7：P24条-37）（2.9：P24条-40）】</p> <p>へ、計測制御系統施設の構造及び設備</p> <p>(1) 計装</p> <p>(i) 核計装の種類</p> <p>原子炉容器外周に設置した炉外核計装の中性子束検出器により、次の3領域に分けて中性子束を測定する。</p> <p>中性子源領域 2チャンネル 中間領域 2チャンネル 出力領域 4チャンネル</p> <p>(ii) その他の主要な計装の種類</p> <p>発電用原子炉施設的安全保護回路のプロセス計装として、原子炉圧力、加圧器水位、1次冷却材流量・温度、蒸気発生器水位、主蒸気ライン圧力、原子炉格納容器圧力等の計測装置を設ける。</p> <p>原子炉格納容器内の温度、圧力、水位、水素濃度及び放射線量率等想定される重大事故等の対応に必要な重要な監視パラメータ及び重要代替パラメータが計測又は監視及び記録ができる設計とする。</p>	<p>ジック回路を指す。</p> <p>・泊の安全保護系のデジタル計算機において、ハードウェア回路は存在しない。</p> <p>記載表現の相違(女川実績の反映)</p> <p>・大阪をリファレンスプラントとしても、女川の審査実績を踏まえ、記載を拡充するもの。</p> <p>記載表現の相違(女川実績の反映)</p> <p>既許可構成の相違</p> <p>既許可記載の相違</p> <p>・新規制基準のうちDB24条の追加要求事項(不正アクセス防止)に対して、既許可時点から設計に変更を伴わない部分に係る、記載の相違。</p> <p>記載の充実(追加要求事項対象外、大阪参照)</p> <p>・新規制基準のうちDB24条の追加要求事項(不正アクセス防止)の対象外だが、先行の新規制基準適合プラントに比べて情報量が不</p>

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

第24条 安全保護回路

大飯発電所3/4号炉（リファレンスプラント）	女川原子力発電所2号炉	泊発電所3号炉	相違理由
<p>(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、原子炉トリップ及び非常用炉心冷却設備作動等を行う。</p> <p>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。</p> <p>(i) 原子炉停止回路の種類 次に示す信号により原子炉をトリップさせる原子炉停止回路を設ける。</p> <ul style="list-style-type: none"> ・ 中性子東高（中性子源領域及び中間領域） ・ 中性子東高（出力領域） ・ 中性子東変化率高（出力領域） ・ 非常用炉心冷却設備作動 ・ 過大温度ΔT高 ・ 過大出力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次冷却材ポンプ回転数低 ・ タービントリップ ・ 蒸気発生器水位低 ・ 地震加速度高 ・ 手動 	<p>(2) 安全保護回路 安全保護回路（安全保護系）は、「原子炉停止回路（原子炉保護系）」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）」で構成する。</p> <p>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。</p> <p>【説明資料（2.1：P24条-27,28）（2.2：P24条28-31）（2.3：P24条-32）（2.4：P24条-33）（2.5：P24条-34,35）（2.6：P24条-36）（2.7：P24条-37,38）】</p> <p>(i) 原子炉停止回路の種類</p> <p>原子炉停止回路（原子炉保護系）は、次に示す条件により発電用原子炉をスクラムさせるため、二重（2チャンネル）の「1 out of 2」方式の回路を設け、2チャンネルの同時動作によって発電用原子炉をスクラムさせる。</p> <ol style="list-style-type: none"> a. 原子炉圧力高 b. 原子炉水位低 c. ドライウェル圧力高 d. 中性子東高（平均出力領域モニタ） e. 中間領域における原子炉周期短（起動領域モニタ） f. 中性子束計装動作不能（起動及び平均出力領域モニタ） g. スクラム排出容器水位高 h. 主蒸気隔離弁閉 i. 主蒸気止め弁閉 j. 蒸気加減弁急速閉 k. 主蒸気管放射能高 l. 地震加速度大 <p>なお、原子炉保護系の電源喪失、モードスイッチ「停止」及び手動の場合にも発電用原子炉はスクラムする。</p>	<p>(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する。 安全保護回路の機能を果たす安全保護系は、原子炉停止回路の機能を果たす原子炉保護設備及びその他の主要な安全保護回路の機能を果たす工学的安全施設作動設備で構成し、マイクロプロセッサを用いる設計とする。 安全保護系は、計測制御系と機能的に分離した設計とする。また、安全保護系は、駆動源の喪失、系統の遮断等が生じた場合にも、最終的に発電用原子炉施設が安全な状態に落ち着く設計とする。 安全保護系は、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。</p> <p>【説明資料（2.1：P24条-30,31）（2.2：P24条31）（2.3：P24条-31,32）（2.4：P24条-33）（2.5：P24条-33）（2.6：P24条-34-36）（2.7：P24条-37）（2.9：P24条-40）】</p> <p>(i) 原子炉停止回路の種類 原子炉保護設備は、原子炉の安全性を損なうおそれのある状態が発生した場合、あるいは発生が予想される場合に、これを抑制あるいは防止するため、異常を検知し原子炉を自動的に緊急停止（トリップ）させる。 原子炉保護設備は、多重チャンネル構成とし、測定変数に対して「2 out of 4」方式等の回路を設け、次に示す信号により原子炉を自動的にトリップさせる。</p> <ol style="list-style-type: none"> a. 中性子源領域中性子東高 b. 中間領域中性子東高 c. 出力領域中性子東高 d. 出力領域中性子東変化率高 e. 非常用炉心冷却設備作動 f. 過大温度ΔT高 g. 過大出力ΔT高 h. 原子炉圧力高 i. 原子炉圧力低 j. 加圧器水位高 k. 1次冷却材流量低 l. 1次冷却材ポンプ電源電圧低 m. 1次冷却材ポンプ電源周波数低 n. タービントリップ o. 蒸気発生器水位低 p. 地震加速度大 <p>また、手動操作時及び原子炉保護設備の電源喪失時にも、原子炉はトリップする設計とする。</p>	<p>足しているため、記載を充実するもの。</p> <p>既許可記載の相違</p> <p>記載表現の相違（安全保護回路／系）</p> <p>記載表現の相違（女川実績の反映）</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p>

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

第24条 安全保護回路

大飯発電所3/4号炉（リファレンスプラント）	女川原子力発電所2号炉	泊発電所3号炉	相違理由
<p>(ii) その他の主要な安全保護回路の種類 以下に示す信号により工学的安全施設作動設備を作動させる回路を設ける。</p> <p>a. 非常用炉心冷却設備作動信号 1次冷却材の確保あるいは過度の反応度添加を抑え、炉心の損傷を防止する。 ・原子炉圧力低</p> <p>・主蒸気ライン圧力低 ・原子炉格納容器圧力高 ・手動</p> <p>b. 主蒸気ライン隔離信号 主蒸気管破断時に、健全側の蒸気発生器からの蒸気流出を防ぎ、1次冷却系統の除熱能力を確保する。 ・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 ・手動</p> <p>c. 原子炉格納容器スプレイ作動信号 1次冷却系統の破断又は原子炉格納容器内での主蒸気管破断時に、原子炉格納容器の減圧及びよう素除去のため、原子炉格納容器スプレイ設備を起動する。 ・原子炉格納容器圧力異常高 ・手動</p> <p>d. 原子炉格納容器隔離信号 1次冷却材喪失事故及び原子炉格納容器内での主蒸気管破断事故後に放射性物質の放出を防止するため、原子炉格納容器の隔離弁を閉止する。 ・非常用炉心冷却設備作動信号 ・原子炉格納容器スプレイ作動信号 ・手動</p> <p>【まとめ資料作成範囲外のため。設置許可(令和3年5月)より引用】↑</p>	<p>(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（工学的安全施設作動回路）には、次のものを設ける。</p> <p>a. 原子炉水位低、主蒸気管放射能高、主蒸気管圧力低、主蒸気管流量大、主蒸気管トンネル温度高、主復水器真空度低のいずれかの信号による主蒸気隔離弁の閉鎖</p> <p>b. ドライウェル圧力高、原子炉水位低、原子炉建屋原子炉棟放射能高のいずれかの信号による常用換気系の閉鎖と非常用ガス処理系の起動</p> <p>c. 原子炉水位低又はドライウェル圧力高の信号による高圧炉心スプレイ系、低圧炉心スプレイ系及び低圧注水系の起動</p> <p>d. 原子炉水位低及びドライウェル圧力高の同時信号による自動減圧系の作動</p> <p>e. 原子炉水位低又はドライウェル圧力高の信号による高圧炉心スプレイ系ディーゼル発電機及び非常用ディーゼル発電機の起動</p> <p>f. 原子炉水位低又はドライウェル圧力高の信号による主蒸気隔離弁以外の隔離弁の閉鎖</p>	<p>(ii) その他の主要な安全保護回路の種類 工学的安全施設作動設備は、発電用原子炉施設の破損、故障等に起因する燃料の破損等による放射性物質の放散の可能性のある場合に、これを抑制又は防止するため、異常を検知し、次に示す条件により工学的安全施設を自動的に作動させる。</p> <p>a. 非常用炉心冷却設備の起動 1次冷却材の確保あるいは過度の反応度添加を抑え、炉心の損傷を防止する。 ・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</p> <p>b. 主蒸気隔離弁の閉止 主蒸気管破断時に、健全側の蒸気発生器からの蒸気流出を防ぎ、1次冷却系統の除熱能力を確保する。 ・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</p> <p>c. 原子炉格納容器スプレイの起動 1次冷却系統の破断又は原子炉格納容器内での主蒸気管破断時に、原子炉格納容器の減圧及びよう素除去のため、原子炉格納容器スプレイ設備を起動する。 ・原子炉格納容器圧力異常高</p> <p>d. 主蒸気隔離弁以外の主要な原子炉格納容器隔離弁の閉止 1次冷却材喪失事故及び原子炉格納容器内での主蒸気管破断事故後に放射性物質の放出を防止するため、原子炉格納容器の隔離弁を閉止する。 ・非常用炉心冷却設備作動信号 ・原子炉格納容器スプレイ作動信号</p> <p>なお、手動操作で上記動作を行うことができる。</p>	<p>既許可記載の相違</p> <p>記載の充実(追加要求事項の対象外、大飯参照)</p>

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

第24条 安全保護回路

大飯発電所3/4号炉（リファレンスプラント）	女川原子力発電所2号炉	泊発電所3号炉	相違理由
<p>(2)安全設計方針</p> <p>1.1.5 計測制御系統施設設計の基本方針</p> <p>1.1.5.1 原子炉制御設備 運転及び制御保護動作に必要な中性子束、温度、圧力等を測定する原子炉計装及びプロセス計装を設けるとともに、通常運転時に起こり得る設計負荷変化及び外乱に対して自動的に原子炉を制御する原子炉制御設備を設ける。</p> <p>1.1.5.2 監視警報装置 通常運転時に異常、故障が発生した場合は、これを早期に検知し所要の対策が講じられるよう中性子束、温度、圧力、放射能等を常時自動的に監視し、警報を発する装置を設ける。 また、誤動作・誤操作による異常、故障の拡大を防止し事故への進展を確実に防止するようインターロックを設ける。</p> <p>1.1.5.3 原子炉保護設備 炉心及び原子炉冷却材圧力バウンダリの健全性が損なわれることのないよう異常状態へ接近するのを検知し、原子炉トリップを行うために原子炉保護設備を設ける。 原子炉保護設備は、必要な場合に確実に作動するように多重性及び独立性を備え、単一故障によって保護機能を喪失しない設計とするとともに、駆動源が喪失した場合には、最終的に安全な状態に落ち着く設計とする。また、これら保護機能が喪失していないことを運転中に確認できるよう設計する。</p> <p>1.1.5.4 工学的安全施設作動設備 1次冷却材喪失等の設計基準事故時に、炉心及び原子炉格納容器バウンダリを保護するため、工学的安全施設を作動させる工学的安全施設作動設備を設ける。工学的安全施設作動設備は、原子炉保護設備と同様に高い信頼性が得られるよう設計する。</p> <p>1.1.5.5 安全保護回路不正アクセス防止 安全保護回路への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。 【説明資料（2.1、2.2、2.3、2.4、2.5、2.6）】</p> <p>1.1.5.6 安全保護回路共用禁止 安全保護回路は2基以上の原子炉施設間で共用しない設計とする。</p>	<p>(2) 安全設計方針</p> <p>1. 安全設計</p> <p>1.1 安全設計の方針</p> <p>1.1.5 安全保護系設計の基本方針</p> <p>原子炉保護系及び工学的安全施設の作動を開始させるための安全保護系は、原子炉保護系及び工学的安全施設作動回路からなり、多重性と独立性とを有する設計とし、単一故障を仮定しても、その安全保護機能が妨げられないような設計とする。また、安全保護系は、系の遮断、駆動源の喪失等においても安全上許容される状態（フェイル・セーフ又はフェイル・アズ・イズ）になるよう設計する。</p> <p>安全保護系については、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。 【説明資料（2.1：P24 条-27,28）（2.2：P24 条 28-31）（2.3：P24 条-32）（2.4：P24 条-33）（2.5：P24 条-34,35）（2.6：P24 条-36）（2.7：P24 条-37,38）】</p>	<p>(2)安全設計方針</p> <p>1. 安全設計</p> <p>1.1 安全設計の方針</p> <p>1.1.5 計測制御系統施設設計の基本方針</p> <p>1.1.5.1 原子炉制御設備 運転及び制御保護動作に必要な中性子束、温度、圧力等を測定する原子炉計装及びプロセス計装を設けるとともに、通常運転時に起こり得る設計負荷変化及び外乱に対して自動的に原子炉を制御する原子炉制御設備を設ける。</p> <p>1.1.5.2 監視警報装置 通常運転時に異常、故障が発生した場合は、これを早期に検知し所要の対策が講じられるよう中性子束、温度、圧力、放射能等を常時自動的に監視し、警報を発する装置を設ける。 また、誤動作・誤操作による異常、故障の拡大を防止し事故への進展を確実に防止するようインターロックを設ける。</p> <p>1.1.5.3 原子炉保護設備 炉心及び原子炉冷却材圧力バウンダリの健全性が損なわれることのないよう異常状態へ接近するのを検知し、原子炉トリップを行うために原子炉保護設備を設ける。 原子炉保護設備は、多重性及び独立性を有する設計とし、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り外しを行った場合においても、その安全保護機能が妨げられない設計とするとともに、原子炉運転中に試験できる設計とする。また、原子炉保護設備は、駆動源の喪失、系統の遮断等においても最終的に発電用原子炉施設が安全な状態に落ち着く設計（フェイル・セーフ又はフェイル・アズ・イズ）とする。</p> <p>1.1.5.4 工学的安全施設作動設備 1次冷却材喪失等の設計基準事故時に、炉心及び原子炉格納容器バウンダリを保護するため、工学的安全施設を作動させる工学的安全施設作動設備を設ける。工学的安全施設作動設備は、原子炉保護設備と同様に高い信頼性が得られるよう設計する。</p> <p>1.1.5.5 安全保護回路不正アクセス防止 安全保護系については、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。 【説明資料（2.1：P24 条-30,31）（2.2：P24 条 31）（2.3：P24 条-31,32）（2.4：P24 条-33）（2.5：P24 条-33）（2.6：P24 条-34-36）（2.7：P24 条-37）（2.9：P24 条-40）】</p> <p>1.1.5.6 安全保護回路共用禁止 安全保護回路は2基以上の発電用原子炉施設間で共用しない設計とする。</p>	<p>記載の充実（追加要求事項の対象外、大飯参照）</p> <p>記載の充実（追加要求事項の対象外、大飯参照）</p> <p>記載の充実（追加要求事項の対象外、大飯参照）</p> <p>既許可記載の相違</p> <p>記載の充実（追加要求事項の対象外、大飯参照）</p> <p>記載表現の相違（安全保護回路／系）</p> <p>記載表現の相違（女川実績の反映）</p> <p>記載の充実（追加要求事項の対象外、大飯参照）</p>

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

第24条 安全保護回路

大阪発電所3/4号炉（リファレンスプラント）	女川原子力発電所2号炉	泊発電所3号炉	相違理由
<p>(3) 適合性説明 第二十四条 安全保護回路</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>適合のための設計方針 第1項第1号について</p> <p>安全保護系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、原子炉停止系統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作動させ、燃料要素の許容損傷限界を超えることがない設計とする。</p> <p>また、制御棒クラスタの連続引抜きのような原子炉停止系統の単一の誤動作に対し、炉心を過出力状態から保護するための「中性子束高原子炉トリップ」信号、「過大出力ΔT高原子炉トリップ」信号を設けるほか、燃料被覆管の損傷を防止するための「過大温度ΔT高原子炉トリップ」信号等を設け、これらの信号によって原子炉を自動的に停止させ、燃料要素の許容損傷限界を超えることがない設計とする。</p>	<p>(3) 適合性説明 (安全保護回路)</p> <p>第二十四条 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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>適合のための設計方針 第1項第1号について</p> <p>(1) 安全保護系は、運転時の異常な過渡変化時に、中性子束及び原子炉圧力等の変化を検出し、原子炉保護系を含む適切な系統の作動を自動的に開始させ、燃料要素の許容損傷限界を超えることがない設計とする。</p> <p>(2) 安全保護系は、偶発的な制御棒引抜きのような原子炉停止系のいかなる単一の誤動作に起因する異常な反応度印加が生じた場合でも、燃料要素の許容損傷限界を超えないよう、中性子束高スクラム及び原子炉周期短スクラムにより発電用原子炉を停止できる設計とする。</p>	<p>(3) 適合性説明 第二十四条 安全保護回路</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>適合のための設計方針 第1項第1号について</p> <p>安全保護系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、原子炉停止系統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作動させ、燃料要素の許容損傷限界を超えることがない設計とする。</p> <p>また、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、反応度制御系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、燃料要素の許容損傷限界を超えないよう、「出力領域中性子束高」信号、「過大出力ΔT高」信号、「過大温度ΔT高」信号等により原子炉を自動的に停止できる設計とする。</p>	<p>記載の充実（追加要求事項の対象外、大飯参照）</p> <p>既許可記載の相違</p>

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

第24条 安全保護回路

大飯発電所3/4号炉（リファレンスプラント）	女川原子力発電所2号炉	泊発電所3号炉	相違理由
<p>第1項第2号について</p> <p>安全保護系は、設計基準事故時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、1次冷却材喪失事故等の事故を検知した場合には、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とともに、必要に応じて工学的安全施設作動設備が動作して非常用炉心冷却設備、原子炉格納容器隔離弁あるいは原子炉格納容器スプレイ設備等の工学的安全施設を自動的に動作させる設計とする。</p>	<p>第1項第2号について</p> <p>安全保護系は、設計基準事故時に異常状態を検知し、原子炉保護系を自動的に作動させる。また、自動的に主蒸気隔離弁の閉鎖、非常用炉心冷却系の起動、非常用ガス処理系の起動を行わせる等の保護機能を有する設計とする。</p> <p>(1) 発電用原子炉は、下記の条件の場合にスクラムする。</p> <ul style="list-style-type: none"> a. 原子炉圧力高 b. 原子炉水位低 c. ドライウエル圧力高 d. 中性子束高（平均出力領域モニタ） e. 中間領域における原子炉周期短（起動領域モニタ） f. 中性子束計装動作不能（起動及び平均出力領域モニタ） g. スクラム排出容器水位高 h. 主蒸気隔離弁閉 i. 主蒸気止め弁閉 j. 蒸気加減弁急速閉 k. 主蒸気管放射能高 l. 地震加速度大 m. 手動 n. モードスイッチ「停止」 <p>(2) その他の主要な安全保護系（工学的安全施設作動回路）には、次のようなものを設ける設計とする。</p> <ul style="list-style-type: none"> a. 原子炉水位低、主蒸気管放射能高、主蒸気管圧力低、主蒸気管流量大、主蒸気管トンネル温度高、主復水器真空度低のいずれかの信号による主蒸気隔離弁閉鎖 b. ドライウエル圧力高、原子炉水位低、原子炉建屋原子炉棟放射能高のいずれかの信号による常用換気系の閉鎖と非常用ガス処理系の起動 c. 原子炉水位低又はドライウエル圧力高の信号による高圧炉心スプレイ系、低圧炉心スプレイ系及び低圧注水系の起動 d. 原子炉水位低及びドライウエル圧力高の同時信号による自動減圧系の作動 e. 原子炉水位低又はドライウエル圧力高の信号による高圧炉心スプレイ系ディーゼル発電機及び非常用ディーゼル発電機の起動 f. 原子炉水位低又はドライウエル圧力高の信号による主蒸気隔離弁以外の隔離弁の閉鎖 	<p>第1項第2号について</p> <p>安全保護系は、設計基準事故時に、その異常な状態を検知し、原子炉停止系の作動を自動的に開始させる設計とする。また、非常用炉心冷却設備の作動、原子炉格納容器隔離弁の閉止、原子炉格納容器スプレイ設備の作動等の工学的安全施設の作動を自動的に開始させる設計とする。</p> <p>(1) 原子炉は、以下の条件の場合にトリップする。</p> <ul style="list-style-type: none"> a. 中性子源領域中性子束高 b. 中間領域中性子束高 c. 出力領域中性子束高 d. 出力領域中性子束変化率高 e. 非常用炉心冷却設備作動 f. 過大温度 ΔT 高 g. 過大出力 ΔT 高 h. 原子炉圧力高 i. 原子炉圧力低 j. 加圧器水位高 k. 1次冷却材流量低 l. 1次冷却材ポンプ電源電圧低 m. 1次冷却材ポンプ電源周波数低 n. タービントリップ o. 蒸気発生器水位低 p. 地震加速度大 q. 手動 <p>(2) 工学的安全施設は、以下のとおり作動する。</p> <ul style="list-style-type: none"> 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止 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止 なお、手動操作で上記動作を行うことができる。 	<p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p>
<p>第1項第3号について</p> <p>安全保護系は、多重性を有するチャンネル構成とし、チャンネルの単</p>	<p>第1項第3号について</p> <p>安全保護系は、十分に信頼性のある少なくとも2チャンネルの保護回</p>	<p>第1項第3号について</p> <p>安全保護系は、十分に信頼性のあるチャンネルにより原則として4チ</p>	<p>既許可記載の相違</p>

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

第24条 安全保護回路

大飯発電所3/4号炉（リファレンスプラント）	女川原子力発電所2号炉	泊発電所3号炉	相違理由
<p>一故障又は使用状態からの単一の取り外しを考慮しても、安全保護機能を果たす設計とする。</p> <p>(1) 安全保護系は、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設計基準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、偽の信号発生等による誤動作を防止するため、「2 out of 3」又は「2 out of 4」構成とする。</p> <p>(2) 例外として、プラント起動時等、その安全保護機能を必要とする期間が短期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ら「1 out of 2」構成とする。</p> <p>第1項第4号について 安全保護回路を構成するチャンネルは、チャンネル毎に専用のケーブルトレイ、計装盤等を設けるとともに、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物理的、電気的に分離し、独立性を図る設計とする。また、各チャンネルの電源も無停電電源4母線から独立に供給する設計とする。</p>	<p>路で構成し、機器又はチャンネルの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、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。</p> <p>具体例は下記のとおりである。</p> <p>(1) 原子炉保護系は、検出器、トリップ接点、論理回路、主トリップ継電器等で構成し、基本的に二重の「1 out of 2」方式とする。</p> <p>安全保護機能を維持するため、原子炉保護系作動回路は、運転中全て励磁状態にあり、電源の喪失、継電器の断線及び検出器を取り外した場合、回路が無励磁状態で、チャンネル・トリップになるようにする。したがって、これらの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維持できる。</p> <p>核計装系は、安全保護回路として必要な最小チャンネル数よりも一つ以上多いチャンネルを持ち、運転中でもバイパスして保守、調整及び校正できる。</p> <p>したがって、これが故障の場合、故障チャンネルはバイパスし、残りのチャンネルにより安全保護回路の機能が維持できる。</p> <p>(2) 工学的安全施設を作動させるチャンネル（検出器を含む。）は、多重性をもった構成とする。</p> <p>したがって、これらの単一故障、使用状態からの単一の取外しを行った場合においても、安全保護機能は維持できる。</p> <p>第1項第4号について 安全保護系は、その系を構成するチャンネル相互が分離され、また計測制御系からも原則として分離し、独立性を持つ設計とする。</p> <p>具体例は下記のとおりである。</p> <p>(1) 原子炉格納容器を貫通する計装配管は、物理的に独立した貫通部を有する2系列を設ける。</p>	<p>チャンネルで構成し、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り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。</p> <p>具体的には次のとおりである。</p> <p>(1) 原子炉保護設備は、原子炉トリップ演算処理装置、トリップチャンネル、原子炉トリップ遮断器等で構成し、「2 out of 4」方式とする。原子炉トリップ演算処理装置及びトリップチャンネルは各々四つ設け、検出器は原子炉トリップ演算処理装置ごとに設ける。</p> <p>原子炉トリップ演算処理装置は、安全保護回路のプロセス計装等からの信号を入力し、原子炉トリップ演算を実施する。この信号が設定値に達した場合、チャンネルトリップ信号を発信する。</p> <p>トリップチャンネルは、各々四つの原子炉トリップ演算処理装置からの信号を入力し、二つ以上の原子炉トリップ演算処理装置の動作により原子炉トリップ信号を発信する。</p> <p>各トリップチャンネルからの信号は、対応するトリップチャンネルに属する原子炉トリップ遮断器に入力され、二つ以上のトリップチャンネルが原子炉トリップ信号を発信した場合、原子炉がトリップする設計とする。</p> <p>(2) 工学的安全施設作動設備は、工学的安全施設作動演算処理装置、工学的安全施設作動装置等で構成し、「2 out of 4」方式とする。工学的安全施設作動演算処理装置は四つ、工学的安全施設作動装置は二つ設ける。</p> <p>工学的安全施設作動演算処理装置は、安全保護回路のプロセス計装からの信号を入力し、工学的安全施設作動演算を実施する。この信号が設定値に達した場合、チャンネルトリップ信号を発信する。</p> <p>工学的安全施設作動装置は、各々四つの工学的安全施設作動演算処理装置からの信号を入力し、二つ以上の工学的安全施設作動演算処理装置の動作により工学的安全施設作動信号を発信する。</p> <p>(3) 原子炉起動時等その安全保護機能を必要とする期間が短期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ら、原子炉保護設備のうち「中性子源領域中性子束高」及び「中間領域中性子束高」原子炉トリップは「1 out of 2」方式とする。</p> <p>第1項第4号について 安全保護系は、通常運転時、保守時、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が分離され、また計測制御系からも原則として分離し、それぞれのチャンネル間の独立性を確保した設計とする。</p> <p>具体的には次のとおりである。</p>	<p>相違理由</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>【女川】 設備の相違（計装配管の共用）</p>

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

第24条 安全保護回路

大飯発電所3/4号炉（リファレンスプラント）	女川原子力発電所2号炉	泊発電所3号炉	相違理由
<p>第1項第5号について 原子炉保護系の演算処理装置、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よう設計する。 その他の安全保護回路は、多重化し、物理的にも分離することによって、計測チャンネル又は論理回路トレインに単一故障が生じても安全側に落着くか、又は、そのままの状態にとどまって安全上支障がない状態を維持できるよう設計する。</p>	<p>(2) 検出器からのケーブル及び電源ケーブルは、独立に中央制御室の各盤に導く。各トリップチャンネルの論理回路は、盤内で独立して設ける。 (3) 原子炉保護系作動回路の電源は、分離・独立した母線から供給する。</p> <p>第1項第5号について 安全保護系の駆動源として電源あるいは空気圧を使用する。</p> <p>この系統に使用する弁等は、フェイル・セーフの設計とする、又は故障と同時に現状維持（フェイル・アズ・イズ）になるようにし、この現状維持の場合でも多重化された他の回路によって保護動作を行うことができる設計とする。 フェイル・セーフとなるものの主要なものを挙げると以下のとおりである。</p> <p>(1) 電源喪失 a. スクラム b. 主蒸気隔離弁閉 c. 格納容器ベント弁閉 (2) 制御用空気喪失 a. スクラム b. 格納容器ベント弁閉</p> <p>また、主蒸気隔離弁以外の工学的安全施設を作動させる安全保護系の場合、駆動源である電源の喪失時には、系統を現状維持とする設計とする。</p> <p>系統の遮断やその他、火災、浸水等不利な状況が発生した場合でも、この工学的安全施設作動回路及び工学的安全施設自体が多重性、独立性を持つことで発電用原子炉施設を十分に安全な状態に導くよう設計する。</p>	<p>(1) 検出器からのケーブル及び電源ケーブルは、チャンネル毎に専用のケーブルトレイ等を設け、独立に安全系計装盤室の各盤に導く。各原子炉トリップ演算処理装置等は、各々独立の盤に設ける。 (2) 安全保護系の電源は、相互に分離及び独立した無停電の計装用交流母線から、独立に供給する設計とする。</p> <p>第1項第5号について 安全保護系は駆動源として電力を使用する。原子炉保護設備の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、系統の遮断等に対して原子炉をトリップさせる方向に作動する設計とする。 工学的安全施設作動設備は、駆動源の喪失、系統の遮断等に対してフェイル・セーフとするか、又は故障と同時に現状維持（フェイル・アズ・イズ）になるようにし、この現状維持の場合でも、多重化された他の回路によって工学的安全施設を作動させることができる設計とする。 電源喪失時にフェイル・セーフとなる主要なものは次のとおりである。</p> <p>(1) 原子炉トリップ (2) 原子炉格納容器隔離弁閉（空気作動弁）</p> <p>系統の遮断やその他、火災、浸水等不利な状況が発生した場合でも、この工学的安全施設作動設備及び工学的安全施設自体が多重性、独立性を持つことで発電用原子炉施設を十分に安全な状態に導くよう設計する。</p>	<p>相違理由</p> <p>・泊は、原子炉格納容器を貫通する計装配管について、チャンネル間又は計測制御系と共用している箇所はない。 既許可記載の相違</p> <p>既許可記載の相違</p> <p>【女川】 設備の相違（安全保護系の駆動源） ・泊は、安全保護系の駆動源は電力のみで、制御用空気喪失による原子炉トリップ動作はない。</p> <p>【女川】 設備の相違（フェイル動作） ・泊は、全ての工学的安全施設作動信号について、フェイル・セーフ又はフェイル・アズ・イズのどちらも選択し得る設計としている。</p> <p>記載の充実（追加要求事項の対象外、女川参照）</p>

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

第24条 安全保護回路

大飯発電所3/4号炉（リファレンスプラント）	女川原子力発電所2号炉	泊発電所3号炉	相違理由
<p>第1項第6号について</p> <p>安全保護系のデジタル計算機は、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ことができる設計とする。</p> <p>(1) 安全保護系のデジタル計算機は、これ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ことで物理的に分離し、外部ネットワークへのデータ伝送の必要がある場合は、ゲートウェイを介して一方向通信（送信のみ）にすることにより送信のみに制限することで機能的に分離する設計とする。</p> <p>(2) 安全保護系のデジタル計算機は、外部からの不正アクセスを防止するため、計算機固有のプログラム及び言語を使用し、一般的なコンピュータウィルスが動作しない環境となる設計とする。</p> <p>(3) 安全保護系のデジタル計算機の設計、製作、試験及び変更管理の各段階において、「安全保護系へのデジタル計算機の適用に関する規程（JEAC4620-2008）」及び「デ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）」に準じて、検証及び妥当性確認（コンピュータウィルスの混入防止を含む。）がなされたソフトウェアを使用する設計とする。</p> <p>(4) 不正な変更等による承認されていない動作や変更を防ぐため、発電所出入管理により、物理的アクセスを制限するとともに、安全保護系のデジタル計算機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。</p> <p>【説明資料（2.1、2.2、2.3、2.4、2.5、2.6）】</p>	<p>第1項第6号について</p> <p>安全保護系のうち、一部デジタル演算処理を行う機器は、これが収納された盤の施錠により、ハードウェアを直接接続させない措置を実施することで物理的に分離するとともに、外部ネットワークへのデータ伝送の必要がある場合は、防護装置（通信状態を監視し、送信元、送信先及び送信内容を制限することにより、目的外の通信を遮断）を介して安全保護回路の信号を一方向（送信機能のみ）通信に制限することで機能的に分離するとともに、固有のプログラム言語の使用による一般的なコンピュータウィルスが動作しない環境等によりウィルス等の侵入を防止することでソフトウェアの内部管理の強化を図り、外部からの不正アクセスを防止する設計とする。</p> <p>また、「安全保護系へのデジタル計算機の適用に関する規程」（JEAC4620-2008）及び「デ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）に準じて設計、製作、試験及び変更管理の各段階で検証及び妥当性確認（コンピュータウィルスの混入防止含む。）がなされたソフトウェア又はハードウェア回路を使用するとともに、発電所での出入管理による物理的アクセスの制限及び設定値変更作業での鍵管理により、不正な変更等による承認されていない動作や変更を防止する設計とする。</p> <p>【説明資料（2.1：P24条-27,28）（2.2：P24条28-31）（2.3：P24条-32）（2.4：P24条-33）（2.5：P24条-34,35）（2.6：P24条-36）（2.7：P24条-37,38）】</p>	<p>第1項第6号について</p> <p>安全保護系のデジタル計算機は、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ことができる設計とする。</p> <p>(1) 安全保護系のデジタル計算機は、これ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ことで物理的に分離し、外部ネットワークへのデータ伝送の必要がある場合は、防護装置（一方向のみに通信を許可する装置等）を介して一方向（送信機能のみ）通信に制限することで機能的に分離する設計とする。</p> <p>(2) 安全保護系のデジタル計算機は、外部からの不正アクセスを防止するため、計算機固有のプログラム及び言語を使用し、一般的なコンピュータウィルスが動作しない環境となる設計とする。</p> <p>(3) 安全保護系のデジタル計算機の設計、製作、試験及び変更管理の各段階において、「安全保護系へのデジタル計算機の適用に関する規程（JEAC4620-2008）」及び「デ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）」に準じて、検証及び妥当性確認（コンピュータウィルスの混入防止含む。）がなされたソフトウェアを使用する設計とする。</p> <p>(4) 不正な変更等による承認されていない動作や変更を防ぐため、発電所出入管理により、物理的アクセスを制限するとともに、安全保護系のデジタル計算機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。</p> <p>【説明資料（2.1：P24条-30,31）（2.2：P24条31）（2.3：P24条-31,32）（2.4：P24条-33）（2.5：P24条-33）（2.6：P24条-34-36）（2.7：P24条-37）（2.9：P24条-40）】</p>	<p>相違理由</p> <p>設備の相違 []</p> <p>泊は、「防護装置（一方向のみに通信を許可する装置）」を根幹の対策として、「ゲートウェイ【大飯】」及び「防護装置（通信状態を監視し、送信元、送信先及び送信内容を制限することにより、目的外の通信を遮断）」【女川】も設置した多層防護としている。</p> <p>記載表現の相違（女川実績の反映）</p> <p>【女川】設備の相違（ハードウェア回路）</p> <p>記載表現の相違（女川実績の反映）</p> <p>【女川】設備の相違（計装配管の共用）</p>
<p>第1項第7号について</p> <p>安全保護系は、計測制御系から分離した設計とする。</p>	<p>第1項第7号について</p> <p>安全保護系と計測制御系とは電源、検出器、ケーブル・ルート及び原子炉格納容器を貫通する計装配管を、原則として分離する設計とする。</p> <p>安全保護系は、原子炉水位及び原子炉圧力を検出する計装配管ヘッド</p>	<p>第1項第7号について</p> <p>安全保護系は、計測制御系から分離した設計とする。</p>	<p>【女川】設備の相違（計装配管の共用）</p>

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

第24条 安全保護回路

大飯発電所3/4号炉（リファレンスプラント）	女川原子力発電所2号炉	泊発電所3号炉	相違理由
<p>安全保護系の一部から計測制御系への信号を取り出す場合には、信号の分岐箇所にて光変換カード又は絶縁増幅器を使用し、計測制御系で回路の短絡、開放等の故障が生じて安全保護系への影響を与えない設計とする。</p> <p>また、安全保護系と計測制御系の盤、ケーブル、ケーブルトレイ等は原則として物理的に分離した配置とする。</p> <p>1.3 気象等 該当なし</p>	<p>の一部を計測制御系と共用すること及び原子炉核計装の検出部が表示、記録計用検出部と共用される以外は計測制御系とは完全に分離する等、計測制御系での故障が安全保護系に影響を与えない設計とする。</p> <p>安全保護系と計測制御系で計装配管を共用する場合は、安全保護系の計装配管として設計する。</p> <p>また、原子炉核計装の検出部が表示、記録計用検出部と共用しているが、計測制御系の短絡、地絡又は断線によって安全保護系に影響を与えない設計とする。</p> <p>1.3 気象等 該当なし</p>	<p>安全保護系の一部から計測制御系への信号を取り出す場合には、信号の分岐箇所にて光変換カード又は絶縁増幅器を使用し、計測制御系で回路の短絡、開放等の故障が生じて安全保護系へ影響を与えない設計とする。</p> <p>また、安全保護系と計測制御系とは電源、検出器及びケーブルルートを、原則として分離する設計とする。</p> <p>1.3 気象等 該当なし</p>	<p>・泊は、原子炉格納容器を貫通する計装配管について、安全保護系と計測制御系とで共用している箇所はない。</p> <p>既許可記載の相違</p>

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

第24条 安全保護回路

大飯発電所3/4号炉（リファレンスプラント）	女川原子力発電所2号炉	泊発電所3号炉	相違理由
<p>1.4 設備等（手順等含む）</p> <p>6. 計測制御系統施設</p> <p>6.3 プロセス計装</p> <p>6.3.1 概要</p> <p>プラントの適切かつ安全な運転のために1次冷却系をはじめとし、各補助系における必要なプロセス量の測定を行い、その信号の一部は、原子炉保護設備、工学的安全施設作動設備、原子炉制御設備に用いる。</p> <p>プロセス計装設備は、検出器のほかに、演算処理装置を収納する計装盤から構成し、主要なパラメータは、中央制御盤に指示、記録及び警報の発信を行う。</p> <p>原子炉の停止及び炉心冷却並びに放射性物質の閉じ込めの機能の状況を監視するために必要なパラメータは、設計基準事故時においても監視でき確実に記録及び保存ができる。</p> <p>6.3.2 設計方針</p> <p>(1) 安全保護回路のプロセス計装は、以下の方針で設計する。</p> <p>c. 安全保護回路のプロセス計装は、単一故障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、安全保護機能を喪失しないよう多重性を確保する設計とする。</p> <p>d. 安全保護回路のプロセス計装は、チャンネル相互を分離し、それぞれのチャンネル間において独立性を確保する設計とする。</p> <p>a. 安全保護回路のプロセス計装は、運転時の異常な過渡変化が生じた場合において、その異常な状態を検知し、原子炉停止系統及び必要な工学的安全施設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設計とする。</p> <p>b. 安全保護回路のプロセス計装は、設計基準事故時に、その異常な状態を検知し、原子炉停止系統及び必要な工学的安全施設を含む適切な系統を自動で作動する設計とする。</p>	<p>1.4 設備等（手順等含む）</p> <p>6. 計測制御系統施設</p> <p>6.3 原子炉プラント・プロセス計装</p> <p>6.3.1 概要</p> <p>発電用原子炉の適切かつ安全な運転のため、原子炉核計装のほかに、発電用原子炉施設の重要な部分には全てプロセス計装を設ける。原子炉プラント・プロセス計装は、温度、圧力、流量、水位等を測定及び指示するものであるが、一部を除き必要な指示及び記録計器は全て中央制御室に設置する。</p> <p>原子炉プラント・プロセス計装は、压力容器計装、再循環系計装、給水系計装、主蒸気系計装、制御棒駆動系計装等の計装で構成する。</p> <p>発電用原子炉の停止、炉心冷却及び放射性物質の閉じ込めの機能の状況を監視するために必要なパラメータは、設計基準事故時においても監視でき、確実に記録及び保存ができる。</p> <p>6.3.2 設計方針</p> <p>原子炉プラント・プロセス計装は、以下の設計方針を満足するように設計する。</p> <p>(1) 通常運転時及び運転時の異常な過渡変化時において、炉心、原子炉冷却材圧力バウンダリ及び原子炉格納容器バウンダリ、並びにそれらに関連する系統の健全性を確保するために必要なパラメータは、予想変動範囲内での監視が可能であるようにプロセス計装を設ける。</p> <p>(2) 設計基準事故時において、事故の状態を知り対策を講じるのに必要なパラメータを監視できるよう、プロセス計装を設けるよう設計する。</p>	<p>1.4 設備等（手順等含む）</p> <p>6. 計測制御設備</p> <p>6.3 プロセス計装</p> <p>6.3.1 概要</p> <p>プロセス計装は、発電用原子炉施設の適切かつ安全な運転のために必要なプロセス量の測定を行い、その信号の一部は、原子炉保護設備、工学的安全施設作動設備及び原子炉制御設備に用いる。</p> <p>プロセス計装は、温度、圧力、流量、水位等の測定を行い、主要なパラメータは、中央制御盤で監視でき、必要なものは警報を発信する。</p> <p>原子炉の停止及び炉心冷却並びに放射性物質の閉じ込めの機能の状況を監視するために必要なパラメータは、設計基準事故時においても監視でき確実に記録及び保存ができる。</p> <p>6.3.2 設計方針</p> <p>(1) 安全保護回路のプロセス計装は、以下の方針で設計する。</p> <p>a. 多重性</p> <p>安全保護回路のプロセス計装は、その系統を構成する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り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。</p> <p>b. 独立性</p> <p>安全保護回路のプロセス計装は、通常運転時、保守時、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確保した設計とする。</p> <p>c. 通常運転時及び運転時の異常な過渡変化時の機能</p> <p>安全保護回路のプロセス計装は、通常運転時及び運転時の異常な過渡変化時において、炉心、原子炉冷却材圧力バウンダリ、原子炉格納容器バウンダリ及びそれらに関連する設備の健全性を確保するために必要なパラメータについて、必要な対策が講じ得るように予想変動範囲内で監視できる設計とする。</p> <p>さらに、運転時の異常な過渡変化時において、その異常な状態を検知し、原子炉をトリップさせ、燃料要素の許容損傷限界を超えない設計とする。</p> <p>d. 設計基準事故時の機能</p> <p>安全保護回路のプロセス計装は、設計基準事故時において、その異常な状態を検知し、原子炉トリップ及び必要な工学的安全施設を自動的に作動させる設計とする。</p>	<p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p>

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

第24条 安全保護回路

大飯発電所3/4号炉（リファレンスプラント）	女川原子力発電所2号炉	泊発電所3号炉	相違理由
<p>e. 安全保護回路のプロセス計装は、駆動源の喪失、系統の遮断その他考慮すべき不利な状況に対して最終的に安全な状態に落ち着くような設計とする。</p> <p>f. 安全保護回路のプロセス計装は、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。</p> <p>g. 安全保護回路のプロセス計装は、計測制御系と分離した設計とし、安全保護回路の一部を計測制御系と共用する場合には、計測制御系の故障、誤操作若しくは使用状態からの単一の取り外しが波及し、その安全保護機能を失わないように、機能的に分離する設計とする。</p> <p>j. 安全保護回路のプロセス計装は、原子炉の運転中に定期的に試験を行い、機能が喪失していないことを確認できるような設計とする。</p> <p>h. 安全確保上最も重要な原子炉停止、炉心冷却及び放射能閉じ込めの3つの機能の状況を監視するのに必要な炉心の中性子束、原子炉水位及び原子炉冷却系の圧力及び温度等は、設計基準事故時においても記録されるとともに事象経過後に参照できるよう当該記録が保存できる設計とする。</p> <p>i. 安全保護回路のプロセス計装は、2基以上の原子炉施設間で共用又は相互に接続しない設計とする。</p>	<p>(3) 安全保護系に関連する原子炉プラント・プロセス計装は、「6.6 安全保護系」に記載する設計方針(4)～(9)を満足するように設計する。</p> <p>(4) 原子炉冷却材圧力バウンダリからの冷却材の漏えいがあった場合、その漏えいを検出するのに必要なプロセス計装を設けるものとする。</p> <p>(5) 安全確保上最も重要な原子炉停止、炉心冷却及び放射能閉じ込めの3つの機能の状況を監視するのに必要な炉心の中性子束、原子炉水位、原子炉冷却材系の圧力及び温度等は、設計基準事故時においても記録されるとともに事象経過後に参照できるように当該記録が保存できる設計とする。</p>	<p>e. 故障時の機能 安全保護回路のプロセス計装は、駆動源の喪失、系統の遮断等が生じた場合においても、最終的に発電用原子炉施設が安全な状態に落ち着く設計とする。</p> <p>f. 不正アクセス防止 安全保護回路のプロセス計装は、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。</p> <p>g. 計測制御系との分離 安全保護回路のプロセス計装は、計測制御系とは機能的に分離した設計とする。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、安全保護系に影響を与えない設計とする。</p> <p>h. 試験可能性 安全保護回路のプロセス計装は、原子炉の運転中に定期的に試験及び検査ができるとともに、その健全性及び多重性の維持を確認するため、独立に各チャンネルの試験及び検査ができる設計とする。</p> <p>i. 電源喪失に対する考慮 安全保護回路のプロセス計装の電源は、無停電の計装用交流母線から給電し、一定時間の全交流動力電源喪失時にも機能を喪失しない設計とする。</p> <p>j. 記録及び保存 安全確保上最も重要な原子炉停止、炉心冷却及び放射能閉じ込めの3つの機能の状況を監視するのに必要な炉心の中性子束、原子炉水位、原子炉冷却系の圧力及び温度等は、設計基準事故時においても記録されるとともに事象経過後に参照できるよう当該記録が保存できる設計とする。</p> <p>k. 共用禁止 安全保護回路のプロセス計装は、2基以上の発電用原子炉施設間で共用又は相互に接続しない設計とする。</p>	<p>既許可記載の相違</p> <p>既許可構成の相違</p> <p>【女川】 記載内容の相違(漏えい検出装置) ・泊において、一次冷却材の漏えい検出装置は一次冷却材設備であり、プロセス計装ではない。</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>既許可構成の相違 記載の充実(追加要求事項の対象外、大飯参照)</p>

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

第24条 安全保護回路

大飯発電所3/4号炉（リファレンスプラント）	女川原子力発電所2号炉	泊発電所3号炉	相違理由
<p>(2) 安全保護回路以外の主要なプロセス計装としては、1次冷却系計装、補助給水系計装、燃料取替用水系計装等があり、これらは以下の方針で設計する。</p> <p>a. 通常運転時及び運転時の異常な過渡変化時において主要なパラメータは、予想変動範囲での監視、記録ができるよう設計する。</p> <p>また、事故時において事故の状態を知り対策を講じるために必要なパラメータは監視、記録できるようにする。</p> <p>c. 主要なプロセス計装の電源は、無停電電源装置より給電する。</p> <p>b. プロセス計装の主要なパラメータは中央制御盤で監視できるようにする。</p> <p>6.3.4 主要設備 6.3.4.1 安全保護回路のプロセス計装 原子炉保護設備及び工学的安全施設作動設備に信号を供給する安全保護回路のプロセス計装は、検出器のほかに演算処理装置を収納する計装盤から構成される。安全保護回路のプロセス計装を第6.3.1表に示す。</p> <p>ここにも示すとおり、これらの計装は単一故障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、安全保護機能を喪失しないよう多重化しており、それぞれのチャンネルは、独立した計装盤に収納することにより物理的に分離している。</p> <p>また、これらの計装に必要な電源は、4台の無停電電源装置からそれぞれ独立に給電すると共に、検出器と計装盤間等の関連する配線もチャンネル相互に分離し電気的にも独立性を保つようにする。</p> <p>さらに、安全保護回路のプロセス計装の信号を制御系に使用する場合には、光変換カード又は絶縁増幅器により両者の間を絶縁し、制御系に</p>	<p>6.3.4 主要設備 (1) 圧力容器計装 原子炉圧力容器について計測する主要な項目は、発電用原子炉の水位及び圧力、原子炉圧力容器胴部の温度及びフランジ部シールの漏えいである。</p> <p>原子炉水位は、連続的に測定し、指示及び記録する。原子炉水位低又は水位高で警報する。原子炉水位低下が更に大きい場合には、原子炉停止（原子炉スクラム）系、工学的安全施設及び原子炉隔離時冷却系を作動させるとともに原子炉再循環ポンプを停止する信号を出す。また、原子炉水位上昇が更に大きい場合にはタービン・トリップを行わせるための信号を出す（第6.3-1図、第6.6-4図、第6.6-5図、第6.6-6図参照）。</p> <p>原子炉圧力は、連続的に測定し、指示及び記録する。原子炉圧力高で警報する。</p> <p>また、原子炉圧力が更に上昇する場合に、原子炉スクラムや主蒸気逃がし安全弁開放等の保護動作を行わせるための信号を出す（第6.6-4図及び「5.1.1.4.3.3 主蒸気逃がし安全弁」参照）。</p> <p>原子炉圧力容器胴部の温度は、上部、中間部、下部について測定し、</p>	<p>(2) 安全保護回路以外のプロセス計装は、以下の方針で設計する。</p> <p>a. 通常運転時及び運転時の異常な過渡変化時の監視 安全保護回路以外のプロセス計装は、通常運転時及び運転時の異常な過渡変化時において、炉心、原子炉冷却材圧力バウンダリ、原子炉格納容器バウンダリ及びそれらに関連する設備の健全性を確保するために必要なパラメータについて、必要な対策が講じ得るように予想変動範囲内で監視、記録ができる設計とする。</p> <p>b. 事故時の監視 安全保護回路以外のプロセス計装は、事故時において、事故の状態を知り対策を講じるのに必要なパラメータを適切な方法で十分な範囲にわたり監視でき、必要なものは記録できる設計とする。</p> <p>c. 試験可能性 安全保護回路以外のプロセス計装は、試験及び検査ができる設計とする。</p> <p>d. 電源喪失に対する考慮 安全保護回路以外の主要なプロセス計装の電源は、無停電の計装用交流母線から給電し、一定時間の全交流動力電源喪失時にも機能を喪失しない設計とする。</p> <p>e. 中央制御盤での監視 プロセス計装の主要なパラメータは中央制御盤で監視できるようにする。</p> <p>6.3.3 主要設備 (1) 安全保護回路のプロセス計装 安全保護回路のプロセス計装は、検出器、デジタル演算処理装置等で構成する。安全保護回路のプロセス計装を第6.3.1表に示す。</p> <p>これらの計装は単一故障あるいは使用状態からの単一の取り外しを行ってもその安全保護機能を失わないよう多重化されている。デジタル演算処理装置はチャンネルごとに独立したラックに収納するとともに、検出器とラック間等の関連する配線も専用のケーブルトレイ等を設け、チャンネル相互間を物理的に分離する。</p> <p>安全保護回路のプロセス計装の電源は、無停電の計装用交流母線からそれぞれ独立に給電することにより、チャンネル相互間を電気的に分離する。</p> <p>ラック及び配線は、実用上可能な限り不燃性又は難燃性材料を使用する。</p> <p>安全保護回路のプロセス計装の信号を制御系に使用する場合には、光変換カード又は絶縁増幅器により両者の間を絶縁し、制御系に生じた短</p>	<p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>既許可構成の相違 記載の充実（追加要求事項の対象外、大飯参照）</p> <p>既許可記載の相違 【女川】 既許可構成の相違 ・炉型の相違による安全保護系の設備構成の相違に伴い、泊と女川では既許可構成が大幅に異なる。</p> <p>記載表現の相違</p>

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

第24条 安全保護回路

大阪発電所3/4号炉（リファレンスプラント）	女川原子力発電所2号炉	泊発電所3号炉	相違理由
<p>生じた短絡、地絡又は断線による故障が安全保護回路に影響を与えることのないようにする。</p> <p style="text-align: center;">【説明資料（2.1、2.2、2.3）】</p> <p>これらの計装の機能をテストする場合には、検出器の出力信号回路に模擬入力を印加することにより、規定の設定値において、必要な動作を確認することができる。また、多重化した検出器は、チャンネル相互の信号を比較することにより、原子炉運転中にもその健全性を確認できる。</p> <p>なお、安全保護回路のプロセス計装の計測信号はすべて中央制御盤上に指示、又は記録し、プラントの適切かつ安全な運転ができるようにする。</p> <p>なお、加圧器水位、主蒸気ライン圧力、原子炉格納容器圧力及び蒸気発生器水位については、事故時において監視、記録できるものとする。</p> <p>6.3.4.2 安全保護回路以外のプロセス計装</p> <p>安全保護系以外の主要なプロセス計装は、次の計装により監視又は記録できるようにする。</p> <p>また、事故時において事故の状態を知り対策を講じるに必要なプロセス計装は第6.3.2表に示すとおりであり、これらは監視、記録できるようにする。</p> <p>(1) 1次冷却系計装</p> <p>1次冷却系計装では、1次冷却材の温度、圧力、サブクール度、加圧器スプレイラインの温度、加圧器逃がしラインの温度、加圧器逃がしタンクの温度、圧力、水位、1次冷却材ポンプの振動、軸受温度、冷却水温度等を連続的に指示又は記録し、必要なものについては警報を発する。</p> <p>なお、炉心冷却状態監視を補助するものとして原子炉水位計を設ける。</p> <p>(2) 化学体積制御系計装</p> <p>化学体積制御系計装では、抽出ラインの圧力、温度、流量、体積制御タンクの圧力、水位、充てんラインの温度、流量、1次冷却材ポンプ封水ラインの温度、流量、原子炉補給水の流量、ほう酸タンクの温度、水位等を指示又は記録し、必要なものについては警報を発する。</p> <p>(3) 主蒸気及び給水、補助給水系計装</p> <p>主蒸気及び給水の圧力、温度、補助給水流量、復水ビット水位等を指示又は記録し、必要なものについては警報を発する。</p> <p>(4) 燃料取替用水系計装</p> <p>燃料取替用水ビット水位等を指示又は記録し、必要なものについては</p>	<p>記録する。原子炉圧力容器上蓋のフランジ部シールの漏れは、2個のOリング間のフランジ面に接続されたドレンラインで検出する。内側のOリングからの漏れは、ドレンラインに設けた圧力検出器によって検出し、圧力高で警報する。</p> <p>(2) 再循環系計装</p> <p>再循環系では、再循環流量、冷却材温度、原子炉再循環ポンプ出入口差圧及び静止形原子炉再循環ポンプ電源装置の出力周波数を連続的に測定し指示、又は記録する。</p> <p>また、炉心流量はジェットポンプのディフューザの差圧により測定する。</p> <p>原子炉再循環ポンプについては、シール漏れ流量、冷却材流量及び温度を計測し、シール漏れ流量高、冷却水流量低及び温度高で警報を出す。また、軸受振動、軸受温度等を測定し、振動大、温度高等により警報を出す。</p> <p>(3) 給水系及び主蒸気系計装</p> <p>原子炉給水流量及び主蒸気流量は、連続的に測定し、指示及び記録する。</p> <p>その他タービン第一段圧力などを測定し、指示及び記録する。</p> <p>(4) 制御棒駆動系計装</p> <p>制御棒駆動系では、制御棒駆動水、スクラムアキュムレータ及びスクラム排出容器並びに制御棒位置に対して、それぞれ適切なプロセス計装を設ける。</p> <p>制御棒駆動系では、制御棒駆動水ポンプ入口圧力、フィルタの圧力降下、原子炉圧力と制御棒駆動水圧との差圧、制御棒駆動水のヘッダ部での流量、制御棒駆動機構の温度（位置指示用計器ウェル内）、アキュムレータ窒素圧力、アキュムレータの漏れ水量及びスクラム排出容器水位などを計測する。</p> <p>制御棒駆動水ポンプ入口圧力低、フィルタの圧力降下大、スクラムアキュムレータの窒素圧力低、スクラムアキュムレータ漏れ水量大及びスクラム排出容器水位高で警報する。スクラム排出容器の水位が更に高くなれば制御棒引抜阻止及び原子炉スクラムのための信号を出す。</p> <p>制御棒位置は、制御棒駆動機構の中心部に設けたインジケータチューブ内のリードスイッチによって検出し指示する。</p> <p>(5) 原子炉格納容器内雰囲気計装</p> <p>原子炉格納容器について計測する主要な項目は、原子炉格納容器内の圧力、温度、湿度、水素濃度、酸素濃度及び放射線レベルである。</p> <p>原子炉格納容器内の圧力、温度及び酸素濃度は、連続的に測定し、指示又は記録する。また、冷却材喪失事故後の原子炉格納容器内の圧力、温度、水素濃度、酸素濃度、放射線レベル等も測定し、記録する。そのほか、ドライウェルの湿度並びにサプレッションチェンバ内のプールの水位及び水温も連続的に測定し、指示又は記録する。</p> <p>ドライウェル圧力高、水素濃度高及び酸素濃度高で警報する。ドライ</p>	<p>絡、地絡又は断線による故障が安全保護系に影響を与えることのないようにする。</p> <p>【説明資料（2.2：P24条31）（2.3：P24条-31、32）（2.4：P24条-33）】</p> <p>これらの計装の機能をテストする場合には、検出器の出力信号回路に模擬入力を印加することにより、規定の設定値において、必要な動作を確認することができる。また、多重化した検出器は、チャンネル相互の信号を比較することにより、原子炉運転中にもその健全性を確認できる。</p> <p>安全保護回路のプロセス計装のパラメータは中央制御盤で監視でき、発電用原子炉施設の適切かつ安全な運転ができる。</p> <p>また、加圧器水位、主蒸気ライン圧力、原子炉格納容器圧力及び蒸気発生器水位については、事故時においても中央制御盤で監視できる。</p> <p>(2) 安全保護回路以外のプロセス計装</p> <p>安全保護回路以外のプロセス計装は、以下の計装により中央制御盤で監視できる。</p> <p>また、事故時において事故の状態を知り対策を講じるのに必要なプロセス計装を第6.3.2表に示す。</p> <p>a. 1次冷却設備計装</p> <p>1次冷却設備計装は、1次冷却材の温度・圧力・サブクール度、加圧器スプレイラインの温度、加圧器逃がしラインの温度、加圧器逃がしタンクの温度・圧力・水位、1次冷却材ポンプの振動・軸受温度、原子炉容器水位等を監視し、必要なものについては警報を発信する。</p> <p>b. 化学体積制御設備計装</p> <p>化学体積制御設備計装は、抽出ラインの圧力・温度・流量、体積制御タンクの圧力・水位、充てんラインの温度・流量、1次冷却材ポンプ封水ラインの温度・流量、1次系純水補給ラインの流量、ほう酸補給ラインの流量、ほう酸タンクの温度・水位等を監視し、必要なものについては警報を発信する。</p> <p>c. 主蒸気及び給水設備計装</p> <p>主蒸気及び給水設備計装は、蒸気発生器水位（広域）、主蒸気及び主給水の圧力・温度・流量、補助給水流量、補助給水ビット水位等を監視し、必要なものについては警報を発信する。</p> <p>d. 燃料取替用水系計装</p> <p>燃料取替用水ビット水位等を指示又は記録し、必要なものについては</p>	<p>相違理由</p> <p>記載表現の相違(女川実績の反映)</p> <p>記載の充実(追加要求事項の対象外、大飯参照)</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>既許可構成の相違</p> <p>記載の充実(追加要求)</p>

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

第24条 安全保護回路

大飯発電所3/4号炉（リファレンスプラント）	女川原子力発電所2号炉	泊発電所3号炉	相違理由
<p>警報を発する。</p> <p>(5) 原子炉格納容器関連計装 スプレィ流量、原子炉格納容器内温度、水位等を指示又は記録し、必要なものについては警報を発する。</p> <p>(6) 原子炉補機冷却系計装 原子炉補機冷却水サージタンク水位等を指示又は記録し、必要なものについては警報を発する。</p> <p>(7) 制御用空気系計装 制御用空気圧力等を指示又は記録し、必要なものについては警報を発する。</p> <p>(8) 非常用炉心冷却系計装 高圧及び低圧注入流量等を指示又は記録し、必要なものについては警報を発する。</p> <p>(9) 燃料貯蔵設備計装 使用済燃料ピットの水位及び温度の異常な状態を検知し、中央制御室に警報を発する。 また、外部電源が利用できない場合でも温度、水位その他使用済燃料ピットの状態を示す事項を監視できる設計とする。</p> <p>(10) その他 上記のほかに、放射性廃棄物処理系、使用済燃料ピット水浄化冷却系、試料採取系、蒸気発生器ブローダウン系、原子炉補機冷却海水系等のプロセス計装を設ける。</p> <p>(11) 記録及び保存 安全保護回路以外のプロセス計装で必要なものについては記録及び保存を行う。</p> <p>(12) プラント計算機 中央制御盤によるプラントの状態把握を補助するものとして、所要の処理能力及び記憶容量を有するプラント計算機を設け、主にプロセス計装からの信号を入力し、圧力、温度、流量、放射線レベル等の印字及び画面表示を行う。</p> <p>【まとめ資料作成範囲外のため。設置許可(令和3年5月)より引用】↓</p>	<p>ウェル圧力の上昇が更に大きい場合には、原子炉保護系及び工学的安全施設を作動させるための信号を出す（第6.6-4 図及び第6.6-6 図参照）。</p> <p>サブプレッションチェンバでは、プール水位低、プール水位高、プール水温高、水素濃度高及び酸素濃度高で警報する。</p> <p>(6) 漏えい検出系計装 原子炉冷却材圧力バウンダリからの冷却材の漏えいは、ドライウェル内ガス冷却装置の凝縮水量、ドライウェル内サンプル水量及びドライウェル内ガス中の核分裂生成物の放射能の測定により約3.8ℓ/minの漏えいを1時間以内に検出できるようにする。測定値は、指示するとともに、冷却材の漏えい量が多い場合には警報する。</p> <p>(7) その他の計装 ほう酸水注入系では、ほう酸水貯蔵タンク水位、ほう酸水温度及びポンプ出口圧力を計測し、ほう酸水貯蔵タンク水位低で警報する。 低圧炉心スプレィ系及び残留熱除去系では、ポンプ出口圧力、流量等を測定し、指示する。 高圧炉心スプレィ系では、ポンプ出口圧力及び流量を測定し、指示する。 また、サブプレッションチェンバ内のプール水位高で警報する。 原子炉隔離時冷却系では、ポンプ出口圧力、流量等を測定し、指示する。</p>	<p>警報を発する。</p> <p>e. 原子炉格納施設計装 原子炉格納施設計装は、格納容器スプレィ流量、格納容器内温度、格納容器再循環サンプル水位等を監視し、必要なものについては警報を発信する。</p> <p>f. 原子炉補機冷却水設備計装 原子炉補機冷却水設備計装は、原子炉補機冷却水サージタンク水位等を監視し、必要なものについては警報を発信する。</p> <p>g. 原子炉補機冷却海水設備計装 原子炉補機冷却海水設備計装は、原子炉補機冷却海水母管圧力等を監視し、必要なものについては警報を発信する。</p> <p>h. 制御用圧縮空気設備計装 制御用圧縮空気設備計装は、制御用空気圧力等を監視し、必要なものについては警報を発信する。</p> <p>i. 非常用炉心冷却設備計装 非常用炉心冷却設備計装は、蓄圧タンク圧力・水位、高圧及び低圧注入流量、燃料取替用水ピット水位等を監視し、必要なものについては警報を発信する。</p> <p>j. 燃料貯蔵設備計装 使用済燃料ピットの水位及び水温の異常な状態を検知し、中央制御室に警報を発信する。 また、外部電源が利用できない場合でも水位、水温その他使用済燃料ピットの状態を示す事項を監視できる設計とする。</p> <p>k. その他 上記のほかに、使用済燃料ピット水浄化冷却設備、放射性廃棄物廃棄設備、試料採取設備等のプロセス計装を設ける。</p> <p>l. 記録及び保存 安全保護回路以外のプロセス計装で必要なものについては記録及び保存を行う。</p> <p>m. プラント計算機 中央制御盤による発電用原子炉施設の状態把握を補助するものとしてプラント計算機を設け、プラント性能計算、データの収集、記録等を行う。</p>	<p>事項の対象外、大飯参照)</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>既許可構成の相違 記載の充実(追加要求事項の対象外、大飯参照)</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>既許可構成の相違 記載の充実(追加要求事項の対象外、大飯参照)</p> <p>既許可構成の相違 記載の充実(追加要求事項の対象外、大飯参照)</p> <p>既許可記載の相違</p>

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

第24条 安全保護回路

大飯発電所3/4号炉（リファレンスプラント）	女川原子力発電所2号炉	泊発電所3号炉	相違理由
<p>6.3.3 主要設備の仕様 プロセス計装設備の主要設備の仕様を第 6.3.1 表及び第 6.3.2 表に示す。</p> <p>6.3.6 試験検査 安全保護系のプロセス計装は、原子炉の運転中に定期的に試験を行い、機能が喪失していないことを確認できる。</p> <p>6.3.5 評価 (1) 安全保護系のプロセス計装は多重化されており、単一故障あるいは使用状態からの単一の取外しを行っても安全保護機能を喪失することはない。 (2) 多重化された安全保護系のプロセス計装は、チャンネル間の分離、独立性を図るため、検出器は相互に距離を隔てて設置するとともに、チャンネルごとに独立した計器ラックに機器を収納している。電源及び配線についてもチャンネルごとに独立な構成としている。 また、計器ラック及び配線は、実用上可能な限り、難燃性又は不燃性材料を使用する設計としている。 (3) 安全保護系のプロセス計装の信号を計測制御系に使用する場合には、絶縁増幅器により絶縁し、計測制御系に生じた故障が安全保護系に影響を与えないようにしている。 (4) 安全保護系のプロセス計装は、電源の喪失又は系の遮断に対して原子炉の保護動作をとる方向に作動するように設計している。 (5) 安全保護系のプロセス計装は、原子炉運転中にも検出器の出力信号回路に模擬入力を印加し、規定の設定値において必要な動作がおこなわれることを確認できる。 また、検出器は、多重化されたチャンネル間の信号を相互比較することにより、原子炉運転中にも健全性が確認できる。 (6) 安全保護系のプロセス計装及び安全保護系以外の主要なプロセス計装の電源は、無停電電源装置から給電される。 したがって、短時間の全動力電源喪失に対しても機能を喪失することはない。 また、非常用所内電源系のみ運転下あるいは外部電源のみ運転下で単一故障を仮定しても安全保護機能を失うことはない。 (7) 通常運転時及び運転時の異常な過渡変化時において、加圧器水位、1次冷却材の圧力、温度及び流量、原子炉格納容器圧力等は、予想</p>	<p>6.3.3 主要設備の仕様 原子炉プラント・プロセス計装の一覧を第 6.3-1 表に示す。</p> <p>6.3.5 試験検査 原子炉プラント・プロセス計装は、定期的に試験又は検査を行い、その機能の健全性を確認する。</p> <p>6.3.6 評価 (1) 原子炉プラント・プロセス計装は、通常運転時及び運転時の異常な過渡変化時において、炉心、原子炉冷却材圧力バウンダリ及び格納容器バウンダリ並びにそれらに関連する系統の健全性を確保するために必要なパラメータを予想変動範囲内で監視することができる設計としている。 (2) 原子炉プラント・プロセス計装は、設計基準事故時において、事故の状態を知り対策を講じるのに必要なパラメータを監視することができる設計としている。 (3) 安全保護系に関連する原子炉プラント・プロセス計装は、「6.6 安全保護系」に記載する設計方針(4)～(9)を満足する設計としている。 (4) 原子炉プラント・プロセス計装は、原子炉冷却材圧力バウンダリからの冷却材の漏えいがあった場合、その漏えいを検出することができる設計としている。</p>	<p>6.3.4 主要仕様 安全保護系のプロセス計装を第 6.3.1 表、事故時監視が必要なプロセス計装を第 6.3.2 表に示す。</p> <p>6.3.5 試験検査 プロセス計装は、その機能の健全性を確認するため、定期的に試験及び検査を行う。 (1) 安全保護系のプロセス計装は原則として4チャンネルで構成し、1つの測定パラメータに対して4チャンネルの検出器からの信号を入力する。これらの信号を使用し、“2 out of 4”の論理回路を構成しているため、原子炉運転中でも、任意の1チャンネルについて模擬入力を印加し、健全性を確認することができる。 この場合、残りのチャンネルの信号により、安全保護機能（原子炉トリップ、非常用炉心冷却設備作動等）を維持することができる。 (2) 多重化された安全保護系のプロセス計装は、チャンネル相互の信号を比較することにより、原子炉運転中にもその健全性を確認することができる。</p> <p>6.3.6 評価 (1) 安全保護系のプロセス計装は多重化されており、単一故障あるいは使用状態からの単一の取外しを行っても安全保護機能を喪失することはない。 (2) 多重化された安全保護系のプロセス計装は、チャンネル間の分離、独立性を図るため、検出器は相互に距離を隔てて設置するとともに、チャンネルごとに独立した計器ラックに機器を収納している。電源及び配線についてもチャンネルごとに独立な構成としている。 また、計器ラック及び配線は、実用上可能な限り、難燃性又は不燃性材料を使用する設計としている。 (3) 安全保護系のプロセス計装の信号を計測制御系に使用する場合には、光変換カード又は絶縁増幅器により絶縁し、計測制御系に生じた故障が安全保護系に影響を与えないようにしている。 (4) 安全保護系のプロセス計装は、電源の喪失又は系の遮断に対して原子炉の保護動作をとる方向に作動するように設計している。 (5) 安全保護系のプロセス計装は、原子炉運転中にも検出器の出力信号回路に模擬入力を印加し、規定の設定値において必要な動作がおこなわれることを確認できる。 また、検出器は、多重化されたチャンネル間の信号を相互比較することにより、原子炉運転中にも健全性が確認できる。 (6) 安全保護系のプロセス計装及び安全保護系以外の主要なプロセス計装の電源は、無停電電源装置から給電される。 したがって、短時間の全動力電源喪失に対しても機能を喪失することはない。 また、非常用所内電源系のみ運転下あるいは外部電源のみ運転下で単一故障を仮定しても安全保護機能を失うことはない。 (7) 通常運転時及び運転時の異常な過渡変化時において、加圧器水位、1次冷却材の圧力、温度及び流量、原子炉格納容器圧力等は、予想</p>	<p>既許可記載の相違</p> <p>記載表現の相違(光変換カード)</p> <p>・泊は、p24-18、6.3.3(1)の記載との整合の観点から記載。</p> <p>・大飯も、p24-18、6.3.4.1には、光変換カードの記載あり。</p>

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

第24条 安全保護回路

大阪発電所3/4号炉（リファレンスプラント）	女川原子力発電所2号炉	泊発電所3号炉	相違理由
<p>変動範囲内での監視が可能である。</p> <p>また、事故時において、事故の状態を知り対策を講じるに必要なパラメータである原子炉格納容器圧力、温度等は、中央制御盤で監視できる。</p> <p>特に、原子炉の停止状態は原子炉トリップ遮断器の開表示と1次冷却材のサンプリングによるほう素濃度の測定により、また、炉心の冷却状態は加圧器水位及び1次冷却材のサブクール度、圧力、温度等により監視あるいは推定できる。</p> <p>(8) プロセス計装の主要なパラメータは、中央制御盤で監視できる。</p> <p>【まとめ資料作成範囲外のため。設置許可(令和3年5月)より引用】↑</p> <p>6.6 原子炉保護設備</p> <p>6.6.1 概要</p> <p>原子炉保護設備は、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により、運転中の異常な過渡変化時あるいは、事故時に際し工学的安全施設の作動とあいまって燃料の許容設計限界、原子炉冷却材圧力バウンダリ及び原子炉格納容器バウンダリを保護するため原子炉停止システムを作動させ、原子炉を自動停止させる。</p> <p>原子炉保護設備は、原子炉プラントの種々のパラメータを監視する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、原子炉トリップ信号及びインターロック回路動作信号を発生する4重トレンの論理回路と原子炉トリップ信号により自動的に開く原子炉トリップ遮断器とで構成する。</p> <p>6.6.2 設計方針</p> <p>原子炉保護設備は、以下の方針で設計する。</p> <p>(3) 原子炉保護設備は、単一故障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、安全保護機能を喪失しないよう多重性を確保する設計とする。</p> <p>(4) 原子炉保護設備は、チャンネル相互を分離し、それぞれのチャンネル間において独立性を確保する設計とする。</p> <p>(1) 原子炉保護設備は、運転時の異常な過渡変化が生じた場合において、その異常な状態を検知し、原子炉停止システムを含む適切な設備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ることがない設計とする。</p>	<p>6.6 安全保護系</p> <p>6.6.1 概要</p> <p>安全保護系は、発電用原子炉の安全性を損なうおそれのある異常な過渡状態や誤動作が生じた場合、あるいはこのような事態の発生が予想される場合に、それを防止あるいは、抑制するために安全保護動作を起こすなどにより発電用原子炉を保護するために設ける。この系は、原子炉保護系を作動させるための原子炉保護系作動回路及び非常用炉心冷却系等の工学的安全施設を作動させるための工学的安全施設作動回路からなる。</p> <p>6.6.2 設計方針</p> <p>安全保護系の設計方針は次のとおりである。</p> <p>(4) 安全保護系は、多重性及び電気的・物理的な独立性を有する設計とし実際に起こると考えられるいかなる単一機器の故障又は単一機器の使用状態からの取外しによっても、その安全保護機能が妨げられないようにする。</p> <p>(1) 安全保護系は、運転時の異常な過渡変化時に、その異常状態を検知し、原子炉保護系を自動的に作動させ、燃料要素の許容損傷限界を超えないようにする。</p> <p>(2) 安全保護系は、偶発的な制御棒引抜きのような原子炉停止系のいかなる単一の誤動作に対しても、燃料要素の許容損傷限界を超えないよ</p>	<p>変動範囲内での監視が可能である。</p> <p>また、事故時において、事故の状態を知り対策を講じるに必要なパラメータである原子炉格納容器圧力、温度等は、中央制御盤で監視できる。</p> <p>特に、原子炉の停止状態は原子炉トリップ遮断器の開表示と1次冷却材のサンプリングによるほう素濃度の測定により、また、炉心の冷却状態は加圧器水位及び1次冷却材のサブクール度、圧力、温度等により監視あるいは推定できる。</p> <p>(8) プロセス計装の主要なパラメータは、中央制御盤で監視できる。</p> <p>6.6 原子炉保護設備</p> <p>6.6.1 概要</p> <p>原子炉保護設備は、原子炉の安全性を損なうおそれのある運転時の異常な過渡変化あるいは設計基準事故が発生した場合、又は発生が予想される場合に、それを抑制あるいは防止するため、異常を検知し原子炉を自動的にトリップさせる。</p> <p>原子炉保護設備は、原子炉プラントの種々のパラメータを監視する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、原子炉トリップ信号及びインターロック回路動作信号を発生する4チャンネルの論理回路と原子炉トリップ信号により自動的に開く原子炉トリップ遮断器とで構成する。</p> <p>6.6.2 設計方針</p> <p>(1) 多重性</p> <p>原子炉保護設備は、そのシステム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り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。</p> <p>(2) 独立性</p> <p>原子炉保護設備は、通常運転時、保守時、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、そのシステム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において独立性を確保する設計とする。</p> <p>(3) 過渡時の機能</p> <p>a. 原子炉保護設備は、運転時の異常な過渡変化時に、その異常な状態を検知し、原子炉停止系を含む適切なシステムを自動的に作動させ、燃料要素の許容損傷限界を超えない設計とする。</p> <p>b. 原子炉保護設備は、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</p>	<p>相違理由</p> <p>既許可記載の相違</p> <p>記載の充実(追加要求事項の対象外、大飯参照)</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p>

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

第24条 安全保護回路

大飯発電所3/4号炉（リファレンスプラント）	女川原子力発電所2号炉	泊発電所3号炉	相違理由
<p>(2) 原子炉保護設備は、設計基準事故時にその異常な状態を検知し、原子炉停止システムを自動的に作動させ、また、必要な場合には手動でも作動できる設計とする。</p> <p>(5) 原子炉保護設備は、駆動源の喪失、系統の遮断その他考慮すべき不利な状況に対して最終的に安全な状態に落ち着くような設計とする。</p> <p>(8) 原子炉保護設備は、原子炉の運転中に定期的に試験を行い、機能が喪失していないことを確認できる設計とする。</p> <p>(9) 原子炉保護設備は、作動状況が確認できる設計とする。</p> <p>(2) 原子炉保護設備は、設計基準事故時にその異常な状態を検知し、原子炉停止システムを自動的に作動させ、また、必要な場合には手動でも作動できる設計とする。</p> <p>(6) 原子炉保護設備のデジタル計算機は、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。 【説明資料（2.1、2.2、2.4）】</p> <p>(7) 原子炉保護設備は、2基以上の原子炉施設間で共用又は相互に接続しない設計とする。</p> <p>6.6.4 主要設備</p>	<p>うにする。</p> <p>(3) 安全保護系は、設計基準事故時にあっては、直ちにこれを検知し、原子炉保護系及び工学的安全施設の作動を自動的に開始させる。</p> <p>(5) 安全保護系は、系の遮断、駆動源の喪失においても、安全上許容される状態（フェイル・セーフ又はフェイル・アズ・イズ）になるようにする。</p> <p>(6) 安全保護系は、一般計測制御系とは極力分離し、部分的に共用した場合でも一般計測制御系の故障が安全保護系に影響を与えないようにする。</p> <p>(7) 安全保護系は、通常運転中においても、定期的に機能試験を行うことができるようにする。</p> <p>(8) 安全保護系は、監視装置、警報等によりその作動状況が確認できる設計とする。</p> <p>(9) 安全保護系は、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ことができる設計とする。 【説明資料（2.1：P24条-27,28）（2.2：P24条28-31）（2.3：P24条-32）（2.4：P24条-33）（2.5：P24条-34,35）（2.6：P24条-36）（2.7：P24条-37,38）】</p> <p>6.6.4 主要設備</p>	<p>投入が生じた場合でも、燃料要素の許容損傷限界を超えない設計とする。</p> <p>(4) 設計基準事故時の機能 原子炉保護設備は、設計基準事故時に、その異常な状態を検知し、原子炉をトリップさせる設計とする。</p> <p>(5) 故障時の機能 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、最終的に発電用原子炉施設が安全な状態に落ち着く設計とする。</p> <p>(6) 計測制御系との分離 原子炉保護設備は、計測制御系とは機能的に分離した設計とする。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、安全保護系へ影響を与えない設計とする。</p> <p>(7) 試験可能性 原子炉保護設備は、原子炉の運転中に定期的に試験及び検査ができるとともに、その健全性及び多重性の維持を確認するため、独立に各チャンネルの試験及び検査ができる設計とする。</p> <p>(8) 電源喪失に対する考慮 原子炉保護設備の電源は、無停電の計装用交流母線から給電し、一定時間の全交流動力電源喪失時にも機能を喪失しない設計とする。</p> <p>(9) 作動状況の確認 原子炉保護設備は、監視機能を設け作動状況が確認できる設計とする。</p> <p>(10) 手動操作 原子炉保護設備は、自動的に作動し、また、必要な場合には手動でも作動させることができる設計とする。</p> <p>(11) 不正アクセス防止 原子炉保護設備のデジタル計算機は、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。 【説明資料（2.1：P24条-30,31）（2.2：P24条31）（2.3：P24条-31,32）（2.4：P24条-33）（2.5：P24条-33）（2.6：P24条-34-36）（2.7：P24条-37）（2.9：P24条-40）】</p> <p>(12) 共用禁止 原子炉保護設備は、2基以上の発電用原子炉施設間で共用又は相互に接続しない設計とする。</p> <p>6.6.3 主要設備</p>	<p>相違理由</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>既許可構成の相違</p> <p>記載表現の相違(女川実績の反映)</p> <p>既許可構成の相違</p> <p>記載の充実(追加要求事項の対象外、大飯参照)</p>

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

第24条 安全保護回路

大飯発電所3/4号炉（リファレンスプラント）	女川原子力発電所2号炉	泊発電所3号炉	相違理由
<p>6.6.4.1 原子炉トリップ遮断器</p> <p>原子炉トリップ遮断器は、第 6.6.1 図に示すように原子炉保護系ロジック・トレインに合わせて 4 重トレイン構成とし、各トレインにそれぞれ 2 台ずつ設けられた計 8 台の遮断器の相互接続により、各ロジック・トレインからの信号に対し“2 out of 4”のロジックを形成している。</p> <p>“2 out of 4”ロジックを形成する原子炉トリップ遮断器は、制御棒駆動装置用電源を制御棒駆動装置に接続する。</p> <p>各ロジック・トレインからのトリップ信号は、対応するトレインに属する 2 台の原子炉トリップ遮断器を同時に開くことができる。</p> <p>原子炉トリップは 4 重トレインのうち、2 トレイン以上の原子炉トリップ遮断器を開くことによって達成される。2 トレイン以上の原子炉トリップ遮断器が開くと制御棒駆動装置への電源が遮断され、制御棒クラスタは自重で炉心に落下する。</p> <p>各原子炉トリップ遮断器の不足電圧コイルは、プラント出力運転中励磁されており、スプリングに抗してトリップブランジャを保持している。原子炉計装あるいは安全保護系のプロセス計装によって監視している変数が設定値に達し、所要の演算処理装置等が動作すると原子炉トリップ遮断器の不足電圧コイルへの直流回路を開く。不足電圧コイルの直流電源が喪失すると、トリップブランジャを解放し、遮断器を開く。制御棒クラスタは、運転員が原子炉トリップ遮断器をリセットするまでは引抜きはできない。また、原子炉トリップ遮断器は、トリップ信号が復帰しないとリセットはできない。</p> <p>また、トリップ遮断器は、“2 out of 4”ロジックを構成しているため、運転中における単独トレインごとのトリップ遮断器の実動作（開放）テストが可能である。</p> <p>原子炉トリップ遮断器は、原子炉補助建屋内の制御棒駆動装置電源室に設置し、必要な場合には、現場手動遮断が可能である。</p> <p>【まとめ資料作成範囲外のため、設置許可(令和3年5月)より引用】↓</p> <p>6.6.4.2 原子炉トリップ信号</p> <p>原子炉トリップ信号としては、次のものがあり、これらをまとめて第 6.6.1 表及び第 6.6.2 図に示す。また、原子炉の保護機能を損なうことなく出力条件によって原子炉トリップ信号のブロック等を行い、運転の継続が可能ないようにパーミッシブ回路を設ける。第 6.6.2 表にパーミッシブ信号一覧表を示す。</p> <p>(1) 中性子源領域中性子東高</p> <p>原子炉停止及び起動時の保護のため、中性子源領域中性子東高の“1 out of 2”信号で原子炉をトリップさせる。このトリップは、中間領域中性子束がパーミッシブ信号-6（P-6、以下同様に記す）の設定値を超えた場合には、手動でブロックできる。</p> <p>更に、出力領域中性子束が P-10 の設定値を超えると自動ブロックされる。</p>	<p>6.6.4.1 原子炉保護系</p> <p>原子炉保護系は、第 6.6-1 図、第 6.6-2 図及び 6.6-3 図に示すように、2 チャンネルで構成する。各チャンネルには、一つの測定変数に対して、少なくとも二つ以上の独立したトリップ接点があり、いずれかの接点の動作でそのチャンネルがトリップし、両チャンネルの同時のトリップの場合に、発電用原子炉がスクラムする。</p> <p>スクラム弁への計器用空気の制御には、2 個のソレノイド作動のスクラムパイロット弁（以下、6. では「パイロット弁」という。）を使用する。このパイロット弁は、三方向形で、各制御棒駆動機構のスクラム弁に対して、二つのソレノイドのうち一つ、あるいは両方が励磁状態にある場合は、スクラム弁のダイヤフラムに空気圧がかかって、弁を閉鎖状態に保つようにしている。パイロット弁の両ソレノイドが無励磁になれば、スクラム弁のダイヤフラムの空気圧がなくなってスクラム弁は開き、制御棒を挿入することになる。各駆動機構のパイロット弁に二つずつあるソレノイドは、原子炉保護系のそれぞれのチャンネルが同時にトリップすれば、無励磁となり発電用原子炉はスクラムするが、単一チャンネルのみのトリップでは一つのソレノイドしか無励磁とならずスクラムしない。</p> <p>(1) 原子炉スクラム条件</p> <p>発電用原子炉は、下記の条件の場合にスクラムする。</p> <ol style="list-style-type: none"> 原子炉圧力高 原子炉水位低 ドライウェル圧力高 中性子東高（平均出力領域モニタ） 中間領域における原子炉周期短（起動領域モニタ） 中性子束計装動作不能（起動及び平均出力領域モニタ） スクラム排出容器水位高 主蒸気隔離弁開 主蒸気止め弁開 蒸気加減弁急速開 主蒸気管放射能高 地震加速度大 手動 モードスイッチ「停止」 <p>下記の場合にも発電用原子炉はスクラムする。</p> <ol style="list-style-type: none"> 原子炉保護系電源喪失 <p>原子炉保護系の電源喪失時には、後述のフェイル・セイフの機能により、スクラムとなる。</p> <ol style="list-style-type: none"> 電気油圧式制御装置（EHC）油圧低 <p>タービン制御油圧が低下したときは、主蒸気止め弁及び蒸気加減弁が急開し、原子炉スクラムとなる。</p> <p>検出器の種類、検出場所及びスクラム設定値は、第 6.6-1 表に示すとおりである。第 6.6-4 図は原子炉保護系の機能説明図である。</p> <p>原子炉保護系は、二重チャンネル、継電器方式の構成で、論理回路及びパイロット弁のソレノイドを制御する主トリップ継電器には、特に高信頼度の継電器を用いる。</p>	<p>(1) 構成</p> <p>原子炉保護設備は第 6.6.1 図に示すように、原子炉トリップ演算処理装置、トリップチャンネル、原子炉トリップ遮断器等で構成し、“2 out of 4”方式とする。また、原子炉トリップ演算処理装置及びトリップチャンネルは、多重化された四つのチャンネルで構成し、各チャンネルには自己診断機能を有するマイクロプロセッサを用いる。</p> <p>原子炉トリップ演算処理装置は、安全保護回路のプロセス計装あるいは炉外核計装からの信号を入力し、原子炉トリップ演算を行い、信号が設定値に達した場合には、チャンネルトリップ信号を発信する。</p> <p>トリップチャンネルは、各々四つの原子炉トリップ演算処理装置からの信号を入力し、二つ以上の原子炉トリップ演算処理装置がチャンネルトリップ信号を発信した場合には、原子炉トリップ信号を発信する。</p> <p>原子炉トリップ遮断器は、トリップチャンネルごとにそれぞれ 2 台ずつ設けられ相互に接続された計 8 台構成とする。各原子炉トリップ遮断器の不足電圧コイルは、原子炉運転中常に対応するトリップチャンネルから直流電源が供給され励磁しているため、原子炉トリップ遮断器は投入状態となっている。各トリップチャンネルからの原子炉トリップ信号は、原子炉トリップ遮断器を投入している不足電圧コイルへの直流電源を遮断し、対応する原子炉トリップ遮断器 2 台を同時に開放する。すなわち、二つ以上のトリップチャンネルが原子炉トリップ信号を発信することにより各原子炉トリップ遮断器が開放し、制御棒制御装置への電源が遮断され、制御棒クラスタが重力で炉心に落下し、原子炉がトリップする。</p> <p>原子炉保護設備の原子炉トリップ演算処理装置、トリップチャンネル及び原子炉トリップ遮断器の駆動源には、電力を使用する。これらは、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・セイフとなり、最終的に発電用原子炉施設が安全な状態に落ち着く。</p> <p>また、原子炉トリップ演算処理装置及びトリップチャンネルは、マイクロプロセッサの故障に対してトリップ信号を発信する。</p> <p>なお、原子炉保護設備は、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が保証されたソフトウェアを使用する。</p> <p>(2) 原子炉トリップ信号</p> <p>原子炉トリップ信号は以下のものがあり、第 7.4.1 表及び第 7.4.2 図に示す。また、第 7.4.2 表にパーミッシブ信号一覧表を示す。パーミッシブ信号は、原子炉停止時及び起動時において安全保護動作に適切なインターロックをかけるための信号である。</p> <ol style="list-style-type: none"> 中性子源領域中性子東高 <p>原子炉停止時及び起動時の異常な原子炉出力上昇に対する原子炉保護のため、中性子源領域中性子東高の“1 out of 2”信号で原子炉をトリップさせる。このトリップは、中間領域中性子束が P-6 の設定値以上では手動でブロックできる。</p> <p>さらに、出力領域中性子束が P-10 の設定値以上では自動的にブロックされる。</p>	<p>既許可記載の相違</p> <p>【女川】</p> <p>既許可構成の相違</p> <ul style="list-style-type: none"> 炉型の相違による安全保護系の設備構成の相違に伴い、泊と女川では既許可構成が大幅に異なる。 <p>既許可記載の相違</p> <p>既許可記載の相違</p>

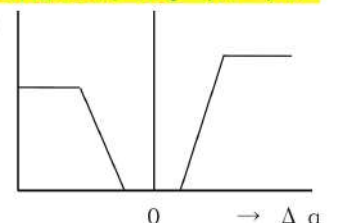
赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

第24条 安全保護回路

大飯発電所3/4号炉（リファレンスプラント）	女川原子力発電所2号炉	泊発電所3号炉	相違理由
<p>(2) 中間領域中性子束高 原子炉停止及び起動時の保護のため、中間領域中性子束高の“1 out of 2”信号で原子炉をトリップさせる。このトリップは、出力領域中性子束がP-10の設定値を超えた場合には、手動でブロックできる。</p> <p>(3) 出力領域中性子束高 出力領域中性子束高には、高設定と低設定があり、通常の出力運転状態では、定格出力値以上に設定した高設定値により、起動時等の低出力運転状態では、定格出力値以下の低設定値により、両者とも出力領域中性子束高の“2 out of 4”信号で、原子炉をトリップさせる。 低設定トリップは、出力領域中性子束がP-10の設定値を超えた場合には、手動でブロックできる。</p> <p>(4) 出力領域中性子束変化率高 制御棒クラスタの飛び出し時の原子炉保護のため、出力領域中性子束増加率高の“2 out of 4”信号によって原子炉をトリップさせる。また、制御棒クラスタ落下時の原子炉保護のため、出力領域中性子束減少率高の“2 out of 4”信号によって原子炉をトリップさせる。</p> <p>(5) 非常用炉心冷却設備作動 非常用炉心冷却設備作動信号が発生した場合には、原子炉をトリップさせる。</p> <p>(6) 過大温度ΔT高 過大温度ΔT高原子炉トリップは、炉心をDNBから保護する。 過大温度ΔT高の設定値は以下のとおりで“2 out of 4”信号で原子炉をトリップさせる。</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> $\text{過大温度}\Delta T\text{設定} = K_1 - K_2 \frac{1 + \tau_1 s}{1 + \tau_2 s} (T - T_0) + K_3 (P - P_0) - f (\Delta q)$ </div> <p>s：ラプラス演算子 T：1次冷却材平均温度 T0：定格出力時の1次冷却材平均温度 P：加圧器圧力 P0：定格運転圧力 K1～K3、τ1、τ2：定数</p>	<p>(2) フェイル・セーフ チャンネル・トリップ、あるいは原子炉スクラムに関連する継電器は、運転中すべて励磁状態にあり、一つ以上の継電器が無励磁状態となると、その継電器が属しているチャンネルはトリップとなる。 したがって、電源の喪失及びコイルの断線、短絡、あるいは配線の断線等の継電器の故障の大部分は、継電器自体が無励磁状態に戻し、チャンネル・トリップになるように働くので、このような回路構成は、大部分の故障条件に対して“フェイル・セーフ”となる。 一方、接点の焼損による溶着など“フェイル・セーフ”に反する方向の故障に対しては、各接点を流れる電流を、定格の50%以下になるように設計することにより、その発生を防止する。 第6.6-1図に示すように、論理回路の継電器接点はすべて直列に接続するので、どの継電器でも1個が無励磁の状態になれば、その継電器接点が属している論理回路の主トリップ継電器の電源は喪失することになる。主トリップ継電器の接点は、各ソレノイド・グループ回路ごとに二つずつ直列につないで、一つの継電器接点が単独で故障して聞かない場合でも、スクラム動作を妨げないようにしている。</p> <p>(3) リセット いずれか一方のチャンネルがトリップした場合で、そのチャンネル・トリップの原因が解除されている場合には、手動でトリップしたチャンネルをリセットすることによりパイロット弁を再び励磁することができる。</p> <p>6.6.4.2 後備原子炉保護系 パイロット弁の一つが、故障によって動作しないという事態が生じた場合に、制御棒が確実に挿入されるように、計装用空気系統に、2個の三方向形のソレノイド作動の後備パイロット弁を設ける。 このソレノイドは直流電源に接続されており、通常は無励磁状態にある。 原子炉保護系の2チャンネルの主トリップ継電器が無励磁状態になった場合に、2個の後備パイロット弁のソレノイドが励磁される。パイロット弁が故障で動作しない場合にも、後備パイロット弁の動作によって、スクラム弁への空気圧がなくなり制御棒を挿入する。この場合の制御棒の挿入時間は、通常の挿入時間より長い、発電用原子炉を停止させる場合、他の制御棒が挿入できれば、後備原子炉保護系がなくても十分発電用原子炉を緊急停止できる。 第6.6-2図に、後備原子炉保護系を含めた原子炉保護系及び制御棒駆動系概略図を示す。</p> <p>6.6.4.3 工学的安全施設作動回路 原子炉保護系のほか、次のような工学的安全施設作動回路を有する。 (1) 工学的安全施設作動回路 工学的安全施設作動回路の主要な機能には、次のようなものがある。 a. 原子炉水位低、主蒸気管放射能高、主蒸気管圧力低、主蒸気管流</p>	<p>b. 中間領域中性子束高 原子炉停止時及び起動時の異常な原子炉出力上昇に対する原子炉保護のため、中間領域中性子束高の“1 out of 2”信号で原子炉をトリップさせる。このトリップは、出力領域中性子束がP-10の設定値以上では手動でブロックできる。</p> <p>c. 出力領域中性子束高 通常の出力運転時の過大出力に対する原子炉保護のため、出力領域中性子束高（高設定）の“2 out of 4”信号で原子炉をトリップさせる。 また、起動時等の低出力運転時の異常な原子炉出力上昇に対する原子炉保護のため、出力領域中性子束高（低設定）の“2 out of 4”信号で原子炉をトリップさせる。このトリップは、出力領域中性子束がP-10の設定値以上では手動でブロックできる。</p> <p>d. 出力領域中性子束変化率高 制御棒クラスタの飛び出し時の原子炉保護のため、出力領域中性子束増加率高の“2 out of 4”信号によって原子炉をトリップさせる。 また、制御棒クラスタの落下時の原子炉保護のため、出力領域中性子束減少率高の“2 out of 4”信号によって原子炉をトリップさせる。</p> <p>e. 非常用炉心冷却設備作動 非常用炉心冷却設備作動信号が発信する場合には、原子炉をトリップさせる。</p> <p>f. 過大温度ΔT高 過大温度ΔT高原子炉トリップには、過大温度ΔT高（DNB防止）と過大温度ΔT高（高温側配管沸騰防止）があり、前者は炉心をDNBから保護し、後者は高温側配管での1次冷却材の沸騰を防止する。 過大温度ΔT高（DNB防止）及び過大温度ΔT高（高温側配管沸騰防止）の設定値は以下のとおりで“2 out of 4”信号で原子炉をトリップさせる。</p> <p>過大温度ΔT高（DNB防止）設定 $= K_1 - K_2 \frac{1 + \tau_1 s}{1 + \tau_2 s} (T - T_0) + K_3 (P - P_0) - f (\Delta q)$</p> <p>過大温度ΔT高（高温側配管沸騰防止）設定 $= K_4 - K_5 \frac{1 + \tau_3 s}{1 + \tau_4 s} (T - T_0) + K_6 (P - P_0)$</p> <p>ここで、s：ラプラス演算子 T：1次冷却材平均温度 T0：定格出力運転時の1次冷却材平均温度 P：加圧器圧力 P0：原子炉運転圧力 K1～K6、τ1～τ4：定数</p>	<p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p>

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

第24条 安全保護回路

大阪発電所3/4号炉 (リファレンスプラント)	女川原子力発電所2号炉	泊発電所3号炉	相違理由
<p>f (Δq)：炉外中性子束検出器（出力領域用）の上半分（φt）と下半分（φb）の指示値の差の関数で、概略を下図に示す（Δq=φt-φb）</p>  <p>過大温度ΔT高による保護限界の代表例を第6.6.3図に示す。</p> <p>(7) 過大出力ΔT高 過大出力ΔT高原子炉トリップは、炉心の過大出力を防止する。 過大出力ΔT高の設定値は以下のとおりで“2 out of 4”信号で原子炉をトリップさせる。</p> $\text{過大出力}\Delta T\text{設定} = K_4 - \left[K_5 \frac{\tau_3 s}{1 + \tau_3 s} + T \right] - [K_6 (T - T_0)] - f(\Delta q)$ <p>ただし、[]で示した項は負の値にならないように零でリミットする。 s：ラプラス演算子 T：1次冷却材平均温度 T0：定格出力時の1次冷却材平均温度 K4~K6、τ3：定数 f(Δq)：過大温度ΔT高と同じ 過大出力ΔT高による保護限界の代表例を第6.6.3図に示す。</p> <p>(8) 原子炉圧力高 1次冷却系の過圧防護のために、加圧器圧力高の“2 out of 4”信号で原子炉をトリップさせる。</p> <p>(9) 原子炉圧力低 原子炉圧力が異常に低下した場合に、炉心を保護するため、加圧器圧力低の“2 out of 4”信号で原子炉をトリップさせる。 このトリップは、出力領域中性子束及びタービン負荷がP-7の設定値以下では自動ブロックされる。</p> <p>(10) 1次冷却材流量低 1次冷却材流量が低下した場合に、炉心をDNBから保護するため、各ループごとの1次冷却材流量低の“2 out of 4”信号で原子炉をトリップさせる。ただし、出力領域中性子束あるいはタービン負荷がP-7の設定値以上では、2ループ以上からの流量低信号の一致で、また、出力領域中性子束がP-8の設定値以上では、いずれかのループからの</p>	<p>最大、主蒸気管トンネル温度高、主復水器真空度低のいずれかの信号による主蒸気隔離弁の閉鎖</p> <p>b. ドライウェル圧力高、原子炉水位低、原子炉建屋原子炉棟放射能高のいずれかの信号による常用換気系の閉鎖と非常用ガス処理系の起動</p> <p>c. 原子炉水位低又はドライウェル圧力高の信号による高圧炉心スプレイ系、低圧炉心スプレイ系及び低圧注水系の起動</p> <p>d. 原子炉水位低及びドライウェル圧力高の同時信号による自動減圧系の作動</p> <p>e. 原子炉水位低又はドライウェル圧力高の信号による高圧炉心スプレイ系ディーゼル発電機及び非常用ディーゼル発電機の起動</p> <p>f. 原子炉水位低又はドライウェル圧力高の信号による主蒸気隔離弁以外の隔離弁の閉鎖</p> <p>第6.6-5図及び第6.6-6図は工学的安全施設作動回路の説明図である。第6.6-2表に工学的安全施設作動回路の信号一覧表を示す。</p> <p>6.6.4.4 バイパス モードスイッチによって安全保護系の回路を以下のようにバイパスする。</p> <p>(1) 「停止」 このモードでは、スクラム信号が出され、全制御棒を炉心に挿入する。このモードにしてから約10秒後にスクラム信号のリセットが可能になる。 また、主蒸気隔離弁閉によるスクラム信号は、原子炉圧力が約42kg/cm²以下のときには自動的にバイパスされ、スクラム排出容器水位高によるスクラム信号も手動で、バイパス可能である。</p> <p>(2) 「燃料取替」 このモードでは、原子炉保護系はスクラム動作可能な状態にあるが、主蒸気隔離弁閉によるスクラム信号は、原子炉圧力が約42kg/cm²以下のときには自動的にバイパスされる。なお、スクラム排出容器水位高によるスクラム信号も手動で、バイパス可能であるが、この場合には制御棒を引抜くことはできない。</p> <p>(3) 「起動」 このモードは、発電用原子炉を起動し、定格の約5%まで出力を上昇させる場合に適用する。また、主蒸気隔離弁が閉で、原子炉を臨界に保つときにも適用する。 このモードでは、主蒸気隔離弁閉によるスクラム信号は、原子炉圧力が約42kg/cm²以下のときには自動的にバイパスされる。</p> <p>(4) 「運転」 このモードでは、バイパスはすべて解除され、運転手順の上で特に許される場合のみ保守上の目的で、個々の計器をバイパスすることができる。</p>	<p>f (Δq)：炉外中性子束検出器（出力領域用）信号の上半分（φt）と下半分（φb）の差の関数で、概略を下図に示す。（Δq=φt-φb）</p>  <p>過大温度ΔT高（DNB防止）及び過大温度ΔT高（高温側配管沸騰防止）による保護限界の代表例を第6.6.3図に示す。</p> <p>g. 過大出力ΔT高 過大出力ΔT高原子炉トリップは、炉心の過大出力を防止する。 過大出力ΔT高の設定値は以下のとおりで“2 out of 4”信号で原子炉をトリップさせる。</p> $\text{過大出力}\Delta T\text{高設定} = K_7 - \left[K_8 \frac{\tau_{5s}}{1 + \tau_{5s}} + T \right] - [K_9 (T - T_0)] - f(\Delta q)$ <p>ただし、[]で示した項は負の値にならないように零でリミットする。 ここで、s：ラプラス演算子 T：1次冷却材平均温度 T0：定格出力運転時の1次冷却材平均温度 K7~K9、τ5：定数 f(Δq)：過大温度ΔT高と同じ 過大出力ΔT高による保護限界の代表例を第6.6.3図に示す。</p> <p>h. 原子炉圧力高 1次冷却設備の過圧防止のために、加圧器圧力高の“2 out of 4”信号で原子炉をトリップさせる。</p> <p>i. 原子炉圧力低 原子炉圧力が異常に低下した場合に、炉心での過度な沸騰を防止するため、加圧器圧力低の“2 out of 4”信号で原子炉をトリップさせる。このトリップは、出力領域中性子束及びタービン負荷がP-7の設定値以下では自動的にブロックされる。</p> <p>j. 1次冷却材流量低 1次冷却材流量が低下した場合に、炉心をDNBから保護するため、各ループの1次冷却材流量低の“2 out of 4”信号で原子炉をトリップさせる。このトリップは、出力領域中性子束及びタービン負荷がP-7の設定値以下では2ループ以上の1次冷却材流量低による原子炉トリップが自動的にブロックされる。また、出力領域中性子</p>	<p>相違理由</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p>

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

第24条 安全保護回路

大飯発電所3/4号炉（リファレンスプラント）	女川原子力発電所2号炉	泊発電所3号炉	相違理由
<p>流量低信号で原子炉をトリップさせる。</p> <p>(11) 1次冷却材ポンプ回転数低 1次冷却材ポンプの回転数が低下した場合の1次冷却材流量の低下に対して、炉心を保護するため、各1次冷却材ポンプ回転数低の“2 out of 4”信号で原子炉をトリップさせる。このトリップは、出力領域中性子束及びタービン負荷がP-7の設定値以下では自動ブロックされる。</p> <p>(12) タービントリップ タービンがトリップした場合は、1次冷却材の温度及び圧力の過度の上昇を避けるため、タービン非常遮断油圧低の“2 out of 4”信号又は4個の主蒸気止め弁全閉信号で原子炉をトリップさせる。このトリップは、出力領域中性子束及びタービン負荷がP-7の設定値以下では自動ブロックされる。</p> <p>(13) 蒸気発生器水位低 蒸気発生器の水位が過度に低下した場合には、蒸気発生器水位低の“2 out of 4”信号で、原子炉をトリップさせる。</p> <p>(14) 加圧器水位高 原子炉圧力高原子炉トリップの後備として、加圧器水位高の“2out of 4”信号で原子炉をトリップさせる。このトリップは、出力領域中性子束及びタービン負荷がP-7の設定値以下では自動ブロックされる。</p> <p>(15) 地震加速度高 水平方向加速度高の“2 out of 3”信号又は垂直方向加速度高の“2 out of 3”信号で原子炉をトリップさせる。</p> <p>(16) 手動 中央制御盤の原子炉トリップスイッチ2個のうちいずれか1個を操作すれば、原子炉はトリップする。</p> <p>6.6.4.3 原子炉トリップ時のインターロック 原子炉がトリップした場合は、タービンをトリップさせ、さらに発電</p>	<p>6.6.4.5 ケーブル、電線路及び計装配管 安全保護系を構成するチャンネルは、相互干渉が起らないように、各チャンネルごとに専用のケーブルトレイ、電線路、計装配管、計装ラック等を設けるとともに、各チャンネル相互を可能な限り物理的、電気的に分離し、独立性を持たせるように設計する。 安全保護系と計測制御系の電源、検出器、ケーブルトレイ、電線路及び計装配管（原子炉格納容器貫通計装配管を含む。）は、原則として分離するように設計する。 安全保護系のうち、計測制御系と共用する原子炉水位及び原子炉圧力を検出する計装配管ヘッダの一部並びに指示・記録計用検出部と共用する原子炉核計装の検出部は、計測制御系の電気的故障（短絡、地絡、断線等）及び機械的故障によって安全保護系に影響を与えないように設計する。</p>	<p>東がP-8の設定値以下では1ループのみの1次冷却材流量低による原子炉トリップが自動的にブロックされる。</p> <p>k. 1次冷却材ポンプ電源電圧低 1次冷却材ポンプの電源電圧が低下した場合の1次冷却材流量の低下に対して、炉心をDNBから保護するため、2台以上の1次冷却材ポンプ電源電圧低の“2 out of 4”信号で原子炉をトリップさせる。このトリップは、出力領域中性子束及びタービン負荷がP-7の設定値以下では自動的にブロックされる。</p> <p>l. 1次冷却材ポンプ電源周波数低 1次冷却材ポンプの電源周波数が低下した場合の1次冷却材流量の低下に対して、炉心をDNBから保護するため、2台以上の1次冷却材ポンプ電源周波数低の“2 out of 4”信号で原子炉をトリップさせる。このトリップは、出力領域中性子束及びタービン負荷がP-7の設定値以下では自動的にブロックされる。</p> <p>m. タービントリップ タービントリップ時の1次冷却材の温度及び圧力の過度の上昇を避けるため、タービン非常遮断油圧低の“2 out of 4”信号又は主蒸気止め弁4個の閉で原子炉をトリップさせる。このトリップは、出力領域中性子束及びタービン負荷がP-7の設定値以下では自動的にブロックされる。</p> <p>n. 蒸気発生器水位低 蒸気発生器の水位が異常に低下した場合には、1次冷却設備から2次冷却設備への除熱能力の喪失に対する保護のため、各蒸気発生器の水位低の“2 out of 4”信号で原子炉をトリップさせる。</p> <p>o. 加圧器水位高 加圧器の滴水を防止するため、あるいは原子炉圧力高原子炉トリップの後備として、加圧器水位高の“2out of 4”信号で原子炉をトリップさせる。このトリップは、出力領域中性子束及びタービン負荷がP-7の設定値以下では自動的にブロックされる。</p> <p>p. 地震加速度大 地震に対する保護のため、水平方向加速度大の“2 out of 4”信号又は鉛直方向加速度大の“2 out of 4”信号で原子炉をトリップさせる。</p> <p>q. 手動 中央制御盤の原子炉トリップスイッチ2個のうちいずれか1個を操作すれば、原子炉はトリップする。</p> <p>(3) 原子炉トリップ時のインターロック 原子炉がトリップした場合には、蒸気タービン及び発電機をトリップ</p>	<p>相違理由</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p>

第24条 安全保護回路

大阪発電所3/4号炉（リファレンスプラント）	女川原子力発電所2号炉	泊発電所3号炉	相違理由
<p>機をトリップさせる。発電機のトリップは、1次冷却材流量確保のため一定時間後とする。また、1次冷却系の過冷却を防止するため、原子炉トリップと、1次冷却材平均温度低の“2 out of 4”信号が一致した場合は、主給水制御弁を全閉させる。</p> <p>6.6.4.4 監視装置 原子炉保護設備の作動状況の確認をするため、次のような監視装置を設ける。 また、原子炉トリップの確認は炉外核計装等で行う。</p> <p>(1) 警報 原子炉保護設備で使用する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が警報設定値に達し、論理回路が動作した場合にはプラントが正常な運転状態から逸脱していることを示すため、中央制御室に警報を発する。 また、多重チャンネル構成を有する原子炉トリップ信号は、1チャンネルでも動作すれば「パーシャルトリップ」警報を発する。</p> <p>(2) 表示灯 多重チャンネル構成を有する原子炉トリップ信号は、1チャンネルでも動作すれば、中央制御盤に設けられた表示灯にトリップ状態を表示する。</p> <p>【まとめ資料作成範囲外のため。設置許可(令和3年5月)より引用】↑</p> <p>6.6.3 主要設備の仕様 原子炉保護設備の主要設備の仕様を第6.6.1表及び第6.6.1図に示す。</p> <p>【まとめ資料作成範囲外のため。設置許可(令和3年5月)より引用】↓</p> <p>6.6.6 試験検査 原子炉保護設備は、原子炉の運転中に定期的に試験を行い、機能が喪失していないことを確認できる。 【まとめ資料作成範囲外のため。設置許可(令和3年5月)より引用】↑</p>	<p>6.6.3 主要設備の仕様 原子炉保護系の主要設備の仕様を第6.6-1表及び第6.6-4図に、工学的安全施設の主要設備の仕様を第6.6-2表、第6.6-5図及び第6.6-6図に示す。</p> <p>6.6.5 試験検査 安全保護系は、原則として原子炉の運転中に定期的に試験を行い、その機能が喪失していないことを確認できる。 (1) 原子炉保護系は、原則として原子炉運転中でも次の試験が、一度に1チャンネルずつできるように設計する。 a. 手動パイロット弁作動試験：各チャンネルの手動スクラムスイッチによる論理回路及びパイロット弁の作動の確認 b. 自動パイロット弁作動試験：各論理回路ごとの鍵付テストスイッチによる論理回路及び、パイロット弁の作動の確認 c. 検出器作動試験：各チャンネルの各検出器の校正用タップから校正用模擬信号を入れることによる論理回路及びパイロット弁の作動の確認 なお、各制御棒のスクラム時間の確認のための、単一制御棒スクラム試験は、定期検査時に行うことができる。 以上のうちa.、b.及びc.の試験により、各チャンネルの独立性の確認も行うことができる。</p>	<p>させる。発電機のトリップは、1次冷却材流量確保のため一定時間後とする。 また、1次冷却設備の過冷却を防止するため、原子炉トリップと1次冷却材平均温度低の一致により、主給水制御弁及び主給水バイパス制御弁を全閉させる。</p> <p>(4) 監視機能 原子炉保護設備の作動状況の確認をするため、以下のような監視機能を設ける。 また、原子炉トリップの確認は炉外核計装等で行う。</p> <p>a. 警報 原子炉保護設備で使用する安全保護系のプロセス計装あるいは炉外核計装からの信号が警報設定値に達し、論理回路が動作した場合には、発電用原子炉施設が通常の運転状態から逸脱していることを示すため、中央制御盤に警報を発信する。 また、多重チャンネル構成を有するチャンネルトリップ信号は、1チャンネルでも動作すればパーシャルトリップ警報を発信する。</p> <p>b. 状態表示 多重チャンネル構成を有するチャンネルトリップ信号は、各チャンネルごとに中央制御盤に作動状態を表示できる。</p> <p>6.6.4 主要仕様 原子炉保護設備の主要仕様を第6.6.1表及び第6.6.1図に示す。</p> <p>6.6.5 試験検査 原子炉保護設備は、その機能の健全性を確認するため、定期的に緊急シャ断のための性能検査及び緊急シャ断検査を行う。 (1) 原子炉トリップ演算処理装置及びトリップチャンネルは4チャンネルで構成しているため、原子炉運転中でも、中性子源領域中性子束高及び中間領域中性子束高を除く任意の1チャンネルについて、模擬入力による原子炉トリップ演算処理装置の設定値確認及びトリップチャンネルの論理回路の作動確認を行うことができる。 この場合、残りの原子炉トリップ演算処理装置及びトリップチャンネルにより、安全保護機能（原子炉トリップ）を維持することができる。 (2) 原子炉トリップ遮断器は四つのトリップチャンネルごとに設け、原子炉運転中でも、任意の一つのトリップチャンネルについて、テストスイッチ操作により原子炉トリップ遮断器が開放することを確認することができる。</p>	<p>相違理由</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p>

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

第24条 安全保護回路

大阪発電所3/4号炉（リファレンスプラント）	女川原子力発電所2号炉	泊発電所3号炉	相違理由
<p>6.6.7 手順等</p> <p>(1) 安全保護系のデジタル計算機が収納された盤については、施錠管理方法を定め運用する。</p> <p>(2) 発電所への出入りについては、出入管理方法を定め運用する。</p> <p>(3) 安全保護系の保守ツールの使用については、パスワードの管理及び入力操作に関する手順等並びにソフトウェアの使用について検証及び妥当性を確認することを定め運用する。</p> <p>(4) 適切に保守管理を行うとともに、故障時においては補修を行う。</p> <p>(5) 保守管理や盤の施錠管理、出入管理、パスワード管理等の管理手順に関する教育を実施する。</p> <p style="text-align: right;">【説明資料（別添）】</p> <p>【まとめ資料作成範囲外のため。設置許可(令和3年5月)より引用】↓</p> <p>6.6.5 評価</p> <p>(1) 単一故障 原子炉保護設備を構成する論理回路及び原子炉トリップ遮断器には多重性を持たせている。すなわち、原則として“2 out of 4”で構成される論理回路は、連絡ケーブルをも含めて4重トレイン構成としている。これらのトレインは、電気的、物理的に分離しているため、単一のトレインの故障で保護機能を失うことはない。</p> <p>(2) 独立性 原子炉保護設備は、相互干渉が起らないように、物理的、電気的に独立性を持たせている。すなわち、論理回路、原子炉トリップ遮断器、連絡ケーブル等は供給電源（直流2母線、無停電電源4母線）を含めて独立な構成としている。</p> <p>(3) フェイルセイフ 原子炉保護設備を構成するリレー、原子炉トリップ遮断器の不足電圧コイルは常時励磁状態とし、駆動電源の喪失、系の遮断に対して原子炉保護動作をとる方向に作動するよう設計している。</p> <p>(4) 運転中試験 原子炉保護設備は、論理回路及び原子炉トリップ遮断器に関し、プラント運転中にも試験ができる設計としている。</p>	<p>(2) 工学的安全施設作動回路は、運転中にテスト信号を出して各々の検出器並びにチャンネルの試験を行うことができる。なお、論理回路を含む全系統の試験については、定期検査時に行うことができるよう設計する。</p> <p>6.6.6 手順等 安全保護系に関して、以下の内容を含む手順等を定め、適切な管理を行う。</p> <p>(1) 安全保護回路を有する制御盤については、施錠管理方法を定め、運用する。</p> <p>(2) 発電所の出入管理方法については、「1.1.1.5 人の不法な侵入等の防止(3)手順等」に示す。</p> <p>(3) 発電所の出入管理に係る教育については、「1.1.1.5 人の不法な侵入等の防止(3)手順等」に示す。</p> <p>6.6.7 評価</p> <p>(1) 安全保護系は、運転時の異常な過渡変化時には、その異常状態を検知し、原子炉保護系を自動的に作動させることにより、燃料要素の許容損傷限界を超えないようにすることができる。</p> <p>(2) 安全保護系は、偶発的な制御棒引抜きのような原子炉停止系のいかなる単一の誤動作に対しても燃料要素の許容損傷限界を超えない設計としている。</p> <p>(3) 安全保護系は、事故時にあつては、直ちにこれを検知し、原子炉保護系及び工学的安全施設の作動を自動的に開始することができる。</p> <p>(4) 安全保護系は、多重性及び電気的・物理的な独立性を有する設計とし、実際に起こると考えられるいかなる単一機器の故障若しくは単一機器の使用状態からの取り外しによっても、その安全保護機能が妨げられることはない。</p> <p>(5) 安全保護系は、系の遮断、駆動源の喪失においても、安全上許容される状態（フェイル・セイフ又はフェイル・アズ・イズ）になる設計としている。</p> <p>(6) 安全保護系は、一般計測制御系とは極力分離し、部分的に共用した場合でも一般計測制御系の故障が安全保護系に影響を与えない設計としている。</p> <p>(7) 安全保護系は、通常運転中においても、定期的に機能試験を行うことができる。</p> <p>(8) 安全保護系は、監視装置、警報等によりその作動状況が確認でき</p>	<p>この場合、残りの原子炉トリップ遮断器により、安全保護機能（原子炉トリップ）を維持することができる。</p> <p>6.6.6 手順等</p> <p>(1) 安全保護系のデジタル計算機が収納された盤については、施錠管理方法を定め運用する。</p> <p>(2) 発電所への出入りについては、出入管理方法を定め運用する。</p> <p>(3) 安全保護系の保守ツールの使用については、パスワードの管理及び入力操作に関する手順等並びにソフトウェアの使用について検証及び妥当性を確認することを定め運用する。</p> <p>(4) 適切に保守管理を行うとともに、故障時においては補修を行う。</p> <p>(5) 保守管理や盤の施錠管理、出入管理、パスワード管理等の管理手順に関する教育を実施する。</p> <p style="text-align: right;">【説明資料（別添）】</p> <p>6.6.7 評価</p> <p>(1) 単一故障 原子炉保護設備を構成する論理回路及び原子炉トリップ遮断器には多重性を持たせている。すなわち、原則として“2 out of 4”で構成される論理回路は、連絡ケーブルをも含めて4チャンネル構成としている。これらのチャンネルは、電気的、物理的に分離しているため、単一のチャンネルの故障で保護機能を失うことはない。</p> <p>(2) 独立性 原子炉保護設備は、相互干渉が起らないように、物理的、電気的に独立性を持たせている。すなわち、論理回路、原子炉トリップ遮断器、連絡ケーブル等は供給電源（直流2母線、無停電電源4母線）を含めて独立な構成としている。</p> <p>(3) フェイル・セイフ 原子炉保護設備を構成するリレー、原子炉トリップ遮断器の不足電圧コイルは常時励磁状態とし、駆動電源の喪失、系の遮断に対して原子炉保護動作をとる方向に作動するよう設計している。</p> <p>(4) 運転中試験 原子炉保護設備は、論理回路及び原子炉トリップ遮断器に関し、プラント運転中にも試験ができる設計としている。</p>	<p>既許可構成の相違</p> <p>記載の充実(追加要求事項の対象外、大阪参照)</p> <p>既許可記載の相違</p>

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

第24条 安全保護回路

大阪発電所3/4号炉（リファレンスプラント）	女川原子力発電所2号炉	泊発電所3号炉	相違理由
<p>論理回路は、テストスイッチを操作して、各チャンネルの双安定回路のリレーをトリップ状態にする等の方法により、正常に動作したことを確認できる。</p> <p>なお、原子炉トリップ遮断器の動作テストは、“2 out of 4” ロジック構成のため、各トレインごとに実動作テストを行うことができる。</p> <p>(5) 手動操作 必要な場合、手動でも原子炉保護動作を行えるように、中央制御盤に原子炉トリップスイッチを2個設け、いずれか1個のスイッチ操作により原子炉トリップ信号を発することができる。</p> <p>(6) 作動状況の確認 原子炉保護設備の作動状況は、警報、表示灯、炉外核計装等により確認することができる。</p> <p>【まとめ資料作成範囲外のため、設置許可(令和3年5月)より引用】↑</p>	<p>る設計としている。</p> <p>(9) 安全保護系は、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ことができる設計としている。</p>	<p>論理回路は、テストスイッチを操作して、各チャンネルの双安定回路のリレーをトリップ状態にする等の方法により、正常に動作したことを確認できる。</p> <p>なお、原子炉トリップ遮断器の動作テストは、“2 out of 4” ロジック構成のため、チャンネルごとに実動作テストを行うことができる。</p> <p>(5) 手動操作 必要な場合、手動でも原子炉保護動作を行えるように、中央制御盤に原子炉トリップスイッチを2個設け、いずれか1個のスイッチ操作により原子炉トリップ信号を発することができる。</p> <p>(6) 作動状況の確認 原子炉保護設備の作動状況は、警報、表示灯、炉外核計装等により確認することができる。</p> <p>(7) 不正アクセス防止 原子炉保護設備のデジタル計算機は、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。</p> <p>【説明資料（2.1：P24条-30,31）（2.2：P24条31）（2.3：P24条-31,32）（2.4：P24条-33）（2.5：P24条-33）（2.6：P24条-34-36）（2.7：P24条-37）（2.9：P24条-40）】</p>	<p>既許可記載の相違</p> <p>記載内容の相違（女川実績の反映）</p>

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

第24条 安全保護回路

大飯発電所3/4号炉（リファレンスプラント）	女川原子力発電所2号炉	泊発電所3号炉	相違理由
<p>6.7 工学的安全施設作動設備</p> <p>6.7.1 概要</p> <p>工学的安全施設作動設備は、1次冷却材喪失事故あるいは主蒸気管破断事故等に際して、炉心、原子炉冷却材圧力バウンダリ及び原子炉格納容器バウンダリを保護するための設備を起動するものである。</p> <p>工学的安全施設作動設備は、安全保護系のプロセス計装から信号を受けて、工学的安全施設を作動させる2トレインの論理回路で構成する。</p> <p>【まとめ資料作成範囲外のため、設置許可(令和3年5月)より引用】↓</p> <p>6.7.2 設計方針</p> <p>(1) 工学的安全施設作動設備は、単一故障あるいは使用状態からの単一の取り外しを行っても、安全保護機能を喪失しないような多重性を有する設計とする。</p> <p>(2) 工学的安全施設作動設備は、チャンネル相互を分離し、チャンネル間の独立性を図る設計とする。</p> <p>(3) 工学的安全施設作動設備は、駆動源の喪失又は系の遮断に対して、最終的に安全な状態に落ち着くような設計とする。</p> <p>(4) 工学的安全施設作動設備は、原子炉の運転中に定期的に試験を行い、機能が喪失していないことを確認できる設計とする。</p>		<p>6.7 工学的安全施設作動設備</p> <p>6.7.1 概要</p> <p>工学的安全施設作動設備は、原子炉冷却材喪失、主蒸気管破断等に際して、炉心の冷却を行い、原子炉格納容器バウンダリを保護し、発電所周辺の公衆の安全を確保するための設備を作動させる。</p> <p>6.7.2 設計方針</p> <p>(1) 多重性</p> <p>工学的安全施設作動設備は、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り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。</p> <p>(2) 独立性</p> <p>工学的安全施設作動設備は、通常運転時、保守時、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において独立性を確保する設計とする。</p> <p>(3) 過渡時の機能</p> <p>工学的安全施設作動設備は、運転時の異常な過渡変化時に、その異常な状態を検知し、原子炉停止系を含む適切な系統を自動的に作動させ、燃料要素の許容損傷限界を超えない設計とする。</p> <p>(4) 設計基準事故時の機能</p> <p>工学的安全施設作動設備は、設計基準事故時に、その異常な状態を検知し、原子炉トリップ及び必要な工学的安全施設を自動的に作動させる設計とする。</p> <p>(5) 故障時の機能</p> <p>工学的安全施設作動設備は、駆動源の喪失、系統の遮断等が生じた場合においても、最終的に発電用原子炉施設が安全な状態に落ち着く設計とする。</p> <p>(6) 計測制御系との分離</p> <p>工学的安全施設作動設備は、計測制御系とは機能的に分離した設計とする。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、安全保護系へ影響を与えない設計とする。</p> <p>(7) 試験可能性</p> <p>工学的安全施設作動設備は、原子炉の運転中に定期的に試験及び検査ができるとともに、その健全性及び多重性の維持を確認するため、独立</p>	<p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p>

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

第24条 安全保護回路

大阪発電所3/4号炉（リファレンスプラント）	女川原子力発電所2号炉	泊発電所3号炉	相違理由
<p>(6) 工学的安全施設作動設備は、作動状況が確認できる設計とする。</p> <p>(5) 工学的安全施設作動設備は、自動的に作動し、また必要な場合には手動でも作動できる設計とする。</p> <p>なお、運転員の手動操作を期待するものは、容易に操作可能で、操作に必要な状態表示があり、操作が正しく行われたことが表示される設計とする。</p> <p>(7) システムの導入段階、更新段階、試験段階でコンピュータウィルスが混入することを防止し、システムへのアクセス管理ができる設計とすることで、承認されていない動作や変更を防ぐ設計とする。</p> <p>6.7.4 主要設備</p>		<p>に各チャンネルの試験及び検査ができる設計とする。</p> <p>(8) 電源喪失に対する考慮 工学的安全施設作動設備は、無停電の計装用交流母線から給電し、一定時間の全交流動力電源喪失時にも機能を喪失しない設計とする。</p> <p>(9) 作動状況の確認 工学的安全施設作動設備は、監視機能を設け作動状況が確認できる設計とする。</p> <p>(10) 手動操作 工学的安全施設作動設備は、自動的に作動し、また、必要な場合には手動でも作動でき運転員の手動操作を期待するものは容易に操作可能な設計とする。 また、手動操作に必要な情報及びその操作が正しく行われたことを示す情報が、明確に表示できる設計とする。</p> <p>(11) 不正アクセス防止 工学的安全施設作動設備のデジタル計算機は、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。</p> <p>【説明資料（2.1：P24条-30, 31）（2.2：P24条31）（2.3：P24条-31, 32）（2.4：P24条-33）（2.5：P24条-33）（2.6：P24条-34-36）（2.7：P24条-37）（2.9：P24条-40）】</p> <p>6.7.3 主要設備 (1) 構成 工学的安全施設作動設備は第6.7.1図に示すように、工学的安全施設</p>	<p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>設備の相違(工学的安全施設作動設備)</p> <p>・泊は、工学的安全施設作動に係わる信号の流れが、原子炉安全保護盤→工学的安全施設作動盤→安全系現場制御監視盤であり、すべての盤がデジタル計算機である。</p> <p>・大飯は、原子炉安全保護盤(デジタル計算機)→安全保護シーケンス盤(アナログ盤)であり、泊でいう工学的安全施設作動盤の機能を原子炉安全保護盤が兼ねている。</p> <p>・以上より、泊は原子炉保護設備と同様に、工学的安全施設作動設備に対しても不正アクセス防止を記載している。</p> <p>既許可記載の相違</p>

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

第24条 安全保護回路

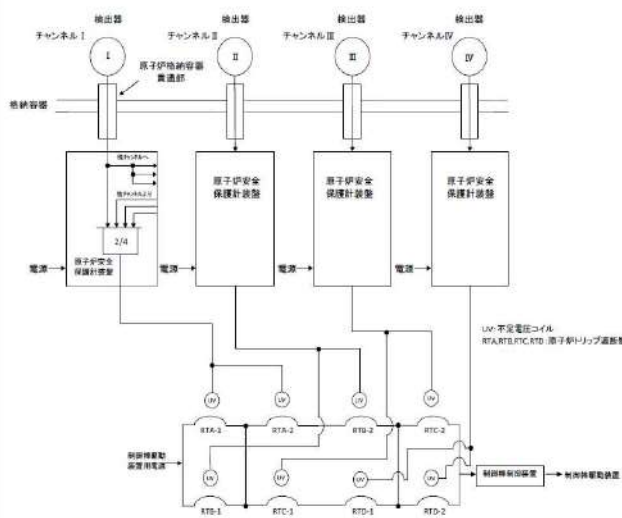
大飯発電所3/4号炉（リファレンスプラント）	女川原子力発電所2号炉	泊発電所3号炉	相違理由
<p>6.7.4.1 作動信号</p> <p>6.7.3 主要設備の仕様 工学的安全施設作動設備の主要設備の仕様を第6.7.1表に示す。</p> <p>【まとめ資料作成範囲外のため。設置許可(令和3年5月)より引用】↑</p>		<p>作動演算処理装置、工学的安全施設作動装置等で構成する。工学的安全施設作動演算処理装置は多重化された四つのチャンネル及び工学的安全施設作動装置は2系列化された工学的安全施設に各々対応した作動装置で構成し、自己診断機能を有するマイクロプロセッサを用いる。</p> <p>工学的安全施設作動演算処理装置は、安全保護回路のプロセス計装からの信号を入力し、工学的安全施設作動演算を行い、信号が設定値に達した場合には、チャンネルトリップ信号を発信する。</p> <p>工学的安全施設作動装置は、各々四つの工学的安全施設作動演算処理装置からの信号を入力し、二つ以上の工学的安全施設作動演算処理装置がチャンネルトリップ信号を発信した場合には、工学的安全施設作動信号を発信する“2 out of 4”方式とする。</p> <p>工学的安全施設作動設備の工学的安全施設作動演算処理装置及び工学的安全施設作動装置の駆動源には、電力を使用する。これらは駆動源の喪失、系統の遮断等が生じた場合においても、フェイル・セーフとなるか、又は故障と同時に現状維持（フェイル・アズ・イズ）になり、この現状維持の場合でも、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。</p> <p>なお、工学的安全施設作動設備は、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が保証されたソフトウェアを使用する。</p> <p>(2) 作動信号</p> <p>6.7.4 主要仕様 工学的安全施設作動設備の主要仕様を第6.7.1表、第6.5.1図に示す</p> <p>6.7.6 手順等 安全保護系の手順については、「6.6.6 手順等」に示す。</p>	<p>相違理由</p> <p>既許可記載の相違</p> <p>既許可記載の相違</p> <p>設備の相違（工学的安全施設作動設備）</p>

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

第24条 安全保護回路

大阪発電所3/4号炉（リファレンスプラント）

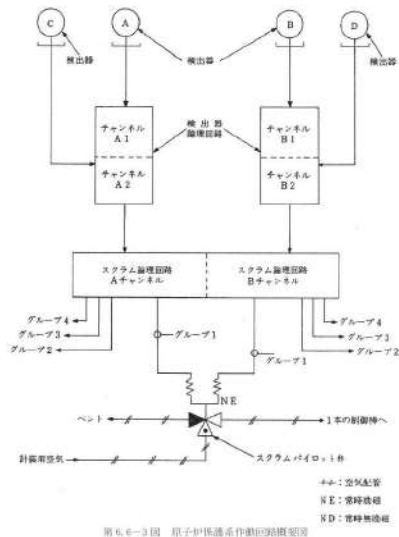
【まとめ資料作成範囲外のため。設置許可(令和3年5月)より引用】↓



第6.6.1図 原子炉保護設備概念図（2 out of 4の場合）

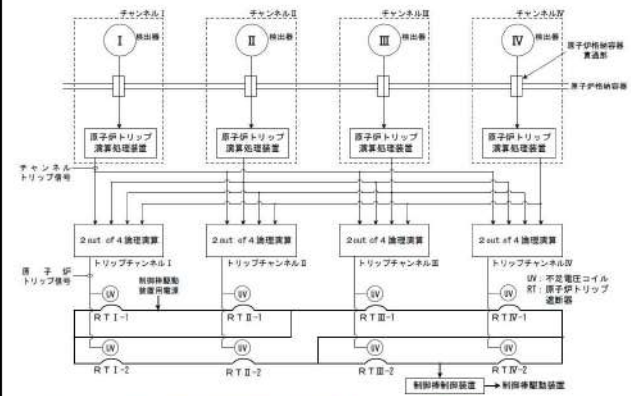
【まとめ資料作成範囲外のため。設置許可(令和3年5月)より引用】↑

女川原子力発電所2号炉

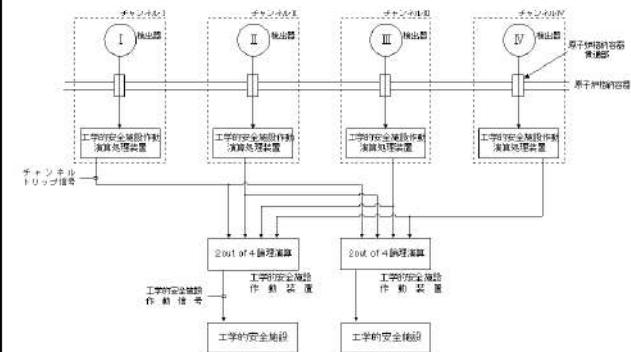


第6.6-3図 原子炉保護系作動回路概図

泊発電所3号炉



第6.6.1図 原子炉保護設備系統図（“2 out of 4”の場合）



第6.7.1図 工学的安全施設作動設備系統図

相違理由

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

第24条 安全保護回路

大阪発電所3/4号炉（リファレンスプラント）	女川原子力発電所2号炉	泊発電所3号炉	相違理由
	<p>2. 追加要求事項に対する適合方針</p> <p>2.1 安全保護回路の不正アクセス行為防止のための措置について</p> <p>「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（安全保護回路）第1項第六号において『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。』が要求されている。</p> <p>女川原子力発電所2号炉の安全保護回路は、検出信号処理において一部デジタル演算処理を行う機器があるほかは、アナログ回路で構成している。安全保護回路（原子炉保護系、工学的安全施設作動回路）の不正アクセス行為による被害防止については、デジタル演算処理を行う機器も含め、下記の対策を実施している。</p> <p>(1) 物理的及び電気的アクセスの制限対策</p> <p>発電所への入城に対しては、出入管理により物理的アクセスを制限する。電気的アクセスについては、安全保護回路を有する制御盤を施錠管理しており、また、保守ツールの接続口自体を設けておらず、回路変更等の不正行為が実施できない構造となっていることにより、管理されない変更を防止している。</p> <p>(2) ハードウェアの物理的な分離又は機能的な分離対策</p> <p>安全保護回路の信号は、安全保護回路→データ収集装置→安全パラメータ表示システム伝送装置→防護装置 [] を介して外部に伝送している。この信号の流れにおいて、安全保護系からは発信されるのみであり、外部からの信号を受信しないこと、及びハードウェアを直接接続しないことで物理的及び機能的分離を行っている。</p> <p>(3) 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防止対策</p> <p>安全保護回路とそれ以外の設備との間で用いる信号はアナログ信号（接点信号を含む）であり、外部ネットワークを介した不正アクセス等による被害を受けることはない。</p> <p>安全保護回路の信号で外部ネットワークへのデータ伝送の必要がある場合は、防護装置 [] を介して安全保護回路の信号を一方（送信機能のみ）通信に制限し外部からのデータ書き込み機能を設けないことでウイルスの侵入及び外部からの不正アクセスを防止している。</p> <p>(4) システムの導入段階、更新段階又は試験段階で承認されていない動作や変更を防ぐ対策</p>	<p>2. 追加要求事項に対する適合方針</p> <p>2.1 安全保護回路の不正アクセス行為防止のための措置について</p> <p>「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（安全保護回路）第1項第六号にて要求されている『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ができるものとする。』に対して、安全保護回路の機能を果たす安全保護系のデジタル計算機である安全保護設備（原子炉安全保護盤、工学的安全施設作動盤、安全系現場制御監視盤）は、下記の対策を実施している。</p> <p>(1) 物理的及び電気的アクセスの制限対策</p> <p>発電所への入城に対しては、出入管理により物理的アクセスを制限する。電気的アクセスについては、安全保護設備の盤を施錠管理しており、また、保守ツールの接続箇所は施錠管理された盤内で常時物理的に切り離しており、ソフトウェア変更等の不正行為が実施できない構造となっていることにより、管理されない変更を防止している。</p> <p>(2) ハードウェアの物理的な分離又は機能的な分離対策</p> <p>安全保護設備の信号は、安全保護設備→ゲートウェイ→防護装置 [] →データ収集計算機→防護装置 [] を介して外部に伝送している。この信号の流れにおいて、安全保護系からは発信されるのみであり、外部からの信号を受信しないこと、及び保守ツールの接続箇所は施錠管理された盤内で常時物理的に切り離すことで物理的及び機能的分離を行っている。</p> <p>(3) 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防止対策</p> <p>安全保護回路の信号で外部ネットワークへのデータ伝送の必要がある場合は、防護装置 [] 等を介して安全保護回路の信号を一方（送信機能のみ）通信に制限している。また、ソフトウェア変更手順を定めることで、ウイルスの侵入及び外部からの不正アクセスを含む管理されないソフトウェアの変更を防止している。</p> <p>(4) システムの導入段階、更新段階又は試験段階で承認されていない動作や変更を防ぐ対策</p>	<p>記載内容の相違(女川実績の反映)</p> <p>【女川】 設備の相違(デジタル計算機) ・泊は、安全保護回路の機能を果たす安全保護系は、デジタル計算機。</p> <p>【女川】 設備の相違(保守ツール接続箇所) ・泊は、安全保護設備(デジタル計算機)への保守ツールの接続箇所は必要。</p> <p>【女川】 設備の相違 [] ・泊は、 [] による対策を根幹としつつ、ゲートウェイ及び [] によって多層防護している。</p> <p>【女川】 設備の相違(設備間の信号) ・泊は、安全保護設備(デジタル計算機)とそれ以外の設備との間の通信はデジタル信号。</p> <p>【女川】 設備の相違 []</p> <p>【女川】 設備の相違(ハードウ</p>

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

第24条 安全保護回路

大飯発電所3/4号炉（リファレンスプラント）	女川原子力発電所2号炉	泊発電所3号炉	相違理由
<p>安全保護回路のうち、一部デジタル演算処理を行う機器のソフトウェア又はハードウェア回路は、「安全保護系へのデジタル計算機の適用に関する規程」（JEAC4620-2008）及び「デ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）に準じて設計、製作、試験及び変更管理の各段階で検証及び妥当性確認がなされたソフトウェア又はハードウェア回路を使用している。</p> <p>安全保護回路のうち、一部デジタル演算処理を行う機器は、固有のプログラム言語を使用（一般的なコンピュータウイルスが動作しない環境）するとともに、保守以外の不要な演算回路へのアクセス制限対策として入域制限及び設定値変更作業での鍵管理、また、保守ツールの接続口自体を設けない構造となっていることにより、関係者以外の不正な変更等を防止している。</p> <p>また、安全保護系のうちデジタル処理部のある機器は、供給者独自のハードウェアを使用した、測定対象に応じた演算処理を行う専用のデジタル処理部であり、不要な機能は有していない（別紙7参照）。</p> <p>(5) 耐ノイズ・サージ対策</p> <p>安全保護回路は、雷・誘導サージ・電磁波障害等による擾乱に対して、制御盤へ入線する電源受電部や外部からの信号入出力部にラインフィルタや絶縁回路を設置している。</p> <p>ケーブルは金属シールド付ケーブルを適用し、金属シールドは接地して電磁波の侵入を防止する設計としている。安全保護回路は、鋼製の筐体に格納し、筐体を接地することで電磁波の侵入を防止する設計としている。</p> <p>※ 通信状態を監視し送信元、送信先及び送信内容を制限することにより、目的外の通信を遮断する装置</p>	<p>安全保護回路のうち、一部デジタル演算処理を行う機器のソフトウェア又はハードウェア回路は、「安全保護系へのデジタル計算機の適用に関する規程」（JEAC4620-2008）及び「デ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）に準じて設計、製作、試験及び変更管理の各段階で検証及び妥当性確認がなされたソフトウェア又はハードウェア回路を使用している。</p> <p>安全保護回路のうち、一部デジタル演算処理を行う機器は、固有のプログラム言語を使用（一般的なコンピュータウイルスが動作しない環境）するとともに、保守以外の不要なソフトウェアへのアクセス制限対策として入域制限及び現場作業での鍵管理、また、保守ツールの接続箇所は施錠管理された盤内で常時物理的に切り離していることにより、関係者以外の不正な変更等を防止している。</p> <p>また、安全保護設備は、供給者独自のハードウェアを使用した、専用のデジタル計算機であり、不要な機能は有していない（別紙7参照）。</p> <p>(5) 耐ノイズ・サージ対策</p> <p>安全保護設備は、雷・誘導サージ・電磁波障害等による擾乱に対して、盤へ入線する電源受電部や外部からの信号入出力部にラインフィルタや絶縁回路を設置している。</p> <p>通信ラインのケーブルは光ケーブルを適用し、サージの影響を防止する設計としている。また、安全保護設備は、開発検証時において耐ノイズ/サージに対する耐性を確認している。（ノイズ・サージ試験/準拠規格 JIS C 61000-4-4、電波障害試験/参考規格 JIS C 61000-4-3 等）</p> <p>※1 ハードウェアレベルで一方向のみ通信を許可する装置 ※2 通信状態を監視し送信元、送信先及び送信内容を制限することにより、目的外の通信を遮断する装置</p>	<p>安全保護設備は、「安全保護系へのデジタル計算機の適用に関する規程」（JEAC4620-2008）及び「デ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）に準じて設計、製作、試験及び変更管理の各段階で検証及び妥当性確認がなされたソフトウェアを使用している。</p> <p>安全保護設備は、固有のプログラム言語を使用（一般的なコンピュータウイルスが動作しない環境）するとともに、保守以外の不要なソフトウェアへのアクセス制限対策として入域制限及び現場作業での鍵管理、また、保守ツールの接続箇所は施錠管理された盤内で常時物理的に切り離していることにより、関係者以外の不正な変更等を防止している。</p> <p>また、安全保護設備は、供給者独自のハードウェアを使用した、専用のデジタル計算機であり、不要な機能は有していない（別紙7参照）。</p> <p>(5) 耐ノイズ・サージ対策</p> <p>安全保護設備は、雷・誘導サージ・電磁波障害等による擾乱に対して、盤へ入線する電源受電部や外部からの信号入出力部にラインフィルタや絶縁回路を設置している。</p> <p>通信ラインのケーブルは光ケーブルを適用し、サージの影響を防止する設計としている。また、安全保護設備は、開発検証時において耐ノイズ/サージに対する耐性を確認している。（ノイズ・サージ試験/準拠規格 JIS C 61000-4-4、電波障害試験/参考規格 JIS C 61000-4-3 等）</p> <p>※1 ハードウェアレベルで一方向のみ通信を許可する装置 ※2 通信状態を監視し送信元、送信先及び送信内容を制限することにより、目的外の通信を遮断する装置</p>	<p>エア回路)</p> <p>・泊の安全保護設備（デジタル計算機）に、ハードウェア回路は存在しない。</p> <p>【女川】 設備の相違(光ケーブル)</p> <p>・泊は、安全保護設備（デジタル計算機）とそれ以外の設備との間の通信はデジタル信号であり、光ケーブルを適用している。</p>


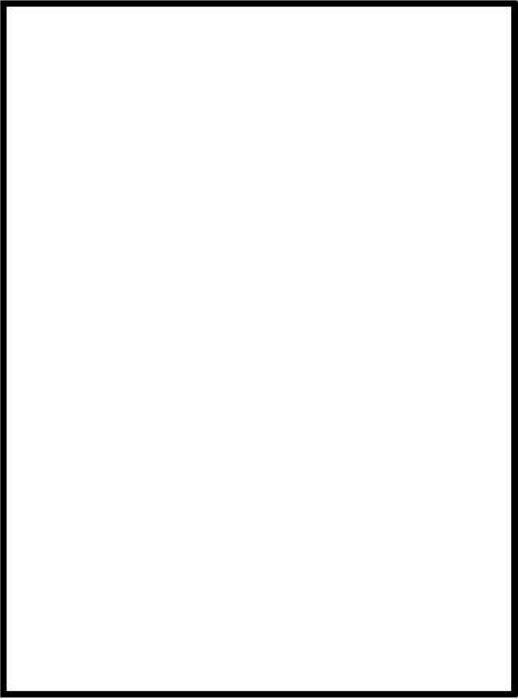
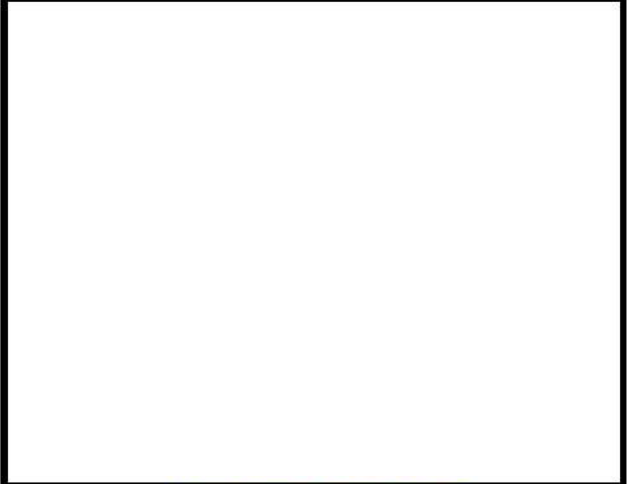
赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

第24条 安全保護回路

大阪発電所3/4号炉（リファレンスプラント）	女川原子力発電所2号炉	泊発電所3号炉	相違理由
<p>2. 安全保護回路</p> <p>2.1 概要</p> <p>「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（安全保護回路）第1項第六号にて要求されている「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ができるものとする。」に対して、安全保護系のデジタル計算機は、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ことができる設計とする。</p>		<p>2.2 概要</p> <p>「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（安全保護回路）第1項第六号にて要求されている「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ができるものとする。」に対して、安全保護設備（原子炉安全保護盤、工学的安全施設作動盤、安全系現場制御監視盤）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ことができる設計とする。</p>	<p>設備の相違(安全保護設備)</p> <ul style="list-style-type: none"> ・泊は、2.1にて用語を定義。 ・大阪は、安全保護系のデジタル計算機として「原子炉安全保護計装盤」のみが該当し、2.2以降は当該盤名称を主語としている。 ・以降、同様の相違は、相違理由の記載を省略する。

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

第24条 安全保護回路

大飯発電所3/4号炉（リファレンスプラント）	女川原子力発電所2号炉	泊発電所3号炉	相違理由
<p>2.2 原子炉安全保護計装盤の物理的分離</p> <p>原子炉安全保護計装盤は、盤の施錠等により、ハードウェアを直接接続させないことで物理的に分離している。例えば、原子炉安全保護計装盤はUSBポートが接続できない構造とすることで、USBメモリの使用による不正アクセスその他の被害を防止している。</p>  <p>図1 USBメモリー使用によるコンピュータウイルス感染の例 (ITセキュリティ教育資料抜粋)</p> <p>2.3 安全保護回路の物理的分離対策</p> <p>安全保護回路は、不正アクセスを防止するため、安全保護系盤等の扉には施錠を行い、許可された者以外はハードウェアを直接接続できない対策を実施している。</p>  <p>第2.3図 安全保護系の施錠管理</p> <p>枠囲みの内容は防護上の観点から公開できません。</p> <p>【比較のため、2.7(2)を移動して掲載】 (2) 電気的分離について</p> <p>安全保護回路からインターフェース部（計測制御系）の分離は、アイソレータや補助継電器等の隔離装置（第2.7-3 図参照）を用いて電気的分離（計測制御系で短絡等の故障が生じて安全保護回路に影響を与えない。）を行う。</p> <p>アイソレータは電気/光変換によって、入力信号と出力信号とを分離しており、補助継電器はコイルと接点間で入力信号と出力信号とを分離している。</p> <p>隔離装置は、入力信号側の回路の電気的故障が出力信号側の回路に伝播しないよう、入力信号と出力信号が電気的に絶縁されている。</p>	<p>2.3 安全保護設備の物理的分離</p> <p>安全保護設備は、盤の施錠等により、許可された者以外にはハードウェアを直接接続させないことで物理的に分離している。例えば、安全保護設備にはUSBポートを設けないことで、USBメモリの使用による不正アクセスその他の被害を防止している。</p>  <p>図1 安全保護設備の物理的分離</p>	<p>2.3 安全保護設備の物理的分離</p> <p>安全保護設備は、盤の施錠等により、許可された者以外にはハードウェアを直接接続させないことで物理的に分離している。例えば、安全保護設備にはUSBポートを設けないことで、USBメモリの使用による不正アクセスその他の被害を防止している。</p>	<p>相違理由</p> <p>記載内容の相違</p> <ul style="list-style-type: none"> 泊は、保守時や事故対応時に、例外的に許可された者がハードウェアを直接接続可能であることを記載している。 <p>設備の相違</p> <ul style="list-style-type: none"> 泊は、安全保護設備に、USBポートが存在しない。 <p>【女川】</p> <p>設備の相違(設備間のデータ伝送)</p> <ul style="list-style-type: none"> 泊は、安全保護設備(デジタル計算機)から他設備へのデータ伝送は、光(デジタル)信号。

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

第24条 安全保護回路

大飯発電所3/4号炉（リファレンスプラント）

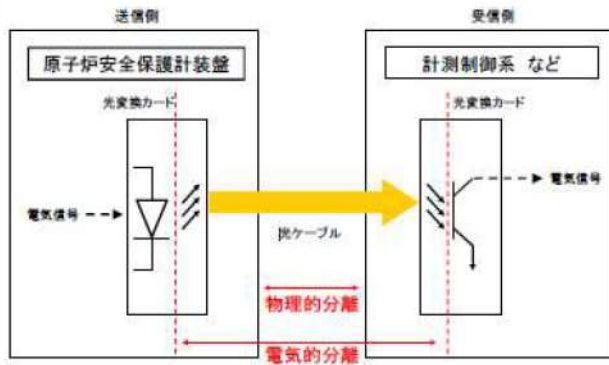
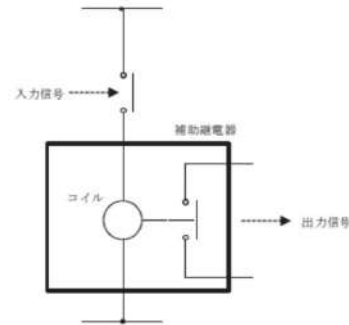
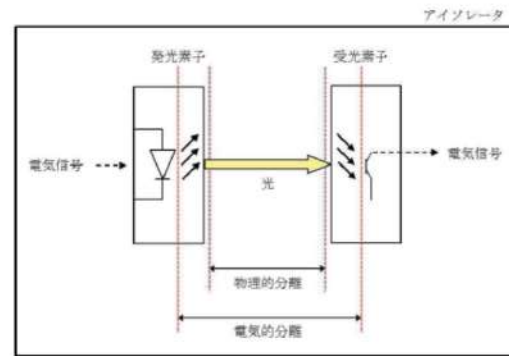


図2 光通信における分離概念図

女川原子力発電所2号炉

また、原子炉核計装系の検出部が表示、記録計用検出部と共用しているが、計測制御系の短絡、地絡又は断線によって安全保護回路に影響を与えない設計とする。



第2.7-3図 計測制御系との分離概念図

泊発電所3号炉

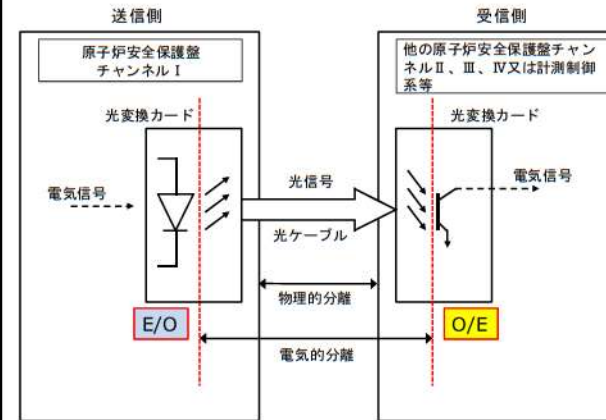


図2 光通信における分離概念図

相違理由

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

第24条 安全保護回路

大阪発電所3/4号炉（リファレンスプラント）	女川原子力発電所2号炉	泊発電所3号炉	相違理由
<p>2.3 原子炉安全保護計装盤の機能的分離</p> <p>原子炉安全保護計装盤の信号を外部へ伝送する場合は、外部ネットワークと直接接続せず、遮断装置（ゲートウェイ）を介した片方向通信に制限している。また、遮断装置のソフトウェアを送信ソフトウェアのみとし、外部からの信号を受信しないことで、機能的分離を行っている。</p> <p>2.4 コンピュータウイルスによる被害の防止</p> <p>原子炉安全保護計装盤は、固有のプログラム言語を使用（一般的なコンピュータウイルスが動作しない環境）するとともに、保守以外のソフトウェアへの不要なアクセス制限対策として、パスワード管理等によって関係者以外の不正な変更等を防止している。また、設計、製作、試験及び変更管理の各段階で後述する検証及び妥当性確認（コンピュータウイルスの混入防止を含む。）がなされたソフトウェアを使用している。</p> <p>さらに、ウイルス侵入防止対策および内部脅威者対策も含め、当社の原子力施設に係る情報システムへの妨害行為又は破壊行為を防止するため、「情報システムセキュリティ計画」を策定し、所要の措置を講じるとともに、同措置によりセキュリティが確保されていることを定期的に確認することとしている。</p> <p>準拠規格 「安全保護系へのデジタル計算機の適用に関する規程」 (JEAC4620-2008)</p>	<p>2.4 安全保護設備の機能的分離</p> <p>安全保護設備の信号を外部へ伝送する場合は、外部ネットワークと直接接続せず、防護装置（一方のみに通信を許可する装置等）を介した一方方向通信に制限し、ハードウェアレベルで外部からの信号を受信しないことで、機能的分離を行っている。</p> <p>2.5 コンピュータウイルスによる被害の防止</p> <p>安全保護設備は、固有のプログラム及び言語を使用（一般的なコンピュータウイルスが動作しない環境）するとともに、保守以外のソフトウェアへの不要なアクセス制限対策としてパスワード管理等によって関係者以外の不正な変更等を防止している。また、設計、製作、試験及び変更管理の各段階で後述する検証及び妥当性確認（コンピュータウイルスの混入防止含む。）がなされたソフトウェアを使用している。</p> <p>さらに、ウイルス侵入防止対策および内部脅威者対策も含め、当社の原子力施設に係る情報システムへの妨害行為又は破壊行為を防止するため、「情報システムセキュリティ計画」を策定し、所要の措置を講じるとともに、同措置によりセキュリティが確保されていることを定期的に確認することとしている。</p> <p>準拠規格 「安全保護系へのデジタル計算機の適用に関する規程」 (JEAC4620-2008)</p>	<p>設備の相違</p> <p>記載表現の相違</p> <ul style="list-style-type: none"> ・泊は、1.2(3)「第1項第6号について」と記載を統一した。 ・大阪も、1.2(3)「第1項第6号について」では「一方方向」と記載している。 	

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

第24条 安全保護回路

大阪発電所3/4号炉（リファレンスプラント）	女川原子力発電所2号炉	泊発電所3号炉	相違理由
<div data-bbox="103 145 674 639" style="border: 2px solid black; height: 310px; width: 255px;"></div> <p data-bbox="219 644 553 667">表1 情報システムセキュリティ計画の概要</p> <p data-bbox="134 671 665 692">出典元：大阪発電所 情報システムセキュリティ計画（原子力運転制御系システム関連）</p>		<div data-bbox="1355 165 1975 660" style="border: 2px solid black; height: 310px; width: 277px;"></div> <p data-bbox="1462 665 1868 687">表1 情報システムセキュリティ計画の概要</p> <p data-bbox="1469 692 1861 715">出典元：泊発電所 情報システムセキュリティ計画</p>	

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

第24条 安全保護回路

大阪発電所3号炉（リファレンスプラント）	女川原子力発電所2号炉	泊発電所3号炉	相違理由
<p>2.5 設計、製作、試験及び変更管理の各段階における検証及び妥当性確認</p> <p>安全保護設備のプログラムは、工場製作段階から以下の想定脅威に対する対策及び品質保証活動に基づくライフプロセスにおける各段階での検証と妥当性の確認等を調達管理に基づき適切に行うことで、高い信頼性を実現している。</p> <p>準拠規格 「安全保護系へのデジタル計算機の適用に関する規程」 (JEAC4620-2008) 「デ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)</p>	<p>2.5 安全保護系の検証及び妥当性確認について</p> <p>安全保護回路のうち、一部デジタル演算処理を行う機器のソフトウェア又はハードウェア回路は、工場製作段階から以下の品質保証活動に基づくライフサイクルプロセスにおける各段階での検証と妥当性確認を適切に行うことで高い信頼性を実現している。</p> <p>安全保護回路のうち一部デジタル演算処理を行う機器の検証及び妥当性確認について別紙-8に示す。</p> <p>【比較のため、2.6を移動して掲載】</p> <p>2.6 想定脅威に対する対策について</p> <p>安全保護回路のうち、デジタル処理を行っている機器については、工場製作段階から第2.6表に示す想定脅威に対する対策を適切に行うことで高い信頼性を有している。</p> <p>現場据付以降の作業におけるインサイダー等に対するセキュリティ対策について別紙4に、安全保護系のうちデジタル処理部のある機器のシステムへ接続可能なアクセスについて別紙5に示す。</p>	<p>2.6 設計、製作、試験及び変更管理の各段階における検証及び妥当性確認</p> <p>安全保護設備は、工場製作段階から以下の品質保証活動に基づくライフサイクルプロセスにおける各段階での検証と妥当性確認を適切に行うことで高い信頼性を実現している。</p> <p>安全保護設備の検証及び妥当性確認について別紙-8に示す。</p> <p>安全保護設備のプログラムは、工場製作段階から以下の想定脅威に対する対策及び品質保証活動に基づくライフプロセスにおける各段階での検証と妥当性の確認等を調達管理に基づき適切に行うことで、高い信頼性を実現している。</p> <p>準拠規格 「安全保護系へのデジタル計算機の適用に関する規程」 (JEAC4620-2008) 「デ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)</p> <p>現場据付以降の作業におけるインサイダー等に対するセキュリティ対策について別紙4に、安全保護設備のシステムへ接続可能なアクセスについて別紙5に示す。</p>	<p>記載内容の相違(女川実績の反映)</p> <p>【女川】 設備の相違(デジタル計算機)</p> <p>記載内容の相違(女川実績の反映)</p> <p>【女川】 設備の相違(デジタル計算機)</p>

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

第24条 安全保護回路

大阪発電所3/4号炉（リファレンスプラント）	女川原子力発電所2号炉	泊発電所3号炉	相違理由																								
<table border="1" data-bbox="85 180 253 456"> <thead> <tr> <th colspan="2">想定脅威</th> </tr> </thead> <tbody> <tr> <td>外部脅威</td> <td>外部からの侵入</td> </tr> <tr> <td rowspan="3">内部脅威</td> <td>設備の脆弱性</td> </tr> <tr> <td>不正ソフトウェア利用</td> </tr> <tr> <td>持込機器・媒体による改ざん・漏えい</td> </tr> <tr> <td>作業環境からの不正アクセス</td> <td></td> </tr> <tr> <td>人的要因</td> <td>作業ミス、知識不足による情報漏えい等</td> </tr> </tbody> </table> <p data-bbox="212 464 566 512">表2 ソフトウェアのウイルス侵入対策 (想定脅威に対する対策 (工場製作及び出荷))</p>	想定脅威		外部脅威	外部からの侵入	内部脅威	設備の脆弱性	不正ソフトウェア利用	持込機器・媒体による改ざん・漏えい	作業環境からの不正アクセス		人的要因	作業ミス、知識不足による情報漏えい等	<p data-bbox="853 153 1193 172">第2.8表 想定脅威に対する対策 (工場製作及び出荷)</p> <div data-bbox="736 177 1308 783" style="border: 2px solid black; width: 100%; height: 100%;"></div> <div data-bbox="1014 794 1283 815" style="border: 1px solid black; width: fit-content; margin: 0 auto; padding: 2px;">利用済の内容は防護上の観点から公開できません。</div>	<table border="1" data-bbox="1361 169 1973 791"> <thead> <tr> <th></th> <th>想定脅威</th> <th>対策</th> </tr> </thead> <tbody> <tr> <td>外部脅威</td> <td>外部からの侵入</td> <td rowspan="4" style="border: 2px solid black; width: 100%; height: 100%;"></td> </tr> <tr> <td rowspan="3">内部脅威</td> <td>設備の脆弱性</td> </tr> <tr> <td>不正ソフトウェア利用</td> </tr> <tr> <td>持込機器・媒体による改ざん・漏えい</td> </tr> <tr> <td>人的要因</td> <td>作業ミス、知識不足による情報漏えい等</td> </tr> </tbody> </table> <p data-bbox="1491 794 1845 842">表2 ソフトウェアのウイルス侵入対策 (想定脅威に対する対策 (工場製作及び出荷))</p>		想定脅威	対策	外部脅威	外部からの侵入		内部脅威	設備の脆弱性	不正ソフトウェア利用	持込機器・媒体による改ざん・漏えい	人的要因	作業ミス、知識不足による情報漏えい等	
想定脅威																											
外部脅威	外部からの侵入																										
内部脅威	設備の脆弱性																										
	不正ソフトウェア利用																										
	持込機器・媒体による改ざん・漏えい																										
作業環境からの不正アクセス																											
人的要因	作業ミス、知識不足による情報漏えい等																										
	想定脅威	対策																									
外部脅威	外部からの侵入																										
内部脅威	設備の脆弱性																										
	不正ソフトウェア利用																										
	持込機器・媒体による改ざん・漏えい																										
人的要因	作業ミス、知識不足による情報漏えい等																										

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

第24条 安全保護回路

大飯発電所3/4号炉（リファレンスプラント）

女川原子力発電所2号炉

泊発電所3号炉

相違理由

段階	JEAC4620
設計プロセス	安全保護設備に対するシステムの要求事項からソフトウェアの設計仕様を決定する。
製作プロセス	ソフトウェア設計仕様からソフトウェアを製作するプロセス。
試験プロセス	製作されたソフトウェアに対して試験を実施するプロセス。ソフトウェア実装に対しては、試験のハードウェアが同一または同等システムとして行う試験がある。
変更プロセス	実施の最終システムソフトウェアを試験するプロセス。
変更プロセス	仕様変更によるソフトウェアの変更するプロセス。

表3 ライフプロセスの各段階での確認

第2.5-1表 ライフサイクルプロセスにおける各段階での対策

段階	内容	検証・妥当性確認方法
設計プロセス	安全保護システムの要求事項からソフトウェア又はハードウェア回路に対する仕様を決定する。	・安全保護システム要求事項がシステム設計要求仕様と正しく反映されていること。 ・システム設計要求仕様がハードウェア、ソフトウェア又はハードウェア回路の設計要求仕様と正しく反映されていること。
製作プロセス	ソフトウェア又はハードウェア回路に対する仕様からソフトウェア又はハードウェア回路を製作する。	設計要求仕様に基づいてソフトウェア又はハードウェア回路が製作されていること。
試験プロセス	製作されたソフトウェア又はハードウェア回路に対して、設計要求どおり製作されていることを試験により確認する。	検証及び妥当性確認が可能なソフトウェア又はハードウェア回路とになっていること。必要な検証を経て製作されたソフトウェア又はハードウェア回路をハードウェアと統合した後の全体システムについて、最終的に安全保護システム要求事項が正しく実現されていることを確認するために妥当性確認を実施。
変更プロセス	ソフトウェア又はハードウェア回路の変更が生じた場合、変更仕様を決定し、変更を行うライフサイクルプロセスから、変更の実施内容に応じて必要とされる各々のプロセスを順次実施する。	必要となる各検証に応じて実施。

段階	内容	対策
設計プロセス	安全保護設備に対するプラントの要求事項から、ソフトウェアの設計仕様を作成する。	[Redacted]
製作プロセス	安全保護設備ソフトウェア設計要求仕様から安全保護設備で実現するためのプログラムを作成する。	
試験プロセス	安全保護設備に対して、ハードウェアを統合し、その統合したシステムが設計要求どおり製作されていることを試験により確認する。	
装荷プロセス	安全保護設備を発電所に搬入・装荷し、本設備のソフトウェアの復元が妥当であることを確認する。 (工場出荷時の状態に復元されていること。)	
変更プロセス	安全保護設備のソフトウェアの変更が生じた場合、変更仕様を決定し、変更を行うライフサイクルプロセスから、変更の実施内容に応じて必要とされる各々のプロセスを順次実施。	

表3 ライフプロセスの各段階での対策

原子炉安全保護計装機のデジタル化にあたっては、システムの設計、製作、試験、変更管理の各段階で、「安全保護系へのデジタル計算機の適用に関する規程」(JEAC4620-2008)及び「デ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、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、当社は供給者による検証及び妥当性確認の各段階において、検証されたソフトウェアを使用していることを確認している。

安全保護回路のうち、一部デジタル演算処理を行う機器のソフトウェア又はハードウェア回路は、設計、製作、試験、変更管理の各段階で「安全保護系へのデジタル計算機の適用に関する規程」(JEAC4620-2008)及び「デ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)に準じて、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ため、検証及び妥当性確認を実施する。

安全保護設備のデジタル化にあたっては、システムの設計、製作、試験、変更管理の各段階で、建設時は「安全保護系へのデジタル計算機の適用に関する指針」(JEAG4609-1999)に基づき検証及び妥当性確認を実施し、「安全保護系へのデジタル計算機の適用に関する規程」(JEAC4620-2008)及び「デ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)に改定されてからは、これらに基づき、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、当社は供給者による検証及び妥当性確認の各段階において、検証及び妥当性確認がなされたソフトウェアを使用していることを確認している。

記載内容の相違(適用規格の版)
 ・泊3号炉建設時、最新のJEAG4609は1999年版。
 ・常に最新版の規格に基づき、V&Vを実施している点で、大飯との差異はない。

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

第24条 安全保護回路

大飯発電所3/4号炉（リファレンスプラント）

導入後の変更についても、下記フロー図のシステム要求事項から試験まで、導入時と同様に検証項目の検証1～妥当性確認までを実施している。

また、当社も各段階において確実に実施されていることを確認するとともに、導入後の変更においても、同様の管理を行っている。

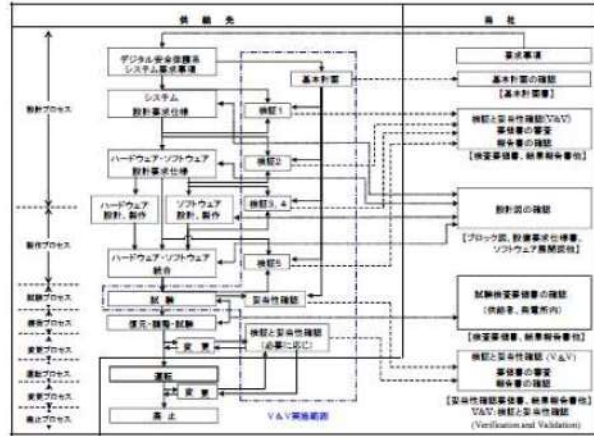


図3 安全保護設備の検証及び妥当性確認

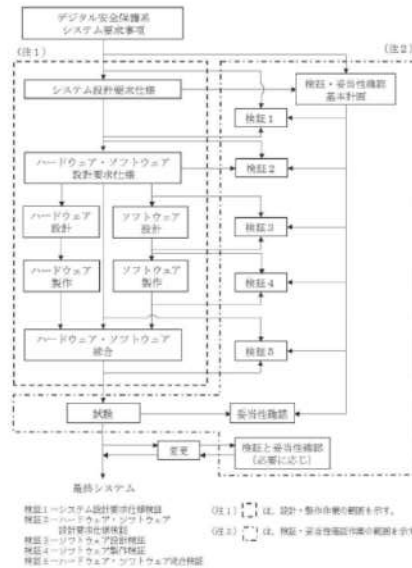
検証項目	検証内容(JEAC4609)
検証1	システム設計要求仕様検証 JEAC4620のデジタル安全保護システム要求事項が正しくシステム設計要求仕様に反映されていることを検証する。
検証2	ハードウェア・ソフトウェア設計要求仕様検証 システム設計要求仕様が正しくハードウェア・ソフトウェア設計要求仕様に反映されていることを検証する。
検証3	ソフトウェア設計検証 ソフトウェア設計要求仕様が正しくソフトウェア設計に反映されていることを検証する。
検証4	ソフトウェア製作検証 ソフトウェア設計通りに正しくソフトウェアが製作されていることを検証する。
検証5	ハードウェア・ソフトウェア統合検証 ハ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通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、JEAC4620のデジタル安全保護システム要求事項を満たしていることを確認する。

表4 検証項目と検証内容

女川原子力発電所2号炉

なお、設計要求仕様の変更及びソフトウェアの変更が生じた際は、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、変更を実施する。必要に応じ、変更箇所及び変更の影響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。

以下に、検証及び妥当性確認の流れと内容を示す。



注：ハードウェア回路の検証にあたっては、「ソフトウェア」の部分で「ハードウェア回路」に置き換えて、検証及び妥当性確認を実施する。

第2.5-1図 検証及び妥当性確認

泊発電所3号炉

導入後の変更についても、下記フロー図のシステム要求事項から試験まで、導入時と同様に検証項目の検証1～妥当性確認までを実施している。

また、当社も各段階において確実に実施されていることを確認するとともに、導入後の変更においても、同様の管理を行っている。

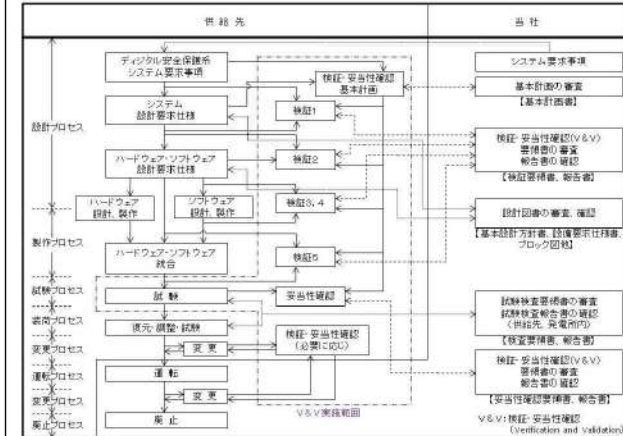


図3 安全保護設備の検証及び妥当性確認

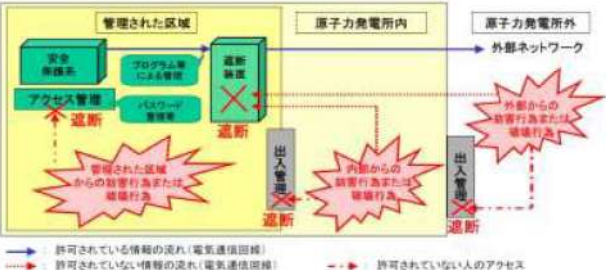
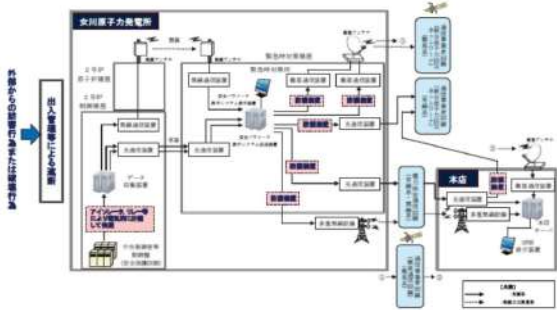

検証項目	検証内容
検証1	システム設計要求仕様検証 安全保護システムへの要求事項が正しく設備の基本設計方針書に反映されていることを検証
検証2	ハードウェア・ソフトウェア設計要求仕様検証 基本設計方針書の要求事項が正しくハードウェア・ソフトウェア設計要求図書に反映されていることを検証
検証3	ソフトウェア設計検証 ソフトウェアの設計要求図書が正しくソフトウェア設計に反映されていることを検証
検証4	ソフトウェア製作検証 ソフトウェア設計通りに正しくソフトウェアが製作されていることを検証
検証5	ハードウェア・ソフトウェア統合検証 ハードウェアとソフトウェアを統合してハードウェア・ソフトウェア設計要求仕様通りのシステムとなっていることを検証
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、デジタル安全保護システム要求事項を満足していることを確認

表4 検証項目と検証内容

相違理由

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

第24条 安全保護回路

大飯発電所3/4号炉（リファレンスプラント）	女川原子力発電所2号炉	泊発電所3号炉	相違理由
<p>2.6 物理的及び電気的アクセスの制限</p> <p>発電所への入城に対する出入管理及び、原子炉安全保護計装盤に対する盤の施錠と貸出管理等により、物理的アクセスを制限している。加えて、原子炉安全保護計装盤扉を開放した場合は中央制御室に警報が発信するため、不正侵入等の物理的アクセスを防止することができる。また、原子炉安全保護計装盤のシステムへのパスワード管理等により、電気的アクセスも制限している。以上の物理的及び電気的アクセスの制限により、管理されないソフトウェアの変更を防止している。</p> <p>原子炉安全保護計装盤を外部ネットワークと接続させる場合には直接接続せず、遮断装置（ゲートウェイ）を介した片方向通信に制限することで、外部からの不正なアクセス及びコンピュータウィルス等の侵入を防止している。</p>  <p>図4 不正アクセス防止の概念図</p>	<p>2.4 外部からの不正アクセス行為の防止について</p> <p>原子力発電所への入城については、出入管理により制限しており、外部からの人的妨害行為又は破壊行為を防止している。</p> <p>安全保護系は、外部ネットワークと直接接続は行っておらず、外部システムと接続する必要があるデータ等については、安全保護回路とデータ収集装置の間に設けたアイソレータやリレー等の隔離装置により電気的に分離しているとともに、信号の流れが安全保護回路からデータ伝送装置へ信号を送信するのみの一方向となっている。また、安全パラメータ表示システム伝送装置と外部システム（統合原子力防災ネットワーク、本店）の間には、防護装置 [] を介して接続している。また、安全保護系のうちデジタル処理部を持つ機器は、外部からのデータ書き込み機能を設けないことでウィルスの侵入等を防止している。</p>  <p>第2.4図 外部ネットワークとの接続構成概要図</p> <p>[] 特図みの内容は防護上の観点から公開できません。</p>	<p>2.7 物理的及び電気的アクセスの制限</p> <p>発電所への入城に対する出入管理及び、安全保護設備に対する盤の施錠と貸出管理等により、物理的アクセスを制限している。加えて、原子炉安全保護計装盤扉を開放した場合は中央制御室に警報が発信するため、不正侵入等の物理的アクセスを防止することができる。また、安全保護設備のシステムへのパスワード管理等により、電気的アクセスも制限している。以上の物理的及び電気的アクセスの制限により、管理されないソフトウェアの変更を防止している。</p> <p>安全保護設備は、外部ネットワークと直接接続は行っておらず、外部システムと接続する必要があるデータ等については、安全保護設備に設けた光変換カードにより電気的に分離しているとともに、ソフトウェアを送信ソフトウェアのみとすることで、信号の流れが安全保護設備からデータ収集計算機へ信号を送信するのみの一方向となっている。また、安全保護設備とデータ収集計算機との間に設けた防護装置 [] により、ハードウェアレベルで信号の流れが安全保護設備から信号を送信するのみの一方向となっている。また、データ収集計算機と外部システムとの間には、防護装置 [] を介して接続している。また、安全保護設備は、ソフトウェア変更を以降2.8に示すとおりに管理することで、ウィルスの侵入を含む管理されないソフトウェアの変更を防止している。</p>  <p>図4 不正アクセス防止の概念図</p>	<p>記載内容の相違(女川実績の反映) 【女川】 設備の相違 []</p>

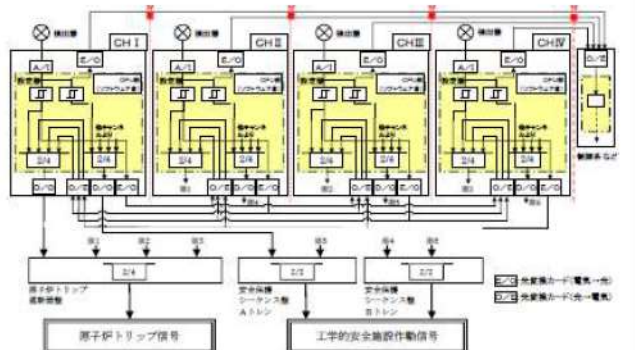
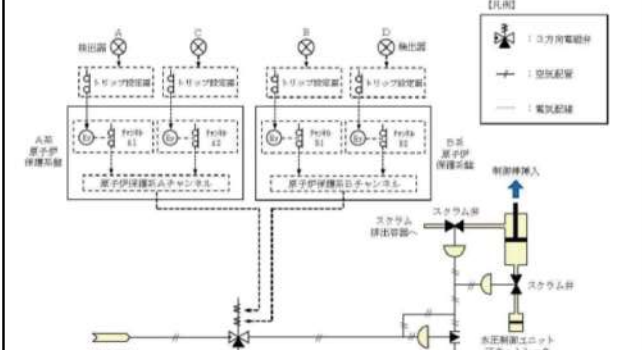
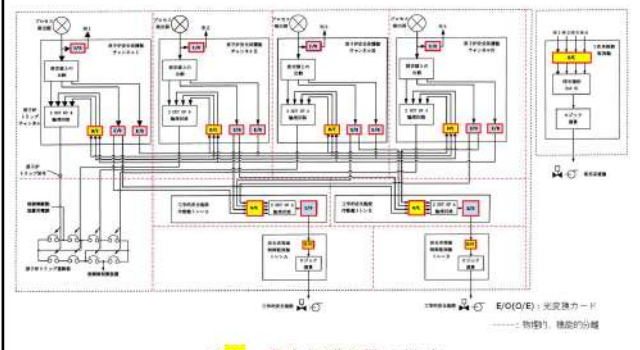
赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

第24条 安全保護回路

大飯発電所3/4号炉（リファレンスプラント）	女川原子力発電所2号炉	泊発電所3号炉	相違理由
<p>2.7 原子炉安全保護計装盤の概要</p> <p>原子炉安全保護計装盤は、プロセス信号（検出器からの信号）を処理、監視するとともに、設定値との比較を行い、原子炉停止信号及び工学的安全施設作動に係わる信号を原子炉トリップ遮断器盤及び安全保護シーケンス盤へ発信する設備である。</p> <p>原子炉安全保護計装盤は、チャンネル毎に盤筐体に収納し、他の各チャンネル間及び計測制御系などとは物理的分離、機能的分離を行っている。システム構成機器又はチャンネルの単一故障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、安全保護機能を喪失することがないように多重性を有する設計としている。</p> <p>また、誤信号発生等による誤動作・誤不動作を防止するため、原子炉保護系は、基本的に二重の「1 out of 2」方式とし、工学的安全施設を作動させる検出器は、多重性を持った構成とする。</p>	<p>2. 安全保護回路</p> <p>2.2 安全保護回路の概要</p> <p>安全保護回路は、検出信号処理において一部デジタル演算処理を行う機器があるほかは、アナログ回路で構成している。また、安全保護回路とそれ以外の設備との間で用いる信号はアナログ信号（接点信号を含む。）であり、外部ネットワークを介した不正アクセス等による被害を受けることはない。</p> <p>例として、原子炉保護系の構成例を第2.2-1 図に示す。</p> <p>安全保護回路は、検出器からの信号を受信し、原子炉保護系を自動的に作動させる回路と、工学的安全施設を作動させる信号を発する工学的安全施設作動回路で構成しており、多重性及び電気的・物理的な独立性を持たせている。</p> <p>安全保護系の構成機器のうちデジタル処理部のある機器として起動領域モニタ（SRNM）、平均出力領域モニタ（APRM）、プロセス放射線モニタリング設備（PRRM）及び主蒸気管トンネル温度の監視装置がある。安全保護系の構成機器のうちデジタル処理部のある機器を第2.2-1 表及び第2.2-2 表に示す。</p> <p>安全保護系は、相互干渉が起らないように、物理的、電気的独立性を持たせている。その系統を構成するチャンネル相互が分離され、独立性を持つ設計とし、多重性を有するチャンネル構成とすることにより、機器又はチャンネルの単一故障又は使用状態からの単一の取り外しを行った場合でも、安全保護系機能を喪失することはない。</p> <p>また、誤信号発生等による誤動作・誤不動作を防止するため、原子炉保護設備及び工学的安全施設作動設備は、基本的に「2 out of 4」方式とし、工学的安全施設を作動させる検出器は、多重性を持った構成とする。</p>	<p>2.8 安全保護設備の概要</p> <p>安全保護設備は、デジタル計算機で構成している。</p> <p>安全保護設備の構成を図5に示す。</p> <p>原子炉安全保護盤は、プロセス信号（検出器からの信号）を処理、監視するとともに、設定値との比較を行い、原子炉停止信号及び工学的安全施設作動に係わる信号を原子炉トリップ遮断器盤及び工学的安全施設作動盤へ発信する設備である。</p> <p>安全保護設備は、チャンネル毎及びトレン毎に盤筐体に収納し、他の各チャンネル間、トレン間及び計測制御系などとは物理的分離、機能的分離を行っている。システム構成機器又はチャンネルの単一故障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も、安全保護機能を喪失することがないように多重性を有する設計としている。</p> <p>また、誤信号発生等による誤動作・誤不動作を防止するため、原子炉保護設備及び工学的安全施設作動設備は、基本的に「2 out of 4」方式とし、工学的安全施設を作動させる検出器は、多重性を持った構成とする。</p>	<p>相違理由</p> <p>記載内容の相違(女川実績の反映)</p> <p>【女川】</p> <p>設備の相違(設備間の信号)</p> <ul style="list-style-type: none"> ・泊は、安全保護設備（デジタル計算機）とそれ以外の設備との通信はデジタル信号。 ・設備の相違(工学的安全施設作動盤) ・泊は、工学的安全施設作動に係わる信号の流れが、原子炉安全保護盤→工学的安全施設作動盤→安全系現場制御監視盤である。 ・大飯は、原子炉安全保護盤→安全保護シーケンス盤(アナログ盤)であり、泊でいう工学的安全施設作動盤の機能を原子炉安全保護盤が兼ねている。 <p>【女川】</p> <p>設備の相違(デジタル計算機)</p> <p>設備の相違(工学的安全施設作動盤)</p> <ul style="list-style-type: none"> ・泊は、工学的安全施設作動盤及び安全系現場制御監視盤を、2系列化して設置している。 <p>記載内容の相違(女川実績の反映)</p>

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

第24条 安全保護回路

大飯発電所3/4号炉（リファレンスプラント）	女川原子力発電所2号炉	泊発電所3号炉	相違理由
<p>また、原子炉安全保護計装盤には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している。ウイルス等の起因事象に関係なく、システムに不具合等があれば中央制御室に警報が発信する。</p>  <p>図5 原子炉安全保護計装盤の構成</p>	<p>【比較のため、2.7(1)を移動して掲載】 2.7 物理的分離及び電気的分離について (1)物理的分離について 安全保護回路と計測制御系とは、電源、検出器、ケーブル・ルート及び原子炉格納容器を貫通する計装配管を原則として分離する設計とする。 計測制御系のケーブルを安全保護回路のケーブルと同じケーブル・ルートに敷設した場合には、安全保護回路のケーブルと同等の扱いとする設計とする。 安全保護回路と計測制御系で計装配管を共用する場合は、安全保護回路の計装配管として設計する。 安全保護系は、原子炉水位及び原子炉圧力を検出する計装配管ヘッダの一部を計測制御系と共用すること、及び原子炉核計装系の検出部※が表示、記録計用検出部と共用される以外は計測制御系とは完全に分離する等、計測制御系での故障が安全保護系に影響を与えない設計とする（第2.7-1,2 図参照）。 ※：検出器、演算装置、電路を含む。</p> <p>なお、今回の設置許可申請に関する改造工事で安全保護回路に変更を施している場合についても基準適合性が図られていることを別紙2のとおり確認した。 また、安全保護系に関わる過去のトラブル情報を抽出し、女川2号炉の安全保護系の設計面へ反映すべき事項を確認した結果、対応済み又は反映不要であることを別紙3のとおり確認した。</p>  <p>第2.2-1図 原子炉保護系の構成例</p>	<p>安全保護系と計測制御系とは、電源、検出器、ケーブルルートを原則として分離する設計とする。</p> <p>計測制御系のケーブルを安全保護系のケーブルと同じケーブルルートに敷設した場合には、安全保護系のケーブルと同等の扱いとする設計とする。</p> <p>安全保護系と計測制御系で計装配管を共用する場合は、安全保護系の計装配管として設計する。</p> <p>安全保護系の一部から計測制御系への信号を取り出す場合には、信号の分岐箇所に変換カード又は絶縁増幅器を使用し、計測制御系で回路の短絡、開放等の故障が生じて安全保護系へ影響を与えない設計とする。</p> <p>また、安全保護設備には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している。ウイルス等の起因事象に関係なく、システムに不具合等があれば中央制御室に警報が発信する。</p> <p>なお、今回の設置許可申請に関する改造工事で安全保護設備に変更を施していないことを別紙2のとおり確認した。</p> <p>また、安全保護系に関わる過去のトラブル情報を抽出し、泊3号炉の安全保護系の設計面へ反映すべき事項を確認した結果、反映不要であることを別紙3のとおり確認した。</p>  <p>図5 安全保護設備の構成</p>	<p>記載内容の相違(女川実績の反映) 【女川】 設備の相違(計装配管の共用) ・泊は、原子炉格納容器を貫通する計装配管について、安全保護系と計測制御系とで共用している箇所はない。</p> <p>記載内容の相違(女川実績の反映)</p> <p>記載内容の相違(女川実績の反映)</p>

泊発電所3号炉 DB基準適合性 比較表

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

第24条 安全保護回路

大飯発電所3/4号炉（リファレンスプラント）	女川原子力発電所2号炉	泊発電所3号炉	相違理由																																																																																																													
	<p>第2.2-1表 原子炉保護系の構成機器</p> <table border="1"> <thead> <tr> <th>信号の種類</th> <th>検出器</th> <th>設定器</th> </tr> </thead> <tbody> <tr><td>原子炉圧力高</td><td>アナログ</td><td>アナログ</td></tr> <tr><td>原子炉水位低</td><td>アナログ</td><td>アナログ</td></tr> <tr><td>ドライウエル圧力高</td><td>アナログ</td><td>アナログ</td></tr> <tr><td>中性子束高（平均出力領域モニタ）</td><td>アナログ</td><td>デジタル</td></tr> <tr><td>中間領域における原子炉周期短（起動領域モニタ）</td><td>アナログ</td><td>デジタル</td></tr> <tr><td>中性子束計装動作不能（起動領域モニタ及び平均出力領域モニタ）</td><td>アナログ</td><td>デジタル</td></tr> <tr><td>スタラム排出容器水位高</td><td>アナログ</td><td>アナログ</td></tr> <tr><td>主蒸気隔離弁閉</td><td>アナログ</td><td></td></tr> <tr><td>主蒸気止め弁閉</td><td>アナログ</td><td></td></tr> <tr><td>蒸気加減弁急閉</td><td>アナログ</td><td></td></tr> <tr><td>主蒸気管放射能高</td><td>アナログ</td><td>デジタル</td></tr> <tr><td>地震加速度大</td><td>アナログ</td><td></td></tr> <tr><td>手動</td><td>アナログ</td><td></td></tr> <tr><td>モードスイッチ「停止」</td><td>アナログ</td><td></td></tr> </tbody> </table> <p>第2.2-2表 工学的安全施設作動系の構成機器</p> <table border="1"> <thead> <tr> <th>機能</th> <th>信号の種類</th> <th>検出器</th> <th>設定器</th> </tr> </thead> <tbody> <tr><td rowspan="6">鎖 主蒸気隔離弁閉</td><td>原子炉水位低</td><td>アナログ</td><td>アナログ</td></tr> <tr><td>主蒸気管放射能高</td><td>アナログ</td><td>デジタル</td></tr> <tr><td>主蒸気管圧力低</td><td>アナログ</td><td>アナログ</td></tr> <tr><td>主蒸気管流量大</td><td>アナログ</td><td>アナログ</td></tr> <tr><td>主蒸気管トンネル温度高</td><td>アナログ</td><td>デジタル</td></tr> <tr><td>主復水器真空度低</td><td>アナログ</td><td>アナログ</td></tr> <tr><td rowspan="4">の非常用サス処理系の起動</td><td>ドライウエル圧力高</td><td>アナログ</td><td>アナログ</td></tr> <tr><td>原子炉水位低</td><td>アナログ</td><td>アナログ</td></tr> <tr><td>原子炉種鼠原子炉種放射能高</td><td>アナログ</td><td>デジタル</td></tr> <tr><td>燃料取替エリア放射能高</td><td>アナログ</td><td>デジタル</td></tr> <tr><td rowspan="2">低圧炉心スプレイス系の起動</td><td>原子炉水位低</td><td>アナログ</td><td>アナログ</td></tr> <tr><td>ドライウエル圧力高</td><td>アナログ</td><td>アナログ</td></tr> <tr><td rowspan="2">系の自動減圧</td><td>原子炉水位低</td><td>アナログ</td><td>アナログ</td></tr> <tr><td>ドライウエル圧力高</td><td>アナログ</td><td>アナログ</td></tr> <tr><td rowspan="2">発電機の起動</td><td>原子炉水位低</td><td>アナログ</td><td>アナログ</td></tr> <tr><td>ドライウエル圧力高</td><td>アナログ</td><td>アナログ</td></tr> <tr><td rowspan="2">離弁閉鎖</td><td>原子炉水位低</td><td>アナログ</td><td>アナログ</td></tr> <tr><td>ドライウエル圧力高</td><td>アナログ</td><td>アナログ</td></tr> </tbody> </table>	信号の種類	検出器	設定器	原子炉圧力高	アナログ	アナログ	原子炉水位低	アナログ	アナログ	ドライウエル圧力高	アナログ	アナログ	中性子束高（平均出力領域モニタ）	アナログ	デジタル	中間領域における原子炉周期短（起動領域モニタ）	アナログ	デジタル	中性子束計装動作不能（起動領域モニタ及び平均出力領域モニタ）	アナログ	デジタル	スタラム排出容器水位高	アナログ	アナログ	主蒸気隔離弁閉	アナログ		主蒸気止め弁閉	アナログ		蒸気加減弁急閉	アナログ		主蒸気管放射能高	アナログ	デジタル	地震加速度大	アナログ		手動	アナログ		モードスイッチ「停止」	アナログ		機能	信号の種類	検出器	設定器	鎖 主蒸気隔離弁閉	原子炉水位低	アナログ	アナログ	主蒸気管放射能高	アナログ	デジタル	主蒸気管圧力低	アナログ	アナログ	主蒸気管流量大	アナログ	アナログ	主蒸気管トンネル温度高	アナログ	デジタル	主復水器真空度低	アナログ	アナログ	の非常用サス処理系の起動	ドライウエル圧力高	アナログ	アナログ	原子炉水位低	アナログ	アナログ	原子炉種鼠原子炉種放射能高	アナログ	デジタル	燃料取替エリア放射能高	アナログ	デジタル	低圧炉心スプレイス系の起動	原子炉水位低	アナログ	アナログ	ドライウエル圧力高	アナログ	アナログ	系の自動減圧	原子炉水位低	アナログ	アナログ	ドライウエル圧力高	アナログ	アナログ	発電機の起動	原子炉水位低	アナログ	アナログ	ドライウエル圧力高	アナログ	アナログ	離弁閉鎖	原子炉水位低	アナログ	アナログ	ドライウエル圧力高	アナログ	アナログ		<p>【女川】 設備の相違(デジタル計算機)</p>
信号の種類	検出器	設定器																																																																																																														
原子炉圧力高	アナログ	アナログ																																																																																																														
原子炉水位低	アナログ	アナログ																																																																																																														
ドライウエル圧力高	アナログ	アナログ																																																																																																														
中性子束高（平均出力領域モニタ）	アナログ	デジタル																																																																																																														
中間領域における原子炉周期短（起動領域モニタ）	アナログ	デジタル																																																																																																														
中性子束計装動作不能（起動領域モニタ及び平均出力領域モニタ）	アナログ	デジタル																																																																																																														
スタラム排出容器水位高	アナログ	アナログ																																																																																																														
主蒸気隔離弁閉	アナログ																																																																																																															
主蒸気止め弁閉	アナログ																																																																																																															
蒸気加減弁急閉	アナログ																																																																																																															
主蒸気管放射能高	アナログ	デジタル																																																																																																														
地震加速度大	アナログ																																																																																																															
手動	アナログ																																																																																																															
モードスイッチ「停止」	アナログ																																																																																																															
機能	信号の種類	検出器	設定器																																																																																																													
鎖 主蒸気隔離弁閉	原子炉水位低	アナログ	アナログ																																																																																																													
	主蒸気管放射能高	アナログ	デジタル																																																																																																													
	主蒸気管圧力低	アナログ	アナログ																																																																																																													
	主蒸気管流量大	アナログ	アナログ																																																																																																													
	主蒸気管トンネル温度高	アナログ	デジタル																																																																																																													
	主復水器真空度低	アナログ	アナログ																																																																																																													
の非常用サス処理系の起動	ドライウエル圧力高	アナログ	アナログ																																																																																																													
	原子炉水位低	アナログ	アナログ																																																																																																													
	原子炉種鼠原子炉種放射能高	アナログ	デジタル																																																																																																													
	燃料取替エリア放射能高	アナログ	デジタル																																																																																																													
低圧炉心スプレイス系の起動	原子炉水位低	アナログ	アナログ																																																																																																													
	ドライウエル圧力高	アナログ	アナログ																																																																																																													
系の自動減圧	原子炉水位低	アナログ	アナログ																																																																																																													
	ドライウエル圧力高	アナログ	アナログ																																																																																																													
発電機の起動	原子炉水位低	アナログ	アナログ																																																																																																													
	ドライウエル圧力高	アナログ	アナログ																																																																																																													
離弁閉鎖	原子炉水位低	アナログ	アナログ																																																																																																													
	ドライウエル圧力高	アナログ	アナログ																																																																																																													

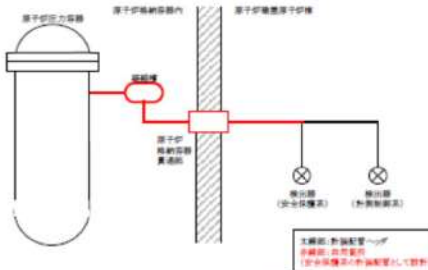
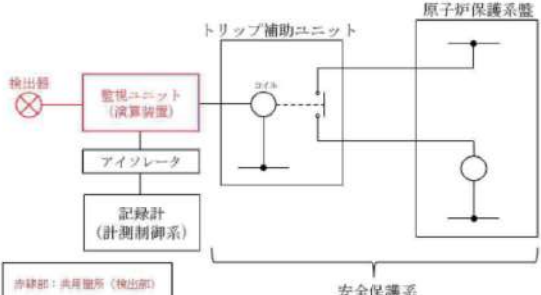
赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

第24条 安全保護回路

大飯発電所3/4号炉（リファレンスプラント）	女川原子力発電所2号炉	泊発電所3号炉	相違理由
	<p>【起動領域モニタ】</p> <p>【平均出力領域モニタ】</p> <p>【主蒸気管放射線モニタ】</p> <p>【原子炉内中性子密度放射線モニタ】 【燃料取扱エア放射線モニタ】 【主蒸気管トンネル温度】</p> <p>第 2.2-2 図 安全保護系 構成図</p>		<p>【女川】 設備の相違(デジタル計算機)</p>

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

第24条 安全保護回路

大飯発電所3/4号炉（リファレンスプラント）	女川原子力発電所2号炉	泊発電所3号炉	相違理由
	 <p>第2.7-1図 原子炉計装設備概念図（原子炉圧力の例）</p> <p>本機例：計装配管へは計装部、計装室計装部保護系へ計装配管にて計装</p>		<p>【女川】 設備の相違（計装配管の共用） ・泊は、原子炉格納容器を貫通する計装配管について、安全保護系と計測制御系とで共用している箇所はない。</p> <p>【女川】 設備の相違（検出器信号の共用） ・泊は、安全保護系の一部から計測制御系への信号を取り出す場合には、信号の分岐箇所にて光変換カードまたは絶縁増幅器を使用しており、安全保護系と計測制御系とで検出部を共用している箇所はない。</p>
	 <p>第2.7-2図 原子炉核計装系概念図（平均出力領域モニタの例）</p> <p>計装部：共用箇所（検出部）</p>		

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

第24条 安全保護回路

大阪発電所3/4号炉 (リファレンスプラント)	女川原子力発電所2号炉	泊発電所3号炉	相違理由
<p>2.8 原子炉安全保護計装盤のソフトウェア変更管理</p> <div style="border: 2px solid black; height: 400px; width: 100%;"></div> <p>2.9 耐ノイズ・サージ対策 原子炉安全保護計装盤は、雷・誘導サージ・電磁波障害などによる擾乱に対して、電源ラインへのラインフィルタの設置、現場との入出力回路への絶縁回路の設置、通信ラインにおける光ケーブルを適用している。 また、開発検証時に耐ノイズ/サージに対する耐性を確認している。 (ノイズ・サージ試験/準拠規格 JIS C 61000-4-4、電波障害試験/参考規格 JIS C 61000-4-3 等)</p>		<p>2.9 安全保護設備のソフトウェア変更管理</p> <div style="border: 2px solid black; height: 400px; width: 100%;"></div> <p>2.10 耐ノイズ・サージ対策 安全保護設備は、雷・誘導サージ・電磁波障害などによる擾乱に対して、電源ラインへのラインフィルタの設置、現場との入出力回路への絶縁回路の設置、通信ラインにおける光ケーブルを適用している。 また、開発検証時に耐ノイズ/サージに対する耐性を確認している。 (ノイズ・サージ試験/準拠規格 JIS C 61000-4-4、電波障害試験/参考規格 JIS C 61000-4-3 等)</p>	<p>相違理由</p> <p>名称の相違(安全計装盤室)</p> <p>運用の相違(パスワード変更頻度) ・泊は、定期保安工事や人事異動により、セキュリティ責任者やパスワードを付与すべき対象者が変更となる都度、パスワードを変更することで、常に必要最小限の者のみにパスワードを付与するよう管理している。</p> <p>運用の相違 ・泊は、ソフトウェアの改造工事の都度、改造後のソフトウェアについてバックアップを取得し、保管することで、常に最新版のソフトウェアをバックアップするよう管理している。</p>

泊発電所3号炉 DB基準適合性 比較表

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

第24条 安全保護回路

大阪発電所3/4号炉（リファレンスプラント）	女川原子力発電所2号炉	泊発電所3号炉	相違理由
	<p>上記2.1～2.7 に示す安全保護回路のセキュリティ対策における実効性の担保にあたり、当社及び安全保護回路に関する設計、工事の受注者が実施している管理内容について別紙6に示す。</p>	<p>上記2.1～2.10 に示す安全保護設備のセキュリティ対策における実効性の担保にあたり、当社及び安全保護設備に関する設計、工事の受注者が実施している管理内容について別紙6に示す。</p>	<p>記載内容の相違 （女川実績の反映）</p>

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

第24条 安全保護回路

大阪発電所3/4号炉（リファレンスプラント）	女川原子力発電所2号炉	泊発電所3号炉	相違理由
<p>別紙1 安全保護回路について、承認されていない動作や変更を防ぐための設計方針</p> <p>安全保護回路はハードワイヤーロジック（リレーや配線によるアナログ回路）で構成されており、検出信号処理において一部デジタル演算処理を行う機器があるほかは、アナログ回路で構成している。これらの回路に対し、承認されていない動作や変更を防ぐ措置として、以下を実施している。</p> <p>安全保護回路の変更が生じる場合は、上流文書から下流文書（別紙1-1 図参照）へ変更内容が反映されていることを設備図書で承認する。</p> <p>デジタル演算処理を行う機器のソフトウェア及びハードウェア回路は設計、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。</p> <p>改造後はインターロック試験や定期事業者検査等にて、安全保護回路が正しく動作することを複数の人間でチェックしている。</p> <p>なお、中央制御室への入域に対しては、出入管理により関係者以外のアクセスを防止している。</p> <p>安全保護系の制御盤の扉に施錠を行い、許可された者以外の回路の変更等の行為を防止している。</p> <p>安全保護回路及び設定値を変更する際は、中央制御室にて発電課長の許可を得て、発電課長の管理する鍵を借用する必要がある、外部からの人的妨害行為又は破壊行為を防止している。</p> <div data-bbox="857 786 1162 1345" data-label="Diagram"> <pre> graph TD A[安全保護系システム要求事項 (設置許可申請書)] --> B[システム設計要求仕様 (系统设计仕様書, 設定値根拠書)] B --> C[ハードウェア設計要求仕様 (インターロックブロック線図)] C --> D[ハードウェア設計・製作 (展開接続図)] D --> E[試験] </pre> </div> <p>別紙 1-1 図 安全保護系の設計・製作・試験の流れ（例）</p>	<p>別紙1 安全保護設備について、承認されていない動作や変更を防ぐための設計方針</p> <p>安全保護設備はデジタル計算機で構成されており、承認されていない動作や変更を防ぐ措置として、以下を実施している。</p> <p>安全保護設備の変更が生じる場合は、上流文書から下流文書（別紙1-1 図参照）へ変更内容が反映されていることを設備図書で承認する。</p> <p>安全保護設備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。</p> <p>改造後はインターロック試験や定期事業者検査等にて、安全保護設備が正しく動作することを複数の人間でチェックしている。</p> <p>なお、中央制御室への入域に対しては、出入管理により関係者以外のアクセスを防止している。</p> <p>安全保護設備の盤の扉に施錠を行い、許可された者以外のソフトウェアの変更等の行為を防止している。</p> <p>安全保護設備に係る現場作業を実施する際は、中央制御室にて発電課長（当直）の許可を得て、発電課長（当直）の管理する鍵を借用する必要がある、外部からの人的妨害行為又は破壊行為を防止している。</p> <div data-bbox="1529 786 1856 1345" data-label="Diagram"> <pre> graph TD A[デジタル安全保護系システム要求事項 (設置許可申請書)] --> B[システム設計要求仕様 (系统设计仕様書, 設定値根拠書)] B --> C[ハードウェア・ソフトウェア設計要求仕様 (機器設計仕様書, インターロックブロック線図)] C --> D[ハードウェア設計・製作 (展開接続図)] C --> E[ソフトウェア設計・製作 (ソフトウェア図)] D --> F[ハードウェア・ソフトウェア統合] E --> F F --> G[試験] </pre> </div> <p>別紙 1-1 図 安全保護設備の設計・製作・試験の流れ（例）</p>	<p>記載内容の相違（女川実績の反映）</p> <p>【女川】設備の相違（デジタル計算機）</p>	

泊発電所3号炉 DB基準適合性 比較表

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

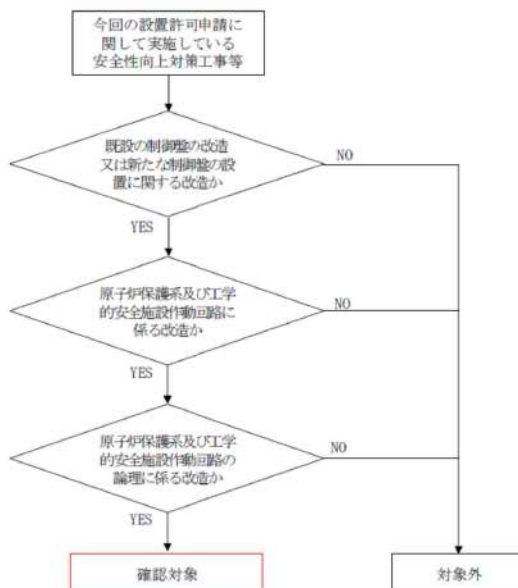
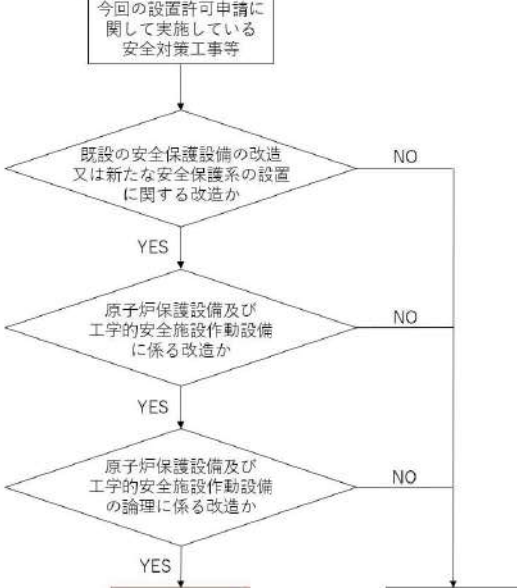
第24条 安全保護回路

大阪発電所3/4号炉（リファレンスプラント）	女川原子力発電所2号炉	泊発電所3号炉	相違理由
	<p>別紙2 今回の設置許可申請に関し、安全保護回路に変更を施している場合の基準適合性</p> <p>2011年3月以降に実施している安全性向上対策工事のうち、安全保護回路の変更に係る工事を抽出し、確認を行った。別紙2-1図の抽出フローに基づき抽出した結果、SA対策で実施するATWS緩和設備（自動減圧系作動阻止機能）設置が抽出された。</p> <p>安全保護回路の変更に係る設備の抽出結果を別紙2-4表に、抽出された設備についての個別の確認結果を(1)に示す。</p> <p>(1) ATWS緩和設備（自動減圧系作動阻止機能）について</p> <p>a. 目的</p> <p>原子炉停止機能喪失事象においては、発電用原子炉が臨界状態であるため、自動減圧系が作動すると、高圧炉心スプレイ系、残留熱除去系（低圧注水モード）及び低圧炉心スプレイ系から大量の冷水が注水され出力の急激な上昇につながる。このため原子炉停止機能喪失事象発生時に自動減圧系及び代替自動減圧回路（代替自動減圧機能）が作動しないようにATWS緩和設備（自動減圧系作動阻止機能）を設置する。</p> <p>b. 設備構成</p> <p>ATWS緩和設備（自動減圧系作動阻止機能）は、既存の自動減圧系の作動を阻止する機能を持つことから、ATWS緩和設備（自動減圧系作動阻止機能）の誤動作により、自動減圧系の作動を阻害することのないよう、十分に信頼性のある回路構成とする。</p> <p>ATWS緩和設備（自動減圧系作動阻止機能）の作動回路を別紙2-2図及び別紙2-3図に示す。ATWS緩和設備（自動減圧系作動阻止機能）は、単一故障により、自動減圧系の機能を阻害しないように、また、多重化された自動減圧系の独立性に悪影響がないように自動減圧系の論理回路ごとに設け、単一故障による誤動作及び不動作の防止のため、2 out of 3論理により動作する設計としている。</p> <p>c. 自動減圧系への影響について追加設置するATWS緩和設備（自動減圧系作動阻止機能）が、自動減圧系に対して悪影響を与えないことを以下に示す。</p>	<p>別紙2 今回の設置許可申請に関し、安全保護設備に変更を施している場合の基準適合性</p> <p>2011年3月以降に実施している安全性向上対策工事のうち、安全保護設備の変更に係る工事を抽出し、確認を行った。別紙2-1図の抽出フローに基づき抽出した結果、原子炉保護設備及び工学的安全施設作動設備の論理に係る改造は抽出されなかった。</p>	<p>記載内容の相違 ・（女川実績の反映） 【女川】 記載内容の相違 ・（工事実績） ・泊は、該当工事なし。 ・なお、ATWS緩和設備は、建設時(2011年3月以前)に設置済み。</p>

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

大阪発電所3/4号炉（リファレンスプラント）	女川原子力発電所2号炉	泊発電所3号炉	相違理由																						
	<p>別紙2-1表 A TWS緩和設備（自動減圧系作動阻止機能）の自動減圧系への影響（1/3）</p> <table border="1" data-bbox="790 183 1299 965"> <thead> <tr> <th>設置許可基準規則 第24条（安全保護回路）</th> <th>自動減圧系への影響</th> </tr> </thead> <tbody> <tr> <td>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。</td> <td>A TWS緩和設備（自動減圧系作動阻止機能）は、原子炉停止機能喪失事象時に自動減圧系の作動を阻止するものであり、運転時の異常な過渡変化時には使用しないため問題ない。</td> </tr> <tr> <td>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。</td> <td>A TWS緩和設備（自動減圧系作動阻止機能）の誤動作により、自動減圧系の作動を阻害することのないよう、以下のとおり十分に信頼性のある回路構成としているため問題ない。 自動減圧系の多重性、独立性に悪影響を与えないよう、区分ごとに自動減圧系作動阻止回路を設置する。 単一故障による誤動作の防止のため、「2 out of 3」論理により動作する設計とする。</td> </tr> <tr> <td>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。</td> <td>A TWS緩和設備（自動減圧系作動阻止機能）の誤動作により、自動減圧系の作動を阻害することのないよう、以下のとおり十分に信頼性のある回路構成としているため問題ない。 自動減圧系の多重性、独立性に悪影響を与えないよう、区分ごとに自動減圧系作動阻止回路を設置する。 単一故障による誤動作の防止のため、「2 out of 3」論理により動作する設計とする。</td> </tr> <tr> <td>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独立性を確保するものとする。こと。</td> <td>自動減圧系の多重性、独立性に悪影響を与えないよう、区分ごとに自動減圧系作動阻止回路を設置しているため問題ない。</td> </tr> <tr> <td>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。</td> <td>自動減圧系の駆動源である電源の喪失で系の現状維持（フェイル・アズ・イズ）、その他の不利な状況が発生した場合でも、多重性、独立性を持つことで発電用原子炉を十分に安全な状態に導くようになっている。追加する自動減圧系阻止回路はこの安全保護動作を阻害する設計ではない。</td> </tr> </tbody> </table> <p>別紙2-2表 A TWS緩和設備（自動減圧系作動阻止機能）の自動減圧系への影響（2/3）</p> <table border="1" data-bbox="790 1029 1299 1292"> <thead> <tr> <th>設置許可基準規則 第24条（安全保護回路）</th> <th>自動減圧系への影響</th> </tr> </thead> <tbody> <tr> <td>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。</td> <td>A TWS緩和設備（自動減圧系作動阻止機能）はリレーや配線等のアナログ回路で構成されており、不正アクセス行為による影響を受けない。</td> </tr> <tr> <td>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。</td> <td>A TWS緩和設備（自動減圧系作動阻止機能）は平均出力領域モニタの信号を共用しているが、隔離装置（リレー）により分離を図っており、自動減圧系に悪影響を与えない設計としている（別紙2-4図参照）。 なお、原子炉水位信号については、計測制御系統施設と共用していない。</td> </tr> </tbody> </table> <p>別紙2-3表 A TWS緩和設備（自動減圧系作動阻止機能）の自動減圧系への影響（3/3）</p> <table border="1" data-bbox="790 1348 1299 1460"> <thead> <tr> <th>設置許可基準規則 第12条（安全施設）</th> <th>自動減圧系への影響</th> </tr> </thead> <tbody> <tr> <td>4 安全施設は、その健全性及び能力を確認するため、その安全機能の重要度に応じ、発電用原子炉の運転中又は停止中に試験又は検査ができるものでなければならない。</td> <td>A TWS緩和設備（自動減圧系作動阻止機能）の設置により、自動減圧系の試験回路に変更を加えないことから、自動減圧系の試験に影響を与えるものではない。</td> </tr> </tbody> </table>	設置許可基準規則 第24条（安全保護回路）	自動減圧系への影響	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。	A TWS緩和設備（自動減圧系作動阻止機能）は、原子炉停止機能喪失事象時に自動減圧系の作動を阻止するものであり、運転時の異常な過渡変化時には使用しないため問題ない。	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。	A TWS緩和設備（自動減圧系作動阻止機能）の誤動作により、自動減圧系の作動を阻害することのないよう、以下のとおり十分に信頼性のある回路構成としているため問題ない。 自動減圧系の多重性、独立性に悪影響を与えないよう、区分ごとに自動減圧系作動阻止回路を設置する。 単一故障による誤動作の防止のため、「2 out of 3」論理により動作する設計とする。	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。	A TWS緩和設備（自動減圧系作動阻止機能）の誤動作により、自動減圧系の作動を阻害することのないよう、以下のとおり十分に信頼性のある回路構成としているため問題ない。 自動減圧系の多重性、独立性に悪影響を与えないよう、区分ごとに自動減圧系作動阻止回路を設置する。 単一故障による誤動作の防止のため、「2 out of 3」論理により動作する設計とする。	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独立性を確保するものとする。こと。	自動減圧系の多重性、独立性に悪影響を与えないよう、区分ごとに自動減圧系作動阻止回路を設置しているため問題ない。	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。	自動減圧系の駆動源である電源の喪失で系の現状維持（フェイル・アズ・イズ）、その他の不利な状況が発生した場合でも、多重性、独立性を持つことで発電用原子炉を十分に安全な状態に導くようになっている。追加する自動減圧系阻止回路はこの安全保護動作を阻害する設計ではない。	設置許可基準規則 第24条（安全保護回路）	自動減圧系への影響	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。	A TWS緩和設備（自動減圧系作動阻止機能）はリレーや配線等のアナログ回路で構成されており、不正アクセス行為による影響を受けない。	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。	A TWS緩和設備（自動減圧系作動阻止機能）は平均出力領域モニタの信号を共用しているが、隔離装置（リレー）により分離を図っており、自動減圧系に悪影響を与えない設計としている（別紙2-4図参照）。 なお、原子炉水位信号については、計測制御系統施設と共用していない。	設置許可基準規則 第12条（安全施設）	自動減圧系への影響	4 安全施設は、その健全性及び能力を確認するため、その安全機能の重要度に応じ、発電用原子炉の運転中又は停止中に試験又は検査ができるものでなければならない。	A TWS緩和設備（自動減圧系作動阻止機能）の設置により、自動減圧系の試験回路に変更を加えないことから、自動減圧系の試験に影響を与えるものではない。		<p>【女川】 記載内容の相違 （工事実績） ・泊は、該当工事なし。 ・なお、A TWS緩和設備は、建設時（2011年3月以前）に設置済み。</p>
設置許可基準規則 第24条（安全保護回路）	自動減圧系への影響																								
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。	A TWS緩和設備（自動減圧系作動阻止機能）は、原子炉停止機能喪失事象時に自動減圧系の作動を阻止するものであり、運転時の異常な過渡変化時には使用しないため問題ない。																								
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。	A TWS緩和設備（自動減圧系作動阻止機能）の誤動作により、自動減圧系の作動を阻害することのないよう、以下のとおり十分に信頼性のある回路構成としているため問題ない。 自動減圧系の多重性、独立性に悪影響を与えないよう、区分ごとに自動減圧系作動阻止回路を設置する。 単一故障による誤動作の防止のため、「2 out of 3」論理により動作する設計とする。																								
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。	A TWS緩和設備（自動減圧系作動阻止機能）の誤動作により、自動減圧系の作動を阻害することのないよう、以下のとおり十分に信頼性のある回路構成としているため問題ない。 自動減圧系の多重性、独立性に悪影響を与えないよう、区分ごとに自動減圧系作動阻止回路を設置する。 単一故障による誤動作の防止のため、「2 out of 3」論理により動作する設計とする。																								
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独立性を確保するものとする。こと。	自動減圧系の多重性、独立性に悪影響を与えないよう、区分ごとに自動減圧系作動阻止回路を設置しているため問題ない。																								
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。	自動減圧系の駆動源である電源の喪失で系の現状維持（フェイル・アズ・イズ）、その他の不利な状況が発生した場合でも、多重性、独立性を持つことで発電用原子炉を十分に安全な状態に導くようになっている。追加する自動減圧系阻止回路はこの安全保護動作を阻害する設計ではない。																								
設置許可基準規則 第24条（安全保護回路）	自動減圧系への影響																								
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。	A TWS緩和設備（自動減圧系作動阻止機能）はリレーや配線等のアナログ回路で構成されており、不正アクセス行為による影響を受けない。																								
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。	A TWS緩和設備（自動減圧系作動阻止機能）は平均出力領域モニタの信号を共用しているが、隔離装置（リレー）により分離を図っており、自動減圧系に悪影響を与えない設計としている（別紙2-4図参照）。 なお、原子炉水位信号については、計測制御系統施設と共用していない。																								
設置許可基準規則 第12条（安全施設）	自動減圧系への影響																								
4 安全施設は、その健全性及び能力を確認するため、その安全機能の重要度に応じ、発電用原子炉の運転中又は停止中に試験又は検査ができるものでなければならない。	A TWS緩和設備（自動減圧系作動阻止機能）の設置により、自動減圧系の試験回路に変更を加えないことから、自動減圧系の試験に影響を与えるものではない。																								

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

大阪発電所3/4号炉（リファレンスプラント）	女川原子力発電所2号炉	泊発電所3号炉	相違理由						
	 <p>別紙2-1図 安全保護回路の論理に係る改造抽出フロー</p> <p>別紙2-4表 安全保護回路の論理に係る改造</p> <table border="1" data-bbox="739 861 1321 1069"> <thead> <tr> <th>改造概要</th> <th>条文</th> <th>安全保護回路への影響評価</th> </tr> </thead> <tbody> <tr> <td>原子炉停止機能喪失時に自動減圧系及び代替自動減圧回路（代替自動減圧機能）の作動を阻止するATWS緩和設備（自動減圧系作動阻止機能）を追加する。</td> <td>第14条</td> <td>ATWS緩和設備（自動減圧系作動阻止機能）は、自動減圧系回路の関連回路として安全保護回路と同等の設計とする。これらは安全保護回路と同様、計測制御系統施設や他の重大事故等対処設備から物理的、電気的に分離する。さらに、安全保護回路として多重化し、それぞれの区分は互いに物理的、電気的に分離する。</td> </tr> </tbody> </table>	改造概要	条文	安全保護回路への影響評価	原子炉停止機能喪失時に自動減圧系及び代替自動減圧回路（代替自動減圧機能）の作動を阻止するATWS緩和設備（自動減圧系作動阻止機能）を追加する。	第14条	ATWS緩和設備（自動減圧系作動阻止機能）は、自動減圧系回路の関連回路として安全保護回路と同等の設計とする。これらは安全保護回路と同様、計測制御系統施設や他の重大事故等対処設備から物理的、電気的に分離する。さらに、安全保護回路として多重化し、それぞれの区分は互いに物理的、電気的に分離する。	 <p>別紙2-1図 安全保護設備の論理に係る改造抽出フロー</p>	<p>記載内容の相違 （女川実績の反映）</p> <p>【女川】 記載内容の相違 （工事実績） ・泊は、該当工事なし。 ・なお、ATWS緩和設備は、建設時（2011年3月以前）に設置済み。</p>
改造概要	条文	安全保護回路への影響評価							
原子炉停止機能喪失時に自動減圧系及び代替自動減圧回路（代替自動減圧機能）の作動を阻止するATWS緩和設備（自動減圧系作動阻止機能）を追加する。	第14条	ATWS緩和設備（自動減圧系作動阻止機能）は、自動減圧系回路の関連回路として安全保護回路と同等の設計とする。これらは安全保護回路と同様、計測制御系統施設や他の重大事故等対処設備から物理的、電気的に分離する。さらに、安全保護回路として多重化し、それぞれの区分は互いに物理的、電気的に分離する。							

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

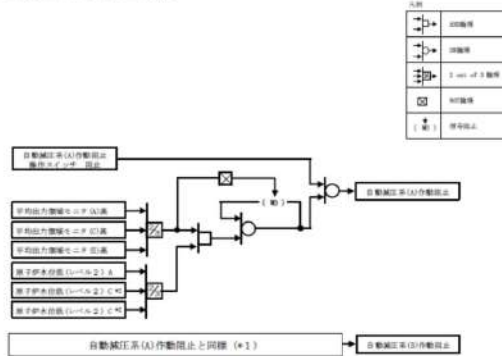
大飯発電所3/4号炉（リファレンスプラント）

女川原子力発電所2号炉

泊発電所3号炉

相違理由

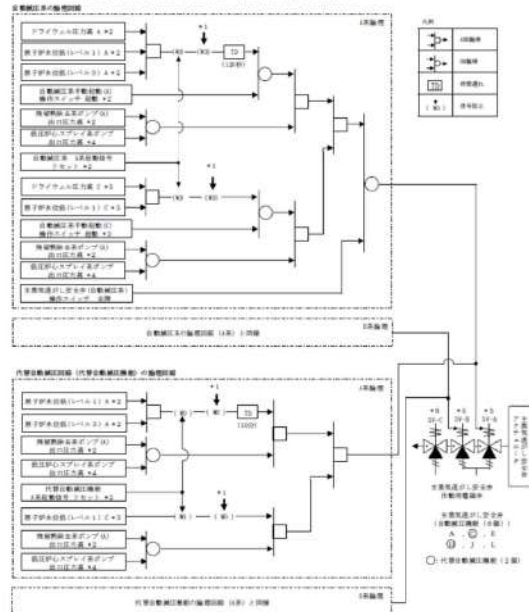
<自動減圧系作動阻止機能>



- *1：自動減圧系(B)作動阻止については、各信号の「A」、「C」、「E」を「B」、「D」、「F」に読み替える。
- *2：「原子炉水位低(レベル2)C」は異なる計測機器からの信号。自動減圧系(B)作動阻止処理においても同じ。

別紙2-2図 ATWS緩和設備（自動減圧系作動阻止機能） 系統概念図(1/2)

<自動減圧系及び代替自動減圧回路（代替自動減圧機能）>

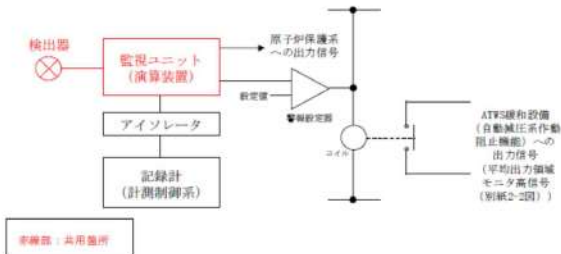


- *1：自動減圧系(A)作動阻止信号（炉出力監視の信号は「A」を「B」に読み替える。）
- *2：炉出力監視の信号は「A」を「B」に読み替える。
- *3：炉出力監視の信号は「C」を「D」に読み替える。
- *4：炉出力監視の信号は「E」を「F」に読み替える。
- *5：自動減圧機能の電源
- *6：別の炉出力監視機能

別紙2-3図 ATWS緩和設備（自動減圧系作動阻止機能） 系統概念図(2/2)

【女川】
 記載内容の相違
 (工事実績)
 ・泊は、建設時
 (2011年3月以前)
 にATWS
 緩和設備を設置済み。

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

大阪発電所3/4号炉（リファレンスプラント）	女川原子力発電所2号炉	泊発電所3号炉	相違理由
	 <p>別紙2-4 図 平均出力領域モニタの信号分離概念図</p> <p>別紙3 安全保護系の過去のトラブル（落雷によるスクラム動作事象等）の反映事項</p> <p>安全保護系に関わる過去のトラブル情報を抽出し、女川2号炉の安全保護系の設計面へ反映すべき事項を下記のとおり抽出した。</p> <p>(1)過去の不具合事例の抽出 安全保護系の設計面に反映が必要となる事象の抽出にあたり、以下を考慮した。 a. 公開情報（原子力施設情報公開ライブラリー「ニューシア」）を対象 b. キーワード検索（安全保護系，原子炉保護系，工学的安全施設作動回路，雷，ノイズ，スクラム等）により抽出 c. 間接的な影響（他設備のトラブル）によって安全保護系へ影響を与えた事象（安全保護系の正動作は除く。）</p> <p>(2)反映が必要となる事象の選定 安全保護系の設計面に反映が必要となる事象について、別紙3-1 図及び別紙3-1 表に基づき抽出した。抽出された過去の不具合事象を別紙3-2 表に示す。</p> <p>(3)過去の不具合事例への対応について 安全保護系の設計面への反映要否について検討を実施した結果、抽出された2件については対応を実施しており、また、その他の不具合事象については反映不要であることを確認した。 なお、今後新知見等が得られれば、設計面への反映を検討していく。</p>	<p>別紙3 安全保護系の過去のトラブル（落雷によるスクラム動作事象等）の反映事項</p> <p>安全保護系に関わる過去のトラブル情報を抽出し、泊3号炉の安全保護設備の設計面へ反映すべき事項を下記のとおり抽出した。</p> <p>(1)過去の不具合事例の抽出 安全保護設備の設計面に反映が必要となる事象の抽出にあたり、以下を考慮した。 a. 公開情報（原子力施設情報公開ライブラリー「ニューシア」）を対象 b. キーワード検索（安全保護系，原子炉保護系，工学的安全施設作動回路，雷，ノイズ，スクラム等）により抽出 c. 間接的な影響（他設備のトラブル）によって安全保護系へ影響を与えた事象（安全保護系の正動作は除く。）</p> <p>(2)反映が必要となる事象の選定 安全保護系の設計面に反映が必要となる事象について、別紙3-1 図及び別紙3-1 表に基づき抽出した結果、泊3号炉の安全保護設備の設計面へ反映すべき事項は抽出されなかった。</p> <p>なお、今後新知見等が得られれば、設計面への反映を検討していく。</p>	<p>【女川】 記載内容の相違 （工事実績） ・泊は、建設時（2011年3月以前）にATWS緩和設備を設置済み。</p> <p>記載内容の相違 （女川実績の反映）</p> <p>【女川】 記載内容の相違 （トラブル反映実績の相違） ・泊は、該当事象なし。</p>

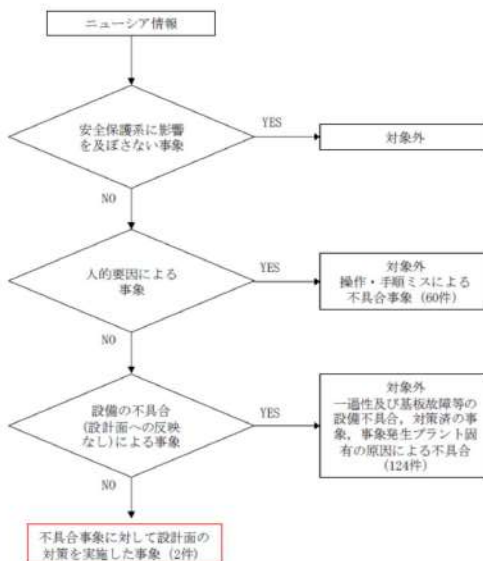
赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

大飯発電所3/4号炉（リファレンスプラント）

女川原子力発電所2号炉

泊発電所3号炉

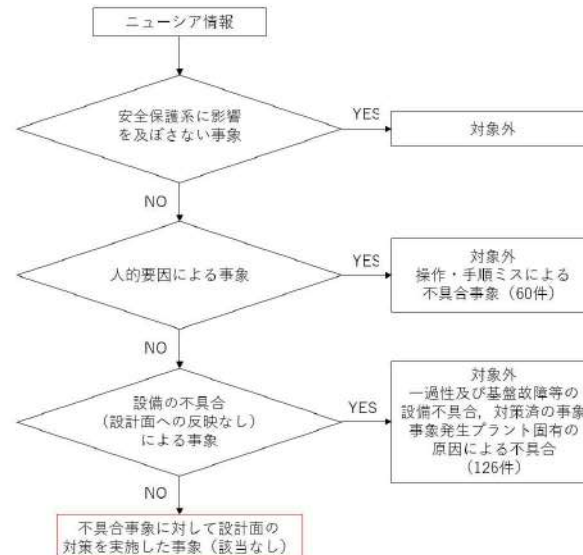
相違理由



別紙3-1図 設計面への反映すべき事項の抽出フロー

別紙3-1表 設計面への反映を不要とする理由

項目	事象例	理由
人的要因による事象	安全処置の実施又は復旧時のミス、作業手順のミス等	作業手順、作業管理等の人的要因によるものであり、設計面へ反映すべき事項ではない。
設備への不具合（設備面への反映なし）による事象	計器・部品の単品故障、一過性故障、偶発故障、既に自社で対策済の事象等	故障した部品の交換等の対策を図ることが基本であること、又は対策済であるため、設計面へ反映すべき事項ではない。
	プラント固有の原因による事象	事象発生プラント固有の原因によるものであり、女川原子力発電所の設計面へ反映すべき事項ではない。



別紙3-1図 設計面への反映すべき事項の抽出フロー

別紙3-1表 設計面への反映を不要とする理由

項目	事象例	理由
人的要因による事象	安全処置の実施又は復旧時のミス、作業手順のミス等	作業手順、作業管理等の人的要因によるものであり、設計面へ反映すべき事項ではない。
設備への不具合（設備面への反映なし）による事象	計器・部品の単品故障、一過性故障、偶発故障、既に自社で対策済の事象等	故障した部品の交換等の対策を図ることが基本であること、又は対策済であるため、設計面へ反映すべき事項ではない。
	プラント固有の原因による事象	事象発生プラント固有の原因によるものであり、泊発電所の設計面へ反映すべき事項ではない。

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

大阪発電所3 / 4号炉 (リファレンスプラント)	女川原子力発電所2号炉	泊発電所3号炉	相違理由																								
	<p style="text-align: center;">別紙3-2表 抽出された過去の不具合事象 (1/2)</p> <table border="1" data-bbox="734 165 1330 480"> <tr> <td>件名</td> <td>女川原子力発電所1号炉中間領域モニタ(I RM)Dチャンネルのバイパスについて</td> </tr> <tr> <td>会社名・プラント名</td> <td>東北電力株式会社 女川原子力発電所1号炉</td> </tr> <tr> <td>発生日</td> <td>平成20年2月14日</td> </tr> <tr> <td>事象概要</td> <td>女川原子力発電所1号炉は、平成20年2月14日1時00分に発電機を解列し、第18回定期検査を開始した。その後、原子炉停止操作を継続していたところ、原子炉内の中性子の量を測定する中間領域モニタ(I RM)Dチャンネル(A～Dチャンネルのうちの1つ)の指示値が測定レンジ7から下がらない事象が発生した。このため、同3時20分に保安規定第27条の運転上の制限を満足しないと判断した。I RMは6チャンネルを有しており、最大で2チャンネルをバイパスできる設計となっていることから、同3時34分に当該チャンネルをバイパスし、保安規定第27条の運転上の制限内に復帰した。当該チャンネルをバイパスしても、他の5チャンネルで原子炉内の中性子量の監視は可能であることから、引き続き原子炉の停止操作を継続し、同日5時36分に原子炉を停止した。</td> </tr> <tr> <td>原因</td> <td>当該チャンネルのI RMを点検した結果、異常が確認されなかった。</td> </tr> <tr> <td>対策</td> <td>当該チャンネルの動作不良の原因は、ノイズの影響によるものと推定した。 ノイズが影響すると考えられる箇所のケーブル・ルートを変更した。</td> </tr> </table> <p style="text-align: center;">別紙3-2表 抽出された過去の不具合事象 (2/2)</p> <table border="1" data-bbox="734 520 1330 1106"> <tr> <td>件名</td> <td>女川原子力発電所1号炉I RM及びS RMの保安規定に定める運転上の制限を満足しない事象について</td> </tr> <tr> <td>会社名・プラント名</td> <td>東北電力株式会社 女川原子力発電所1号炉</td> </tr> <tr> <td>発生日</td> <td>平成22年2月23日</td> </tr> <tr> <td>事象概要</td> <td> <ul style="list-style-type: none"> ・発電停止後の原子炉停止操作過程において、原子炉内の中性子の量を監視している4個(A～Dチャンネル)ある中性子源領域モニタ(以下、「S RM」という。)の1個(Bチャンネル)が他チャンネルと比べて高い指示値を示すという動作不良が発生し、また、I RMの指示値がレンジ7(5%)より下がらない事象が継続していたことから、原子炉施設保安規定に定める運転上の制限を満足していないと判断した(2月23日)。(なお、他のI RMチャンネルについては異常なくレンジ1まで低下している。) ・S RMは1個をバイパスできる設計となっていることから、当該チャンネルをバイパスし、原子炉施設保安規定に定める運転上の制限内に復帰した(2月23日)。 ・当該チャンネルをバイパスしても他の3個で原子炉内の中性子量の監視は可能であることから、引き続き原子炉停止操作を継続し、原子炉を停止した(2月23日)。 ・ノイズの影響調査を実施した。 </td> </tr> <tr> <td>原因</td> <td>原因調査の結果、ノイズの影響を受けていることが確認されたが流入経路の特定には至らなかった。</td> </tr> <tr> <td>対策</td> <td> <ol style="list-style-type: none"> 1. S RMについて、指示値に影響を及ぼさない値まで監視ユニットにてディスクリ調整を行い、指示降下・安定したことを確認した。また、ケーブル・コネクタ等の健全性の確認及び外来ノイズ低減として以下の対策を実施した。 <ul style="list-style-type: none"> ○ペネトレーション内ケーブル整理 ○電線管アースボンドの取付け ○ディスクリ設定の見直し ○ケーブルBOXへのクッション設置 2. I RMについて、放電作業を実施し、指示値がレンジ7からレンジ1まで低下したことを確認した。また、ケーブル・コネクタ等の健全性の確認及び外来ノイズ低減対策を実施した。 <ul style="list-style-type: none"> ○ペネトレーション内ケーブル整理 ○電線管アースボンドの取付け ○ジッパーチューブの布設 ○ケーブルBOXへのクッション設置 </td> </tr> </table>	件名	女川原子力発電所1号炉中間領域モニタ(I RM)Dチャンネルのバイパスについて	会社名・プラント名	東北電力株式会社 女川原子力発電所1号炉	発生日	平成20年2月14日	事象概要	女川原子力発電所1号炉は、平成20年2月14日1時00分に発電機を解列し、第18回定期検査を開始した。その後、原子炉停止操作を継続していたところ、原子炉内の中性子の量を測定する中間領域モニタ(I RM)Dチャンネル(A～Dチャンネルのうちの1つ)の指示値が測定レンジ7から下がらない事象が発生した。このため、同3時20分に保安規定第27条の運転上の制限を満足しないと判断した。I RMは6チャンネルを有しており、最大で2チャンネルをバイパスできる設計となっていることから、同3時34分に当該チャンネルをバイパスし、保安規定第27条の運転上の制限内に復帰した。当該チャンネルをバイパスしても、他の5チャンネルで原子炉内の中性子量の監視は可能であることから、引き続き原子炉の停止操作を継続し、同日5時36分に原子炉を停止した。	原因	当該チャンネルのI RMを点検した結果、異常が確認されなかった。	対策	当該チャンネルの動作不良の原因は、ノイズの影響によるものと推定した。 ノイズが影響すると考えられる箇所のケーブル・ルートを変更した。	件名	女川原子力発電所1号炉I RM及びS RMの保安規定に定める運転上の制限を満足しない事象について	会社名・プラント名	東北電力株式会社 女川原子力発電所1号炉	発生日	平成22年2月23日	事象概要	<ul style="list-style-type: none"> ・発電停止後の原子炉停止操作過程において、原子炉内の中性子の量を監視している4個(A～Dチャンネル)ある中性子源領域モニタ(以下、「S RM」という。)の1個(Bチャンネル)が他チャンネルと比べて高い指示値を示すという動作不良が発生し、また、I RMの指示値がレンジ7(5%)より下がらない事象が継続していたことから、原子炉施設保安規定に定める運転上の制限を満足していないと判断した(2月23日)。(なお、他のI RMチャンネルについては異常なくレンジ1まで低下している。) ・S RMは1個をバイパスできる設計となっていることから、当該チャンネルをバイパスし、原子炉施設保安規定に定める運転上の制限内に復帰した(2月23日)。 ・当該チャンネルをバイパスしても他の3個で原子炉内の中性子量の監視は可能であることから、引き続き原子炉停止操作を継続し、原子炉を停止した(2月23日)。 ・ノイズの影響調査を実施した。 	原因	原因調査の結果、ノイズの影響を受けていることが確認されたが流入経路の特定には至らなかった。	対策	<ol style="list-style-type: none"> 1. S RMについて、指示値に影響を及ぼさない値まで監視ユニットにてディスクリ調整を行い、指示降下・安定したことを確認した。また、ケーブル・コネクタ等の健全性の確認及び外来ノイズ低減として以下の対策を実施した。 <ul style="list-style-type: none"> ○ペネトレーション内ケーブル整理 ○電線管アースボンドの取付け ○ディスクリ設定の見直し ○ケーブルBOXへのクッション設置 2. I RMについて、放電作業を実施し、指示値がレンジ7からレンジ1まで低下したことを確認した。また、ケーブル・コネクタ等の健全性の確認及び外来ノイズ低減対策を実施した。 <ul style="list-style-type: none"> ○ペネトレーション内ケーブル整理 ○電線管アースボンドの取付け ○ジッパーチューブの布設 ○ケーブルBOXへのクッション設置 		<p>【女川】 記載内容の相違 (トラブル反映実績の相違) ・泊は、該当事象なし。</p>
件名	女川原子力発電所1号炉中間領域モニタ(I RM)Dチャンネルのバイパスについて																										
会社名・プラント名	東北電力株式会社 女川原子力発電所1号炉																										
発生日	平成20年2月14日																										
事象概要	女川原子力発電所1号炉は、平成20年2月14日1時00分に発電機を解列し、第18回定期検査を開始した。その後、原子炉停止操作を継続していたところ、原子炉内の中性子の量を測定する中間領域モニタ(I RM)Dチャンネル(A～Dチャンネルのうちの1つ)の指示値が測定レンジ7から下がらない事象が発生した。このため、同3時20分に保安規定第27条の運転上の制限を満足しないと判断した。I RMは6チャンネルを有しており、最大で2チャンネルをバイパスできる設計となっていることから、同3時34分に当該チャンネルをバイパスし、保安規定第27条の運転上の制限内に復帰した。当該チャンネルをバイパスしても、他の5チャンネルで原子炉内の中性子量の監視は可能であることから、引き続き原子炉の停止操作を継続し、同日5時36分に原子炉を停止した。																										
原因	当該チャンネルのI RMを点検した結果、異常が確認されなかった。																										
対策	当該チャンネルの動作不良の原因は、ノイズの影響によるものと推定した。 ノイズが影響すると考えられる箇所のケーブル・ルートを変更した。																										
件名	女川原子力発電所1号炉I RM及びS RMの保安規定に定める運転上の制限を満足しない事象について																										
会社名・プラント名	東北電力株式会社 女川原子力発電所1号炉																										
発生日	平成22年2月23日																										
事象概要	<ul style="list-style-type: none"> ・発電停止後の原子炉停止操作過程において、原子炉内の中性子の量を監視している4個(A～Dチャンネル)ある中性子源領域モニタ(以下、「S RM」という。)の1個(Bチャンネル)が他チャンネルと比べて高い指示値を示すという動作不良が発生し、また、I RMの指示値がレンジ7(5%)より下がらない事象が継続していたことから、原子炉施設保安規定に定める運転上の制限を満足していないと判断した(2月23日)。(なお、他のI RMチャンネルについては異常なくレンジ1まで低下している。) ・S RMは1個をバイパスできる設計となっていることから、当該チャンネルをバイパスし、原子炉施設保安規定に定める運転上の制限内に復帰した(2月23日)。 ・当該チャンネルをバイパスしても他の3個で原子炉内の中性子量の監視は可能であることから、引き続き原子炉停止操作を継続し、原子炉を停止した(2月23日)。 ・ノイズの影響調査を実施した。 																										
原因	原因調査の結果、ノイズの影響を受けていることが確認されたが流入経路の特定には至らなかった。																										
対策	<ol style="list-style-type: none"> 1. S RMについて、指示値に影響を及ぼさない値まで監視ユニットにてディスクリ調整を行い、指示降下・安定したことを確認した。また、ケーブル・コネクタ等の健全性の確認及び外来ノイズ低減として以下の対策を実施した。 <ul style="list-style-type: none"> ○ペネトレーション内ケーブル整理 ○電線管アースボンドの取付け ○ディスクリ設定の見直し ○ケーブルBOXへのクッション設置 2. I RMについて、放電作業を実施し、指示値がレンジ7からレンジ1まで低下したことを確認した。また、ケーブル・コネクタ等の健全性の確認及び外来ノイズ低減対策を実施した。 <ul style="list-style-type: none"> ○ペネトレーション内ケーブル整理 ○電線管アースボンドの取付け ○ジッパーチューブの布設 ○ケーブルBOXへのクッション設置 																										

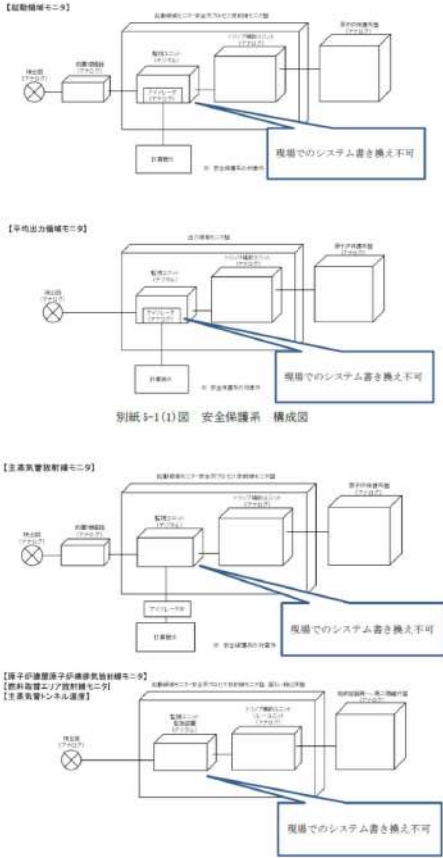
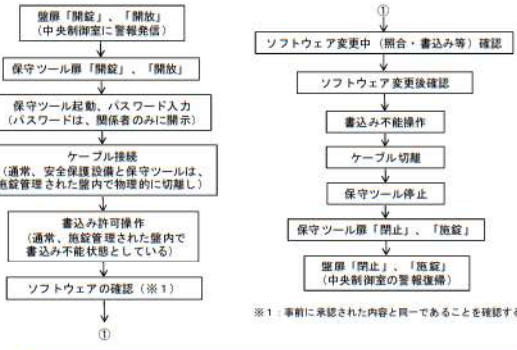
泊発電所3号炉 DB基準適合性 比較表

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

第24条 安全保護回路

大阪発電所3/4号炉（リファレンスプラント）	女川原子力発電所2号炉	泊発電所3号炉	相違理由
<p>大阪発電所3/4号炉（リファレンスプラント）</p> <p>参考1</p> <p>安全保護系の過去のトラブル（落雷によるスクラム動作事象等）の反映事項において、柏崎の落雷事象を反映不要とした理由</p> <p>柏崎刈羽原子力発電所6号機で発生した落雷によるスクラム事象は、原子炉建屋外壁埋設となっていた信号ケーブルに雷サージ電流が侵入したことが原因と考えられる。</p> <p>女川原子力発電所2号炉における安全保護回路のケーブルは、建屋内に集約されており、原子炉建屋外壁埋設となっていないため、上記事象はプラント固有の原因と判断し、設計面へ反映が必要となる事象の抽出フロー（別紙3-1図）により反映不要としている。</p> <p>なお、安全保護回路を含む重要安全施設に対する落雷影響については、6条「外部からの衝撃による損傷の防止」（別添資料1「補足資料14 落雷影響評価について」）において評価し、機能が損なわれないことを確認している。</p> <p>別紙4 現場据付以降の作業時における、インサイダー等に対するセキュリティ対策</p> <p>安全保護回路について、検出器から論理回路入口までの構成機器のうちデジタル演算処理を行う機器は、起動領域モニタ（SRNM）、平均出力領域モニタ（APRM）、プロセス放射線モニタリング設備（PrRM）及び主蒸気管トンネル温度の監視装置である。これらについては以下の対策を実施する。</p> <p>(I)作業管理</p> <p>a. デジタル処理を行っている機器により警報設定値の変更作業実施の際には、中央制御室にて発電課長の許可を得て、運転責任者の管理する鍵を借用する必要がある。</p> <p>b. 安全保護回路の点検作業は、当社が承認した作業要領書に基づき行う。また、デジタル処理を行っている機器は不正に取り外した場合には信号が異常となり警報が発生する。</p> <p>c. 当社が承認した作業要領書にて作業を実施しており、作業後に当社が設定値に異常がないこと及び回路が正常に動作することを確認している。</p>	<p>女川原子力発電所2号炉</p> <p>参考1</p> <p>安全保護系の過去のトラブル（落雷によるスクラム動作事象等）の反映事項において、柏崎の落雷事象を反映不要とした理由</p> <p>柏崎刈羽原子力発電所6号機で発生した落雷によるスクラム事象は、原子炉建屋外壁埋設となっていた信号ケーブルに雷サージ電流が侵入したことが原因と考えられる。</p> <p>泊発電所3号炉における安全保護系のケーブルは、建屋内に集約されており、原子炉建屋外壁埋設となっていないため、上記事象はプラント固有の原因と判断し、設計面へ反映が必要となる事象の抽出フロー（別紙3-1図）により反映不要としている。</p> <p>なお、安全保護系を含む重要安全施設に対する落雷影響については、6条「外部からの衝撃による損傷の防止」（別添資料1「補足資料14 落雷影響評価について」）において評価し、機能が損なわれないことを確認している。</p> <p>別紙4 現場据付以降の作業時における、インサイダー等に対するセキュリティ対策</p> <p>安全保護設備について、以下の対策を実施する。</p> <p>(I)作業管理</p> <p>a. 安全保護設備に係る現場作業実施の際には、中央制御室にて発電課長（当直）の許可を得て、運転責任者の管理する鍵を借用する必要がある。</p> <p>b. 安全保護設備の点検作業は、当社が承認した作業要領書に基づき行う。また、安全保護設備を構成する機器は不正に取り外した場合には警報が発生する。</p> <p>c. 当社が承認した作業要領書にて作業を実施しており、作業後に当社が承認されていない変更がないことを確認している。</p>	<p>泊発電所3号炉</p> <p>参考1</p> <p>安全保護系の過去のトラブル（落雷によるスクラム動作事象等）の反映事項において、柏崎の落雷事象を反映不要とした理由</p> <p>柏崎刈羽原子力発電所6号機で発生した落雷によるスクラム事象は、原子炉建屋外壁埋設となっていた信号ケーブルに雷サージ電流が侵入したことが原因と考えられる。</p> <p>泊発電所3号炉における安全保護系のケーブルは、建屋内に集約されており、原子炉建屋外壁埋設となっていないため、上記事象はプラント固有の原因と判断し、設計面へ反映が必要となる事象の抽出フロー（別紙3-1図）により反映不要としている。</p> <p>なお、安全保護系を含む重要安全施設に対する落雷影響については、6条「外部からの衝撃による損傷の防止」（別添資料1「補足資料14 落雷影響評価について」）において評価し、機能が損なわれないことを確認している。</p> <p>別紙4 現場据付以降の作業時における、インサイダー等に対するセキュリティ対策</p> <p>安全保護設備について、以下の対策を実施する。</p> <p>(I)作業管理</p> <p>a. 安全保護設備に係る現場作業実施の際には、中央制御室にて発電課長（当直）の許可を得て、運転責任者の管理する鍵を借用する必要がある。</p> <p>b. 安全保護設備の点検作業は、当社が承認した作業要領書に基づき行う。また、安全保護設備を構成する機器は不正に取り外した場合には警報が発生する。</p> <p>c. 当社が承認した作業要領書にて作業を実施しており、作業後に当社が承認されていない変更がないことを確認している。</p>	<p>相違理由</p> <p>記載内容の相違（女川実績の反映）</p> <p>記載内容の相違（女川実績の反映）</p> <p>【女川】記載の相違（デジタル計算機）</p>

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

大飯発電所3/4号炉（リファレンスプラント）	女川原子力発電所2号炉	泊発電所3号炉	相違理由
	<p>別紙5 安全保護回路のうちデジタル処理部のある機器のシステムへ接続可能なアクセスについて</p> <p>安全保護回路の構成機器のうちデジタル処理部のある機器としては、起動領域モニタ（SRNM）、平均出力領域モニタ（APRM）、プロセス放射線モニタリング設備（PRRM）及び主蒸気管トンネル温度の監視装置がある。</p> <p>これらのデジタル処理部のある機器は、測定対象に応じた演算処理を行う専用のデジタル処理部であり、不要な機能は有しておらず、汎用のソフトウェアやハードウェアを使用していない。また、保守ツール等のシステムへ接続可能な機器の接続箇所はなく、現場でのシステムの書き換えができない構造となっているため、外部ネットワークからの接続や電気的アクセスはできない。</p>  <p>別紙5-1(1)図 安全保護系 構成図</p> <p>別紙5-1(2)図 安全保護系 構成図</p>	<p>別紙5 安全保護設備のシステムへ接続可能なアクセスについて</p> <p>安全保護設備は、専用のデジタル計算機であり、不要な機能は有しておらず、汎用のソフトウェアやハードウェアを使用していない。また、保守ツールの接続箇所は、施錠管理された盤内で常時物理的に切り離しており、ソフトウェア変更は以下の手順（別紙5-1図）で実施することで、管理されないソフトウェアの変更を防止している。</p>  <p>別紙5-1図 安全保護設備に係るソフトウェア変更手順</p>	<p>記載内容の相違（女川実績の反映）</p> <p>【女川】</p> <p>記載の相違（デジタル計算機）</p>

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

第24条 安全保護回路

大阪発電所3/4号炉（リファレンスプラント）

女川原子力発電所2号炉

泊発電所3号炉

相違理由

別紙6 安全保護系のセキュリティ対策に関する当社及び受注者の対応について

安全保護系のセキュリティ対策における実効性の担保に当たっては、機器の設計・製作については、当社の設計管理プロセスにより受注者の実施内容を管理している。また、機器への物理的アクセス（出入管理・鍵管理）については、当社が定めた社内手順に従い管理している。

別紙6-1表 安全保護回路のセキュリティ対策に関する当社及び受注者の対応 (1/3)

対策	当社の実施内容	受注者側の実施内容
1. 物理的及び電気的アクセスの制限対策【2.1(1)、2.2】	発電所の出入管理 ・保守フェールの接続口を設計上閉鎖可能な状態の不正行為が実施できない設計 ・保安保護系の信号は防振装置、遮断機、保守フェールの接続口を設計上閉鎖可能な状態とし、外部からの侵入を受け付けない設計	左記手順に従い実施 当社が提示する調達要求仕様に従い機器の設計管理を実施中
2. ハードウェアの物理的・機能的分離【2.1(2)、2.4、2.7、2.9】	保護回路への物理的・機能的分離 ・一方のみ（安全保護回路から見て）、外部からの侵入を受け付けない設計	左記手順に従い実施 当社が提示する調達要求仕様に従い機器の設計管理を実施中
3. 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防止対策【2.1(3)、2.3】	保護回路への物理的・機能的分離 ・一方のみ（安全保護回路から見て）、外部からの侵入を受け付けない設計	左記手順に従い実施 当社が提示する調達要求仕様に従い機器の設計管理を実施中

機器の内部は防護上の観点から公開できません。

別紙6-1表 安全保護回路のセキュリティ対策に関する当社及び受注者の対応 (2/3)

対策	当社の実施内容	受注者側の実施内容
4. システムの導入試験、更新プログラム等の接続口を設計上閉鎖可能な状態とし、外部からの侵入を受け付けない設計【2.1(4)、2.4(3)、2.5】	更新プログラムの導入試験、更新プログラム等の接続口を設計上閉鎖可能な状態とし、外部からの侵入を受け付けない設計	当社が提示する調達要求仕様に従い機器の設計管理を実施中
5. 保守フェール・サービス対策【2.1(5)】	保守フェールの接続口を設計上閉鎖可能な状態とし、外部からの侵入を受け付けない設計	当社が提示する調達要求仕様に従い機器の設計管理を実施中
6. 安全保護回路の設計【2.3、別紙1】	発電所の出入管理 ・保守フェールの接続口を設計上閉鎖可能な状態とし、外部からの侵入を受け付けない設計	左記手順に従い実施 当社が提示する調達要求仕様に従い機器の設計管理を実施中

別紙6-1表 安全保護回路のセキュリティ対策に関する当社及び受注者の対応 (3/3)

対策	当社の実施内容	受注者側の実施内容
7. 想定脅威に対する対策【2.6、別紙4】	(1) 工務製作・出荷段階 ・外部脅威に対する対策（外部からの侵入） ・内部脅威に対する対策（不正ソフトウェア、改ざん、不正アクセス等） ・人的要因（知識不足による情報漏えい等） ・物理的アクセスの制限 ・物理的アクセス時の鍵管理 ・作業準備書に基づく点検	機器の設計管理プロセス等により受注者の実施内容を管理 左記手順に従い実施 当社が提示する調達要求仕様に従い機器の設計管理を実施中
8. 物理的分離・電気的分離【2.7】	保護回路への物理的・機能的分離 ・一方のみ（安全保護回路から見て）、外部からの侵入を受け付けない設計	左記手順に従い実施 当社が提示する調達要求仕様に従い機器の設計管理を実施中

- ※1 受注者とは、安全保護回路に関する設計、工事を受注する者を指す。
- ※2 事業者の設計管理
機器の設計・製作に当たっては、以下により管理するプロセスを構築している。
①業務の計画段階～発注の発案、設計・開発に必要な要求事項を明確化。

機器の内部は防護上の観点から公開できません。

別紙6 安全保護設備のセキュリティ対策に関する当社及び受注者の対応について

安全保護設備のセキュリティ対策における実効性の担保に当たっては、機器の設計・製作については、当社の設計管理プロセスにより受注者の実施内容を管理している。また、機器への物理的アクセス（出入管理・鍵管理）については、当社が定めた社内手順に従い管理している。

別紙6-1表 安全保護設備のセキュリティ対策に関する当社及び受注者の対応 (1/3)

対策	当社の実施内容	受注者側の実施内容
1. 物理的及び電気的アクセスの制限対策【2.1(1)、2.3、2.7、2.9】	発電所の出入管理 ・保守フェールの接続口を設計上閉鎖可能な状態の不正行為が実施できない設計 ・保安保護系の信号は防振装置、遮断機、保守フェールの接続口を設計上閉鎖可能な状態とし、外部からの侵入を受け付けない設計	左記手順に従い実施 当社が提示する調達要求仕様に従い機器の設計管理を実施中
2. ハードウェアの物理的・機能的分離【2.1(2)、2.4、2.7、2.9】	保護回路への物理的・機能的分離 ・一方のみ（安全保護回路から見て）、外部からの侵入を受け付けない設計	左記手順に従い実施 当社が提示する調達要求仕様に従い機器の設計管理を実施中
3. 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防止対策【2.1(3)、2.4、2.7、2.9】	保護回路への物理的・機能的分離 ・一方のみ（安全保護回路から見て）、外部からの侵入を受け付けない設計	左記手順に従い実施 当社が提示する調達要求仕様に従い機器の設計管理を実施中

別紙6-1表 安全保護設備のセキュリティ対策に関する当社及び受注者の対応 (2/3)

対策	当社の実施内容	受注者側の実施内容
4. システムの導入試験、更新プログラム等の接続口を設計上閉鎖可能な状態とし、外部からの侵入を受け付けない設計【2.1(4)、2.4(3)、2.5、2.6、2.7、2.9、別紙5、6】	更新プログラムの導入試験、更新プログラム等の接続口を設計上閉鎖可能な状態とし、外部からの侵入を受け付けない設計	当社が提示する調達要求仕様に従い機器の設計管理を実施中
5. 保守フェール・サービス対策【2.1(5)、2.10】	保守フェールの接続口を設計上閉鎖可能な状態とし、外部からの侵入を受け付けない設計	当社が提示する調達要求仕様に従い機器の設計管理を実施中
6. 安全保護回路の設計【2.6、別紙1】	発電所の出入管理 ・保守フェールの接続口を設計上閉鎖可能な状態とし、外部からの侵入を受け付けない設計	左記手順に従い実施 当社が提示する調達要求仕様に従い機器の設計管理を実施中

別紙6-1表 安全保護設備のセキュリティ対策に関する当社及び受注者の対応 (3/3)

対策	当社の実施内容	受注者側の実施内容
7. 想定脅威に対する対策【2.6、別紙4】	(1) 工務製作・出荷段階 ・外部脅威に対する対策（外部からの侵入） ・内部脅威に対する対策（不正ソフトウェア、改ざん、不正アクセス等） ・人的要因（知識不足による情報漏えい等） ・物理的アクセスの制限 ・物理的アクセス時の鍵管理 ・作業準備書に基づく点検	機器の設計管理プロセス等により受注者の実施内容を管理 左記手順に従い実施 当社が提示する調達要求仕様に従い機器の設計管理を実施中
8. 物理的分離・電気的分離【2.7】	保護回路への物理的・機能的分離 ・一方のみ（安全保護回路から見て）、外部からの侵入を受け付けない設計	左記手順に従い実施 当社が提示する調達要求仕様に従い機器の設計管理を実施中

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

第24条 安全保護回路

大阪発電所3/4号炉（リファレンスプラント）	女川原子力発電所2号炉	泊発電所3号炉	相違理由
<p>大飯発電所3/4号炉（リファレンスプラント）</p> <p>別紙7 安全保護回路のうちデジタル部分について、システム設計と実際のデバイスが具備している機能との差（未使用機能等）による影響の有無</p> <p>システム設計に基づき、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、安全保護回路のうち、デジタル演算処理を行う機器は、工場出荷前試験及び導入時における試験を実施することにより、要求される機能を満足することの確認及び未使用機能等による悪影響がないことの確認が供給者によって確実に実施されていることを確認している。</p> <p>別紙8 安全保護回路のうち一部デジタル演算処理を行う機器の検証及び妥当性確認について</p> <p>安全保護回路のうち、一部デジタル演算処理を行う機器のソフトウェア又はハードウェア回路は、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、変更管理の各段階で「安全保護系へのデジタル計算機の適用に関する規程」（JEAC4620-2008）及び「デジタル安全保護系の検証及び妥当性確認に関する指針」（JEG4609-2008（以下「JEG4609」という。））に準じた検証及び妥当性確認を実施する。</p> <p>女川2号炉においては、起動領域モニタ（SRNM）、平均出力領域モニタ（APRM）、プロセス放射線モニタリング設備（PRRM）においてハードウェア回路を用いており、主蒸気管トンネル温度にはソフトウェアを用いている。</p> <p>以下にこれらソフトウェア及びハードウェア回路の検証及び妥当性確認の概要を示す。</p> <p>これらの機器に用いるソフトウェアはJEG4609に基づき、また、ハードウェア回路はJEG4609を準用して、検証及び妥当性確認を実施している（別紙8-1図）。</p> <p>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。</p> <p>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。</p> <p>b. システム設計要求仕様がハードウェア、ソフトウェア又はハードウェア回路の設計要求仕様に正しく反映されていること。</p>	<p>①設計・開発段階一連の事項にたい設計を行い、その内容が要求事項に準じて妥当であることを検証。 ②調達段階一設計内容を調達仕様と明確化し受注者に発注、調達要求により受注者が提出する設備図書・工事要領書を確認・承認。また、試験結果を確認し、調達要求どおり製作されたことを確認。</p> <p>※2 受注者の設計管理 当社が指定する調達仕様に従い、設計・製作を行う。設計・製作に当たっては、設備図書、工事要領書を作成し、当社の承認を受ける。また、試験により調達仕様どおり製作されたことを確認し、その結果を当社に報告書として提出。</p> <p>別紙7 安全保護設備について、システム設計と実際のデバイスが具備している機能との差（未使用機能等）による影響の有無</p> <p>システム設計に基づき、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、安全保護設備は、工場出荷前試験及び導入時における試験を実施することにより、要求される機能を満足することの確認及び未使用機能等による悪影響がないことの確認が供給者によって確実に実施されていることを確認している。</p> <p>別紙8 安全保護設備の検証及び妥当性確認について</p> <p>安全保護設備のソフトウェアは、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、変更管理の各段階で「安全保護系へのデジタル計算機の適用に関する規程」（JEAC4620-2008）及び「デジタル安全保護系の検証及び妥当性確認に関する指針」（JEG4609-2008（以下「JEG4609」という。））に準じた検証及び妥当性確認を実施する。</p> <p>以下にこれらソフトウェアの検証及び妥当性確認の概要を示す。（別紙8-1図）。</p> <p>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。</p> <p>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。</p> <p>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。</p>	<p>※1 受注者とは、安全保護設備に関する設計、工事を受注する者を指す。 ※2 事業者の設計管理 機種の設計・製作に当たっては、以下により管理するプロセスを構築している。 ①業務の計画段階一業務の実施、設計・開発に必要な要求事項を明確化。 ②設計・開発段階一要求事項にたい設計を行い、その内容が要求事項に対して妥当であることを検証。 ③調達段階一設計内容を調達仕様と明確化し受注者に発注、調達要求により受注者が提出する設備図書・工事要領書を確認・承認。また、試験結果を確認し、調達要求どおり製作されたことを確認。</p> <p>※3 受注者の設計管理 当社が指定する調達仕様に従い、設計・製作を行う。設計・製作に当たっては、設備図書、工事要領書を作成し、当社の承認を受ける。また、並より調達仕様どおり製作されたことを確認し、その結果を当社に報告書として提出。</p> <p>別紙7 安全保護設備について、システム設計と実際のデバイスが具備している機能との差（未使用機能等）による影響の有無</p> <p>別紙8 安全保護設備の検証及び妥当性確認について</p> <p>安全保護設備のソフトウェアは、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、変更管理の各段階で「安全保護系へのデジタル計算機の適用に関する規程」（JEAC4620-2008）及び「デジタル安全保護系の検証及び妥当性確認に関する指針」（JEG4609-2008（以下「JEG4609」という。））に準じた検証及び妥当性確認を実施する。</p> <p>以下にこれらソフトウェアの検証及び妥当性確認の概要を示す。（別紙8-1図）。</p> <p>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。</p> <p>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。</p> <p>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。</p>	<p>相違理由</p> <p>記載内容の相違（女川実績の反映）</p> <p>記載内容の相違（女川実績の反映）</p> <p>【女川】 記載の相違（ハードウェア回路）</p>

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

大飯発電所3/4号炉（リファレンスプラント）	女川原子力発電所2号炉	泊発電所3号炉	相違理由
	<p>c. 上記設計要求仕様に基づいてソフトウェア又はハードウェア回路が製作されていること。</p> <p>d. 検証及び妥当性確認が可能なソフトウェア又はハードウェア回路となっていること。必要な検証を経て製作されたソフトウェア又はハードウェア回路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を確認するために妥当性確認を行う。</p> <p>注：ハードウェア回路の検証に当たっては、「ソフトウェア」の部分に「ハードウェア」に置き換えて、検証及び妥当性確認を実施する。</p> <p>別紙8-1 図 検証及び妥当性確認</p>	<p>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。</p> <p>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を確認するために妥当性確認を行う。</p> <p>別紙8-1 図 安全保護設備の検証及び妥当性確認</p>	

泊発電所3号炉 DB基準適合性 比較表

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

第24条 安全保護回路（別添）

大飯発電所3/4号炉（リファレンスプラント）	女川原子力発電所2号炉	泊発電所3号炉	相違理由
<p style="text-align: right;">別添</p> <p style="text-align: center;">大飯3号炉及び4号炉 技術的能力説明資料 安全保護回路</p>	<p style="text-align: right;">別添</p> <p style="text-align: center;">女川原子力発電所2号炉 運用、手順説明資料 安全保護回路</p>	<p style="text-align: right;">別添</p> <p style="text-align: center;">泊発電所3号炉 技術的能力説明資料 安全保護回路</p>	

大飯発電所3/4号炉 (リファレンスプラント)	女川原子力発電所2号炉	泊発電所3号炉	相違理由
<p>2.4条 安全保護回路</p> <p>設置許可基準 第6号 不正アクセスその他の電子計算機に使用目的に反する動作をさせず、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。</p> <p>【解説】 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反する動作をさせず、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、機能的分離に相当し、システムへの導入段階、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。</p> <p>【後段規制との対応】 工：工認 (基本設計方針、添付書類) 保：保安規定 (運用、手順に係る事項、下位文書含む) 緑：核物質防護規定 (下位文書含む)</p> <p>【添付六、八への反映事項】 〇：添付六、八に反映 □：当該条文に該当しない (他条文での反映事項他)</p>	<p>第24条 安全保護回路</p> <p>設置許可基準 第24条 第1項第6号 不正アクセス行為その他の電子計算機に使用目的に反する動作をさせず、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。</p> <p>【解説】 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反する動作をさせず、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。</p> <p>【後段規制との対応】 工：工認 (基本設計方針、添付書類) 保：保安規定 (運用、手順に係る事項、下位文書含む) 緑：核物質防護規定 (下位文書含む)</p> <p>【添付六、八への反映事項】 〇：添付六、八に反映 □：当該条文に該当しない (他条文での反映事項他)</p>	<p>第2.4条 安全保護回路</p> <p>【追加重要事項】 第二十四条 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。</p> <ol style="list-style-type: none"> 運転時の異常な運転状態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の系統と併せて検察することにより、燃料要素の許容損傷限界を越えないようにできるものとする。 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。 安全保護回路を構成する機械若しくは装置又はチャンネルは、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。 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。 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、発電用原子炉施設より安全な状態に移行するが、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のない状態を維持できるものとする。 不正アクセス行為その他の電子計算機に使用目的に反する動作をさせず、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。 計測制御系統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。 <p>承認されていない動作や変更を防ぐことができること。</p> <p>〇：運用による対応 □：設備による対応</p>	<p>相違理由</p>

赤字：設備、運用又は体制の相違（設計方針の相違）
 青字：記載箇所又は記載内容の相違（記載方針の相違）
 緑字：記載表現、設備名称の相違（実質的な相違なし）

第24条 安全保護回路（別添）

大飯発電所3/4号炉（リファレンスプラント）	女川原子力発電所2号炉	泊発電所3号炉	相違理由																																																																																																	
<p>設計基準に係る運用対策等（設計基準）</p> <table border="1"> <thead> <tr> <th>設置許可基準対象条文</th> <th>対象項目</th> <th>区分</th> <th>運用対策等</th> </tr> </thead> <tbody> <tr> <td rowspan="10">第24条 安全保護回路</td> <td rowspan="2">固有のプログラム及び言語を使用した原子炉安全保護計装盤</td> <td>運用・手順</td> <td>—</td> </tr> <tr> <td>保守・点検</td> <td>保守計画に基づき、適切に保守・点検を実施する。また、故障時においては補修を実施する。</td> </tr> <tr> <td rowspan="2">運転管理</td> <td>教育・訓練</td> <td>補修に関する教育を実施する。</td> </tr> <tr> <td>運用・手順</td> <td>運転管理手順に従い、適切に管理を実施する。</td> </tr> <tr> <td rowspan="2">原子炉安全保護計装盤の施錠</td> <td>保守・点検</td> <td>—</td> </tr> <tr> <td>教育・訓練</td> <td>運転管理手順に関する教育を実施する。</td> </tr> <tr> <td rowspan="3">パスワード管理（原子炉保護系設備）</td> <td>運用・手順</td> <td>パスワード管理及び入力操作に関する手順に従い適切に管理・操作を実施する。</td> </tr> <tr> <td>保守・点検</td> <td>—</td> </tr> <tr> <td>教育・訓練</td> <td>パスワード管理、入力操作に関する教育を実施する。</td> </tr> <tr> <td rowspan="3">安全保護系は外部ネットワークと直接接続しない※</td> <td>運用・手順</td> <td>—</td> </tr> <tr> <td>保守・点検</td> <td>保守計画に基づき、適切に保守・点検を実施する。また、故障時においては補修を実施する。</td> </tr> <tr> <td>教育・訓練</td> <td>補修に関する教育を実施する。</td> </tr> </tbody> </table> <p>※外部からのアクセスができない対応を実施している。</p>	設置許可基準対象条文	対象項目	区分	運用対策等	第24条 安全保護回路	固有のプログラム及び言語を使用した原子炉安全保護計装盤	運用・手順	—	保守・点検	保守計画に基づき、適切に保守・点検を実施する。また、故障時においては補修を実施する。	運転管理	教育・訓練	補修に関する教育を実施する。	運用・手順	運転管理手順に従い、適切に管理を実施する。	原子炉安全保護計装盤の施錠	保守・点検	—	教育・訓練	運転管理手順に関する教育を実施する。	パスワード管理（原子炉保護系設備）	運用・手順	パスワード管理及び入力操作に関する手順に従い適切に管理・操作を実施する。	保守・点検	—	教育・訓練	パスワード管理、入力操作に関する教育を実施する。	安全保護系は外部ネットワークと直接接続しない※	運用・手順	—	保守・点検	保守計画に基づき、適切に保守・点検を実施する。また、故障時においては補修を実施する。	教育・訓練	補修に関する教育を実施する。	<p>別添-1表 運用、手順に係る対策等（設計基準）</p> <table border="1"> <thead> <tr> <th>設置許可基準対象条文</th> <th>対象項目</th> <th>区分</th> <th>運用対策等</th> </tr> </thead> <tbody> <tr> <td rowspan="4">第24条 安全保護回路</td> <td rowspan="4">施錠管理</td> <td>運用・手順</td> <td>・施錠管理に関する管理方法を定める。</td> </tr> <tr> <td>体制</td> <td>（運転員、保修員による識別及び施錠管理）</td> </tr> <tr> <td>保守・点検</td> <td>—</td> </tr> <tr> <td>教育・訓練</td> <td>—</td> </tr> </tbody> </table>	設置許可基準対象条文	対象項目	区分	運用対策等	第24条 安全保護回路	施錠管理	運用・手順	・施錠管理に関する管理方法を定める。	体制	（運転員、保修員による識別及び施錠管理）	保守・点検	—	教育・訓練	—	<p>技術的能力に係る運用対策等（設計基準）</p> <p>【第24条 安全保護回路】</p> <table border="1"> <thead> <tr> <th>対象項目</th> <th>区分</th> <th>運用対策等</th> </tr> </thead> <tbody> <tr> <td rowspan="3">固有のプログラム及び言語を使用した安全保護設備</td> <td>運用・手順</td> <td>—</td> </tr> <tr> <td>保守・点検</td> <td>適切に保守管理を実施するとともに、必要に応じ補修を行う。</td> </tr> <tr> <td>教育・訓練</td> <td>補修に関する教育を実施する。</td> </tr> <tr> <td rowspan="2">施錠管理（安全保護設備の施錠）</td> <td>運用・手順</td> <td>施錠管理手順に従い、適切に管理を実施する。</td> </tr> <tr> <td>保守・点検</td> <td>—</td> </tr> <tr> <td rowspan="2">パスワード管理（安全保護設備）</td> <td>運用・手順</td> <td>パスワード管理及び入力操作に関する手順に従い、適切に管理・操作を実施する。</td> </tr> <tr> <td>保守・点検</td> <td>—</td> </tr> <tr> <td rowspan="2">安全保護系は外部ネットワークと直接接続しない※</td> <td>運用・手順</td> <td>—</td> </tr> <tr> <td>保守・点検</td> <td>適切に保守管理を実施するとともに、必要に応じ補修を行う。</td> </tr> <tr> <td rowspan="2">出入管理（発電所の入域を管理）</td> <td>運用・手順</td> <td>出入管理手順に関する教育を実施する。</td> </tr> <tr> <td>保守・点検</td> <td>—</td> </tr> <tr> <td rowspan="2">ゲートウェイ</td> <td>運用・手順</td> <td>—</td> </tr> <tr> <td>保守・点検</td> <td>保守計画に基づき、適切に保守・点検を実施する。また、故障時においては補修を実施する。</td> </tr> <tr> <td rowspan="3">検証及び妥当性確認がなされたソフトウェアの使用</td> <td>運用・手順</td> <td>管理手順（検証及び妥当性がなされたソフトウェアの使用の手順含む）手順に従い適切に管理を実施する。</td> </tr> <tr> <td>体制</td> <td>（保修員による管理）</td> </tr> <tr> <td>保守・点検</td> <td>—</td> </tr> <tr> <td rowspan="3">検証及び妥当性確認がなされたソフトウェアの使用</td> <td>運用・手順</td> <td>管理手順（検証及び妥当性がなされたソフトウェアの使用の手順含む）に従い、適切に管理を実施する。</td> </tr> <tr> <td>体制</td> <td>（保修員による管理）</td> </tr> <tr> <td>教育・訓練</td> <td>管理手順（検証及び妥当性がなされたソフトウェアの使用）に関する教育を実施する。</td> </tr> </tbody> </table> <p>※外部からのアクセスができない対応を実施している。</p>	対象項目	区分	運用対策等	固有のプログラム及び言語を使用した安全保護設備	運用・手順	—	保守・点検	適切に保守管理を実施するとともに、必要に応じ補修を行う。	教育・訓練	補修に関する教育を実施する。	施錠管理（安全保護設備の施錠）	運用・手順	施錠管理手順に従い、適切に管理を実施する。	保守・点検	—	パスワード管理（安全保護設備）	運用・手順	パスワード管理及び入力操作に関する手順に従い、適切に管理・操作を実施する。	保守・点検	—	安全保護系は外部ネットワークと直接接続しない※	運用・手順	—	保守・点検	適切に保守管理を実施するとともに、必要に応じ補修を行う。	出入管理（発電所の入域を管理）	運用・手順	出入管理手順に関する教育を実施する。	保守・点検	—	ゲートウェイ	運用・手順	—	保守・点検	保守計画に基づき、適切に保守・点検を実施する。また、故障時においては補修を実施する。	検証及び妥当性確認がなされたソフトウェアの使用	運用・手順	管理手順（検証及び妥当性がなされたソフトウェアの使用の手順含む）手順に従い適切に管理を実施する。	体制	（保修員による管理）	保守・点検	—	検証及び妥当性確認がなされたソフトウェアの使用	運用・手順	管理手順（検証及び妥当性がなされたソフトウェアの使用の手順含む）に従い、適切に管理を実施する。	体制	（保修員による管理）	教育・訓練	管理手順（検証及び妥当性がなされたソフトウェアの使用）に関する教育を実施する。	
設置許可基準対象条文	対象項目	区分	運用対策等																																																																																																	
第24条 安全保護回路	固有のプログラム及び言語を使用した原子炉安全保護計装盤	運用・手順	—																																																																																																	
		保守・点検	保守計画に基づき、適切に保守・点検を実施する。また、故障時においては補修を実施する。																																																																																																	
	運転管理	教育・訓練	補修に関する教育を実施する。																																																																																																	
		運用・手順	運転管理手順に従い、適切に管理を実施する。																																																																																																	
	原子炉安全保護計装盤の施錠	保守・点検	—																																																																																																	
		教育・訓練	運転管理手順に関する教育を実施する。																																																																																																	
	パスワード管理（原子炉保護系設備）	運用・手順	パスワード管理及び入力操作に関する手順に従い適切に管理・操作を実施する。																																																																																																	
		保守・点検	—																																																																																																	
		教育・訓練	パスワード管理、入力操作に関する教育を実施する。																																																																																																	
	安全保護系は外部ネットワークと直接接続しない※	運用・手順	—																																																																																																	
保守・点検		保守計画に基づき、適切に保守・点検を実施する。また、故障時においては補修を実施する。																																																																																																		
教育・訓練		補修に関する教育を実施する。																																																																																																		
設置許可基準対象条文	対象項目	区分	運用対策等																																																																																																	
第24条 安全保護回路	施錠管理	運用・手順	・施錠管理に関する管理方法を定める。																																																																																																	
		体制	（運転員、保修員による識別及び施錠管理）																																																																																																	
		保守・点検	—																																																																																																	
		教育・訓練	—																																																																																																	
対象項目	区分	運用対策等																																																																																																		
固有のプログラム及び言語を使用した安全保護設備	運用・手順	—																																																																																																		
	保守・点検	適切に保守管理を実施するとともに、必要に応じ補修を行う。																																																																																																		
	教育・訓練	補修に関する教育を実施する。																																																																																																		
施錠管理（安全保護設備の施錠）	運用・手順	施錠管理手順に従い、適切に管理を実施する。																																																																																																		
	保守・点検	—																																																																																																		
パスワード管理（安全保護設備）	運用・手順	パスワード管理及び入力操作に関する手順に従い、適切に管理・操作を実施する。																																																																																																		
	保守・点検	—																																																																																																		
安全保護系は外部ネットワークと直接接続しない※	運用・手順	—																																																																																																		
	保守・点検	適切に保守管理を実施するとともに、必要に応じ補修を行う。																																																																																																		
出入管理（発電所の入域を管理）	運用・手順	出入管理手順に関する教育を実施する。																																																																																																		
	保守・点検	—																																																																																																		
ゲートウェイ	運用・手順	—																																																																																																		
	保守・点検	保守計画に基づき、適切に保守・点検を実施する。また、故障時においては補修を実施する。																																																																																																		
検証及び妥当性確認がなされたソフトウェアの使用	運用・手順	管理手順（検証及び妥当性がなされたソフトウェアの使用の手順含む）手順に従い適切に管理を実施する。																																																																																																		
	体制	（保修員による管理）																																																																																																		
	保守・点検	—																																																																																																		
検証及び妥当性確認がなされたソフトウェアの使用	運用・手順	管理手順（検証及び妥当性がなされたソフトウェアの使用の手順含む）に従い、適切に管理を実施する。																																																																																																		
	体制	（保修員による管理）																																																																																																		
	教育・訓練	管理手順（検証及び妥当性がなされたソフトウェアの使用）に関する教育を実施する。																																																																																																		
<p>技術的能力に係る運用対策等（設計基準）</p> <table border="1"> <thead> <tr> <th>設置許可基準対象条文</th> <th>対象項目</th> <th>区分</th> <th>運用対策等</th> </tr> </thead> <tbody> <tr> <td rowspan="10">第24条 安全保護回路</td> <td rowspan="3">出入管理（発電所の入域を管理）</td> <td>運用・手順</td> <td>出入管理手順に従い、適切に管理を実施する。</td> </tr> <tr> <td>保守・点検</td> <td>—</td> </tr> <tr> <td>教育・訓練</td> <td>出入管理手順に関する教育を実施する。</td> </tr> <tr> <td rowspan="2">ゲートウェイ</td> <td>運用・手順</td> <td>—</td> </tr> <tr> <td>体制</td> <td>（保修員によるゲートウェイの保守・点検）</td> </tr> <tr> <td rowspan="3">検証及び妥当性確認がなされたソフトウェアの使用</td> <td>運用・手順</td> <td>管理手順（検証及び妥当性がなされたソフトウェアの使用の手順含む）手順に従い適切に管理を実施する。</td> </tr> <tr> <td>体制</td> <td>（保修員による管理）</td> </tr> <tr> <td>保守・点検</td> <td>—</td> </tr> <tr> <td rowspan="2">検証及び妥当性確認がなされたソフトウェアの使用</td> <td>運用・手順</td> <td>管理手順（検証及び妥当性がなされたソフトウェアの使用）の教育を実施する。</td> </tr> <tr> <td>教育・訓練</td> <td>—</td> </tr> </tbody> </table>	設置許可基準対象条文	対象項目	区分	運用対策等	第24条 安全保護回路	出入管理（発電所の入域を管理）	運用・手順	出入管理手順に従い、適切に管理を実施する。	保守・点検	—	教育・訓練	出入管理手順に関する教育を実施する。	ゲートウェイ	運用・手順	—	体制	（保修員によるゲートウェイの保守・点検）	検証及び妥当性確認がなされたソフトウェアの使用	運用・手順	管理手順（検証及び妥当性がなされたソフトウェアの使用の手順含む）手順に従い適切に管理を実施する。	体制	（保修員による管理）	保守・点検	—	検証及び妥当性確認がなされたソフトウェアの使用	運用・手順	管理手順（検証及び妥当性がなされたソフトウェアの使用）の教育を実施する。	教育・訓練	—																																																																							
設置許可基準対象条文	対象項目	区分	運用対策等																																																																																																	
第24条 安全保護回路	出入管理（発電所の入域を管理）	運用・手順	出入管理手順に従い、適切に管理を実施する。																																																																																																	
		保守・点検	—																																																																																																	
		教育・訓練	出入管理手順に関する教育を実施する。																																																																																																	
	ゲートウェイ	運用・手順	—																																																																																																	
		体制	（保修員によるゲートウェイの保守・点検）																																																																																																	
	検証及び妥当性確認がなされたソフトウェアの使用	運用・手順	管理手順（検証及び妥当性がなされたソフトウェアの使用の手順含む）手順に従い適切に管理を実施する。																																																																																																	
		体制	（保修員による管理）																																																																																																	
		保守・点検	—																																																																																																	
	検証及び妥当性確認がなされたソフトウェアの使用	運用・手順	管理手順（検証及び妥当性がなされたソフトウェアの使用）の教育を実施する。																																																																																																	
		教育・訓練	—																																																																																																	