資料６－１

泊発電所３号炉審査資料	
資料番号	DB24　r.8.0
提出年月日	令和5年2月16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）

第24条　安全保護回路

令和５年２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。

第24条：安全保護回路

＜目　次＞

3.　技術的能力説明資料

（別添資料）泊発電所３号炉　技術的能力説明資料　安全保護回路

＜概　要＞

１．において，設計基準対象施設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。

２．において，設計基準対象施設について，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。

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。

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（表１）。

表１　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。	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。	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。	変更なし
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。		変更なし
三　安全保護回路を構成する機械若しくは器具又はチャンネルは、単一故障が起きた場合又は使用状態からの単一の取り外しを行った場合において、安全保護機能を失わないよう、多重性を確保するものとすること。	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	三　系統を構成するチャンネルは、それぞれ互いに分離	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
互いに分離し、それぞれのチャンネル間において安全保護機能を失わないように独立性を確保するものとすること。	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。	
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。	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こと。	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こと。	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

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
	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

1.2 追加要求事項に対する適合性

(1) 位置，構造及び設備

ロ．発電用原子炉施設の一般構造

(3) その他の主要な構造

（ⅰ）本発電用原子炉施設は，(1)耐震構造，(2)耐津波構造に加え，以下の基本的方針のもとに安全設計を行う。

a. 設計基準対象施設

(s) 安全保護回路

安全保護回路は，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。

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。

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。

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。

安全保護回路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。

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。

【説明資料（2.1：P24 条-39，40）（2.2：P24 条-40）（2.3：P24 条-40，41）（2.4：P24 条-42）（2.5：P24 条-42）（2.6：P24 条-43-45）（2.7：P24 条-46）（2.9：P24 条-49）】

ヘ．計測制御系統施設の構造及び設備

(1) 計装

（ⅰ）核計装の種類

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。

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

（ⅱ）その他の主要な計装の種類

発電用原子炉施設の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。

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となる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。

(2) 安全保護回路

安全保護回路（安全保護系）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。

安全保護回路は，原子炉停止回路（原子炉保護設備）及びその他の主要な安全保護回路（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。

安全保護回路は，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。

【説明資料（2.1：P24 条-39,40）（2.2：P24 条-40）（2.3：P24 条-40,41）（2.4：P24 条-42）（2.5：P24 条-42）（2.6：P24 条-43-45）（2.7：P24 条-46）（2.9：P24 条-49）】

（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。

原子炉停止回路（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。

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

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。

（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。

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

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

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

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

なお，手動操作で上記動作を行うことができる。

(2) 安全設計方針

1. 安全設計

1.1 安全設計の方針

1.1.5 計測制御系統施設設計の基本方針

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。

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。

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・セイフ又はフェイル・アズ・イズ）とする。

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。

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-39,40）（2.2：P24 条-40）（2.3：P24 条-40,41）（2.4：P24 条-42）（2.5：P24 条-42）（2.6：P24 条-43-45）（2.7：P24 条-46）（2.9：P24 条-49）】

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。

(3) 適合性説明

第二十四条　安全保護回路

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。 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。 三　安全保護回路を構成する機械若しくは器具又はチャンネルは、単一故障が起きた場合又は使用状態からの単一の取り外しを行った場合において、安全保護機能を失わないよう、多重性を確保するものとすること。 四　安全保護回路を構成するチャンネルは、それぞれ互いに分離し、それぞれのチャンネル間において安全保護機能を失わないように独立性を確保するものとすること。 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。 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。 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。

適合のための設計方針

第１項第１号について

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。

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。

第1項第2号について

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。

(1) 原子炉は，以下の条件の場合にトリップする。

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

(2) 工学的安全施設は，以下のとおり作動する。

ａ．原子炉圧力低と加圧器水位低の一致，原子炉圧力異常低，主蒸気ライン圧力低，原子炉格納容器圧力高のいずれかの信号による非常用炉心冷却設備の起動
ｂ．原子炉格納容器圧力異常高信号による原子炉格納容器スプレイ設備の起動
ｃ．原子炉格納容器圧力異常高，主蒸気ライン圧力低，主蒸気ライン圧力減少率高のいずれかの信号による主蒸気隔離弁の閉止
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。

第１項第３号について

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。

具体的には次のとおりである。

(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。

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。

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。

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。

(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。

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。

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。

(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。

第１項第４号について

安全保護系は，通常運転時，保修時，試験時，運転時の異常な過渡変化時及び設計基準事故時において，その安全保護機能を失わないように，その系統を構成するチャンネル相互が分離され，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。

具体的には次のとおりである。

(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。

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・セイフとするか，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・セイフとなる主要なものは次のとおりである。

(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）

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。

第１項第６号について

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。

(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（ハードウェアレベルで一方向のみに通信を許可する装置），防護装置（ソフトウェア的に一方向のみに通信を許可する装置）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する装置）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。

(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プログラム言語を使用し，一般的なコンピュータウイルスが動作しない環境となる設計とする。

(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，「安全保護系へのディジタル計算機の適用に関する規程（JEAC4620-2008）」及び「ディジタル安全保護系の検証及び妥当性確認に関する指針（JEAG4609-2008）」に準じて，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する設計とする。

(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。また，安全保護系のデジタル計算機が収納された盤を施錠管理し，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とともに，保守ツールのパスワード管理により，電気的アクセスを制限する設計とする。

【説明資料（2.1：P24 条-39,40）（2.2：P24 条-40）（2.3：P24 条-40,41）（2.4：P24 条-42）（2.5：P24 条-42）（2.6：P24 条-43-45）（2.7：P24 条-46）（2.9：P24 条-49）】

第1項第7号について

安全保護系は，計測制御系から分離した設計とする。

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も安全保護系への影響を与えない設計とする。

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。

1.3 気象等

該当なし

1.4 設備等（手順等含む）

6. 計測制御設備

6.3 プロセス計装

6.3.1 概要

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。

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。

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。

6.3.2 設計方針

(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。

a．多重性

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。

b．独立性

安全保護回路のプロセス計装は，通常運転時，保修時，試験時，運転時の異常な過渡変化時及び設計基準事故時において，その安全保護機能を失わないように，その系統を構成するチャンネル相互を分離し，それぞれのチャンネル間の独立性を確保した設計とする。

c．通常運転時及び運転時の異常な過渡変化時の機能

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。

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。

d．設計基準事故時の機能

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。

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。

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ことができる設計とする。

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。安全保護回路から計測制御系へ信号を取り出す場合には，計測制御系に故障が生じても，安全保護系に影響を与えない設計とする。

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。

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。

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。

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。

(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。

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。

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。

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。

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。

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。

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。

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に多重化されている。

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。

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。

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。

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。

【説明資料（2.3：P24 条-40, 41）（2.4：P24 条-42）（2.8：P24 条-47, 48）】

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，必要な動作をすること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。

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。

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。

(2) 安全保護回路以外のプロセス計装

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。

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。

a．１次冷却設備計装

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。

b．化学体積制御設備計装

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。

c．主蒸気及び給水設備計装

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。

d．原子炉格納施設計装

原子炉格納施設計装は，格納容器スプレイ流量，格納容器内温度，格納容器再循環サンプ水位等を監視し，必要なものについては警報を発信する。

e．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。

f．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。

g．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。

h．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。

i．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信する。

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。

j．その他

上記のほかに，放射性廃棄物廃棄設備，使用済燃料ピット水浄化冷却設備，試料採取設備等のプロセス計装を設ける。

k．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。

l．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。

6.3.4 主要仕様

安全保護回路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。

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) 安全保護回路のプロセス計装は原則として4チャンネルで構成し，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回路のプロセス計装は，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。

6.3.6 評価

(1) 安全保護回路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回路のプロセス計装は，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) 安全保護回路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) 安全保護回路のプロセス計装は，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) 安全保護回路のプロセス計装は，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) 安全保護回路のプロセス計装及び安全保護回路以外の主要なプロセス計装の電源は，無停電電源装置から給電される。

したがって，一定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の運転下あるいは外部電源のみの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，予想変動範囲内での監視が可能である。

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。

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。

(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。

6.6 原子炉保護設備

6.6.1 概要

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。

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，安全保護回路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。

6.6.2 設計方針

(1) 多重性

原子炉保護設備は，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。

(2) 独立性

原子炉保護設備は，通常運転時，保修時，試験時，運転時の異常な過渡変化時及び設計基準事故時において，その安全保護機能を失わないように，その系統を構成するチャンネル相互を分離し，それぞれのチャンネル間において独立性を確保する設計とする。

(3) 過渡時の機能

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。

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。

(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。

(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。

(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も，安全保護系へ影響を与えない設計とする。

(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。

(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。

(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。

(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。

(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ことができる設計とする。

【説明資料（2.1：P24 条-39，40）（2.2：P24 条-40）（2.3：P24 条-40，41）（2.4：P24 条-42）（2.5：P24 条-42）（2.6：P24 条-43-45）（2.7：P24 条-46）（2.9：P24 条-49）】

(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。

6.6.3 主要設備

(1) 構成

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。

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。

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。

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。

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。

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。

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。

(2) 原子炉トリップ信号

原子炉トリップ信号は以下のものがあり，第6.6.1表及び第6.6.2図に示す。また，第6.6.2 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。

ａ．中性子源領域中性子束高

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，中性子源領域中性子束高の“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，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。

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。

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。

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。

ｄ．出力領域中性子束変化率高

制御棒クラスタの飛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。

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。

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。

過大温度ΔＴ高（ＤＮＢ防止）設定

$$=K_1-K_2\frac{1+\tau_1 s}{1+\tau_2 s}(T-T_0)+K_3(P-P_0)-f(\Delta q)$$

過大温度ΔＴ高（高温側配管沸騰防止）設定

$$=K_4-K_5\frac{1+\tau_3 s}{1+\tau_4 s}(T-T_0)+K_6(P-P_0)$$

ここで，ｓ：ラプラス演算子

Ｔ：１次冷却材平均温度

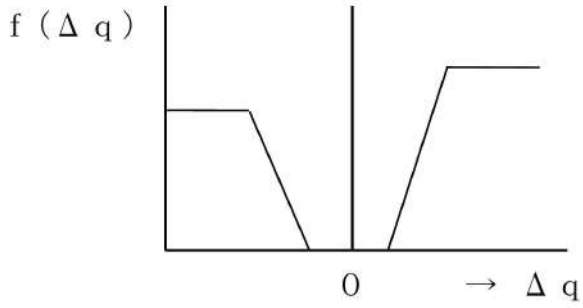
T_0：定格出力運転時の１次冷却材平均温度

Ｐ：加圧器圧力

P_0：原子炉運転圧力

K_1～K_6，τ_1～τ_4：定数

ｆ（Δｑ）：炉外中性子束検出器（出力領域用）信号の上半分（ϕ ｔ）と下半分（ϕ ｂ）の差の関数で，概略を下図に示す。（Δｑ＝ϕ ｔ－ϕ ｂ）



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。

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。

$$\text{過大出力}\Delta T\text{ 高設定}=K_7-\left[K_8\frac{\tau_5 s}{1+\tau_5 s}T\right]-\left[K_9(T-T_0)\right]-f(\Delta q)$$

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

T_0：定格出力運転時の１次冷却材平均温度

K_7～K_9，τ_5：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。

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。

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。

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，出力領域中性子束が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。

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。

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。

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４個の主蒸気止め弁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。

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。

o．加圧器水位高

加圧器の満水を防止するため，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“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．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。

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。

(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。

(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。

a．警報

原子炉保護設備で使用する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が警報設定値に達し，論理回路が作動した場合には，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。

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。

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。

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，定期的に緊急しゃ断のための性能検査及び緊急しゃ断検査を行う。

(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。

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。

6.6.6 手順等

(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。

(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。詳細は，「1.1.1.5 人の不法な侵入等の防止(3)手順等」に示す。

(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。

(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。

(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。

【説明資料（別添）】

6.6.7 評価

(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ので，単一のチャンネルの故障で保護機能を失うことはない。

(2) 独立性

原子炉保護設備は，相互干渉が起こらないように，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。

(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。

(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。

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。

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。

(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。

(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。

(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ことができる設計としている。

6.7 工学的安全施設作動設備

6.7.1 概要

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。

6.7.2 設計方針

(1) 多重性

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。

(2) 独立性

工学的安全施設作動設備は，通常運転時，保修時，試験時，運転時の異常な過渡変化時及び設計基準事故時において，その安全保護機能を失わないように，その系統を構成するチャンネル相互を分離し，それぞれのチャンネル間において独立性を確保する設計とする。

(3) 過渡時の機能

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。

(4) 設計基準事故時の機能

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。

(5) 故障時の機能

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。

(6) 計測制御系との分離

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も，安全保護系へ影響を与えない設計とする。

(7) 試験可能性

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，独立に各チャンネルの試験及び検査ができ

る設計とする。

(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。

(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。

(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。

(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ことができる設計とする。

【説明資料（2.1：P24 条-39,40）（2.2：P24 条-40）（2.3：P24 条-40,41）（2.4：P24 条-42）（2.5：P24 条-42）（2.6：P24 条-43-45）（2.7：P24 条-46）（2.9：P24 条-49）】

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。

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。

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。

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・セイフとなるか，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。

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。

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 6.7.1 図に示す。

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。

6.7.7 評価

(1) 単一故障

工学的安全施設作動回路を構成する論理回路には，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，2系列化している。これらの系列は，電気的，物理的に分離しているので，単一の系列の故障で機能を失うことはない。

(2) 独立性

工学的安全施設作動回路は，相互干渉が起こらないように，物理的，電気的独立性を持たせている。すなわち，論理回路，連絡ケーブル等は供給電源を含めて独立な構成としている。

(3) 運転中試験

工学的安全施設作動回路は，運転中にも論理回路の試験ができる。すなわち，テストスイッチを操作することにより論理回路が正常に動作したことを確認できる。

(4) 手動操作

必要な場合，手動でも工学的安全施設作動を行えるように，中央制御盤に操作スイッチを設け，以下の作動信号をそれぞれ発することができる。

a. 非常用炉心冷却設備作動信号

b. 原子炉格納容器スプレイ作動信号

c. 主蒸気ライン隔離信号

d. 原子炉格納容器隔離信号

(5) 作動状況の確認

工学的安全施設の作動状況はプロセス計装，警報及び表示灯によって確認することができる。

(6) 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ことができる設計としている。

第6.3.1表　安全保護回路のプロセス計装

項　　目	チャンネル数	検　出　器
原子炉圧力	4	圧力伝送器
加圧器水位	4	差圧伝送器
1次冷却材流量	4／ループ	差圧伝送器
1次冷却材温度	4	測温抵抗式温度計
蒸気発生器水位	4／蒸気発生器	差圧伝送器
主蒸気ライン圧力	4／ループ	圧力伝送器
原子炉格納容器圧力	4	圧力伝送器
タービン第1段圧力	4	圧力伝送器
1次冷却材ポンプ電源電圧	4	不足電圧継電器
1次冷却材ポンプ電源周波数	4	周波数継電器
タービン非常遮断油圧	4	圧力スイッチ
主蒸気止め弁位置	4	弁位置スイッチ
地震加速度		
水平方向(上部階)	4	加速度検出器
水平方向(下部階)	4	加速度検出器
鉛直方向(下部階)	4	加速度検出器

第 6.3.2 表　事故時監視が必要なプロセス計装

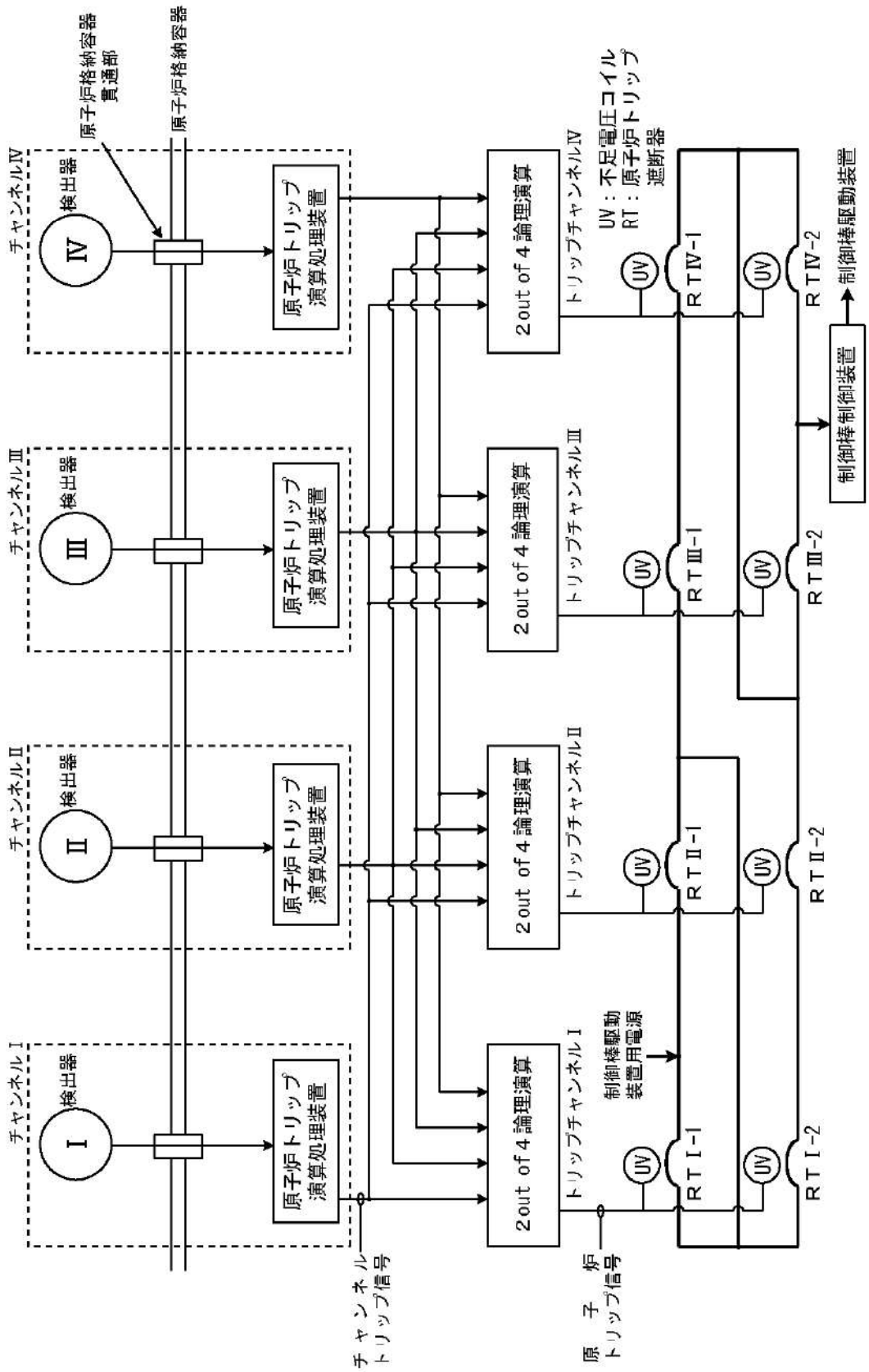
項　　目	名　　称
1 次 冷 却 設 備 計 装	1 次冷却材温度（広域－高温側，低温側） 1 次冷却材圧力（広域） 原子炉容器水位
化 学 体 積 制 御 設 備 計 装	ほう酸タンク水位
主 蒸 気 及 び 給 水 設 備 計 装	補助給水流量 蒸気発生器水位（広域） 補助給水ピット水位
原 子 炉 格 納 施 設 計 装	格納容器内温度 格納容器再循環サンプ水位（広域，狭域）
原子炉補機冷却水設備計装	原子炉補機冷却水サージタンク水位
原子炉補機冷却海水設備計装	原子炉補機冷却海水母管圧力
制 御 用 圧 縮 空 気 設 備 計 装	制御用空気圧力
非 常 用 炉 心 冷 却 設 備 計 装	高圧注入流量 低圧注入流量 燃料取替用水ピット水位

第6.6.1表　原子炉トリップ信号一覧表

原子炉トリップ信号	検　出　器	作動ロジック	インターロック	作動限界値又は計画設定値
中性子源領域中性子束高	中性子源領域中性子束検出器	1／2	（P－6）設定値以上で手動ブロック （P－10）設定値以上で自動ブロック	10^5 cps (注2)
中間領域中性子束高	中間領域中性子束検出器	1／2	（P－10）設定値以上で手動ブロック	定格出力の25% (注2)
出力領域中性子束高 a．低設定 b．高設定	出力領域中性子束検出器 出力領域中性子束検出器	2／4 2／4	低設定については （P－10）設定値以上で手動ブロック	低設定：定格出力の35% (注1) 高設定：定格出力の118% (注1)
出力領域中性子束変化率高 a．増加率高 b．減少率高	出力領域中性子束検出器 出力領域中性子束検出器	2／4 2／4		増加率高：定格出力の＋10%（時定数1秒の不完全微分演算において）(注2) 減少率高：定格出力の－7%（時定数1秒の不完全微分演算において）(注2)
非常用炉心冷却設備作動			第7.5.1表参照	第7.5.1表参照
過大温度ΔT高 a．DNB防止 b．高温側配管満膨防止	1次冷却材温度検出器 加圧器圧力検出器 出力領域中性子束検出器 1次冷却材温度検出器 加圧器圧力検出器	2／4 2／4		第7.4.3図参照 (注1)
過大出力ΔT高	1次冷却材温度検出器 出力領域中性子束検出器	2／4		第7.4.3図参照 (注1)
原子炉圧力高	加圧器圧力検出器	2／4		16.61MPa[gage] (注1)
原子炉圧力低	加圧器圧力検出器	2／4	（P－7）設定値以下で自動ブロック	12.73MPa[gage] (注1)
1次冷却材流量低	1次冷却材流量検出器	各ループ2／4	1ループは（P－8）設定値以下で自動ブロック 2ループ以上は（P－7）設定値以下で自動ブロック	定格流量の87% (注1)
1次冷却材ポンプ電源電圧低	1次冷却材ポンプ電源低電圧リレー	2台以上の1次冷却材ポンプ電源電圧低の2／4	（P－7）設定値以下で自動ブロック	定格電圧の65% (注1)
1次冷却材ポンプ電源周波数低	1次冷却材ポンプ電源周波数リレー	2台以上の1次冷却材ポンプ電源周波数低の2／4	（P－7）設定値以下で自動ブロック	46.5Hz (注2)
タービントリップ	タービン非常遮断油圧検出器 主蒸気止め弁	2／4 4個　閉	（P－7）設定値以下で自動ブロック	タービン非常遮断油圧6.86MPa[gage] (注2)
蒸気発生器水位低	蒸気発生器水位検出器	各蒸気発生器2／4		狭域計器スパンの0%水位 (注1)
加圧器水位高	加圧器水位検出器	2／4	（P－7）設定値以下で自動ブロック	計器スパンの100%水位 (注2)
地震加速度大 a．水平方向加速度大 b．鉛直方向加速度大	水平方向加速度検出器 鉛直方向加速度検出器	2／4 2／4		水平方向：350Gal（上部階）(注2) ：240Gal（下部階）(注2) 鉛直方向：120Gal（下部階）(注2)
手　動		1／2		—

（注1）　添付書類十で使用する作動限界値（実際のセット値は，本表の数値に基づき，詳細設計により決定する。）

（注2）　計画設定値（現段階での計器のセット値であり，実際のセット値は，本表の数値に基づき，詳細設計により決定する。）

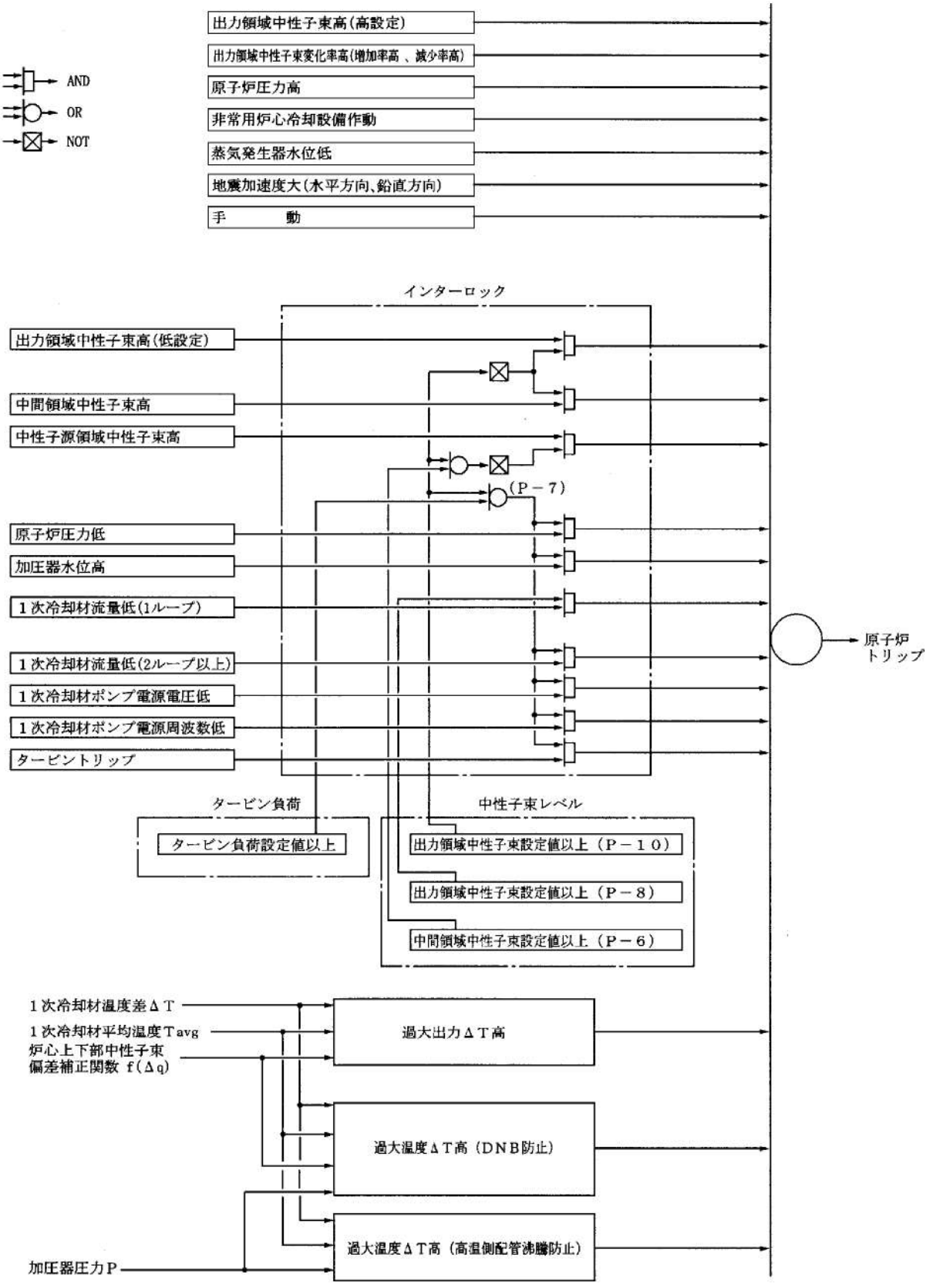


第 6.6.1 図　原子炉保護設備系統図（“2 out of 4”の場合）

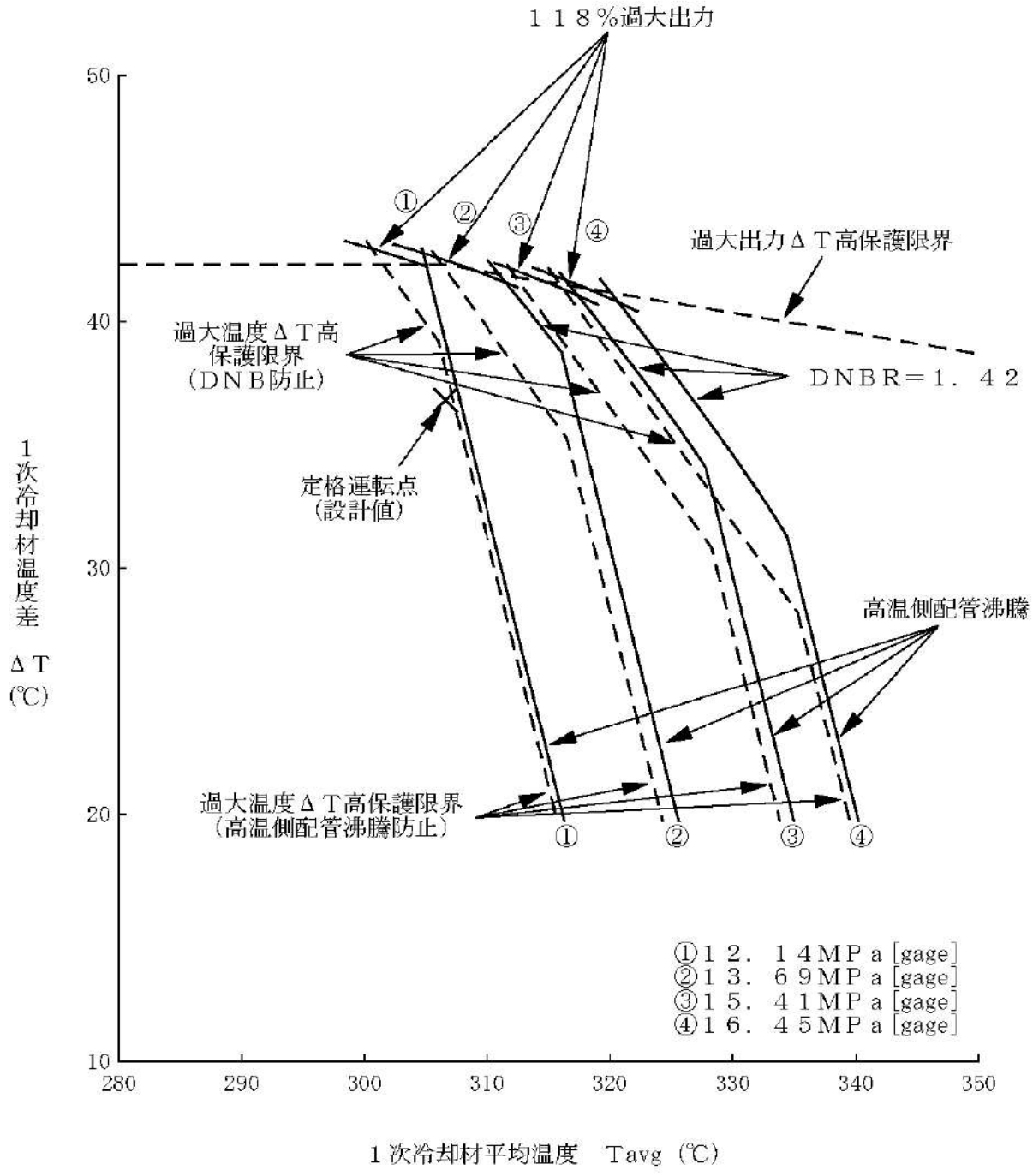
第6.6.2表　原子炉トリップ信号に関するパーミッシブ信号一覧表

パーミッシブ信号の記号	機　　能	入力信号	計画設定値(注)
P－6	中性子源領域中性子束高原子炉トリップの手動ブロック許可	中間領域中性子束高	10^{-10} A
P－7	a．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許可 b．1次冷却材ポンプ電源電圧低による原子炉トリップ許可 c．1次冷却材ポンプ電源周波数低による原子炉トリップ許可 d．タービントリップによる原子炉トリップ許可 e．原子炉圧力低による原子炉トリップ許可 f．加圧器水位高による原子炉トリップ許可	出力領域中性子束高 あるいは タービン第1段圧力高	原子炉出力の10% タービン出力の10%
P－8	1ループの1次冷却材流量低による原子炉トリップ許可	出力領域中性子束高	原子炉出力の40%
P－10	a．中性子源領域中性子束高原子炉トリップの自動ブロック b．中間領域中性子束高原子炉トリップの手動ブロック許可 c．出力領域中性子束高（低設定）原子炉トリップの手動ブロック許可	出力領域中性子束高	原子炉出力の10%

（注）　P－8以外は現段階での計器のセット値であり，実際のセット値は，本表の数値に基づき，詳細設計により決定する。



第 6.6.2 図　原子炉保護設備信号図



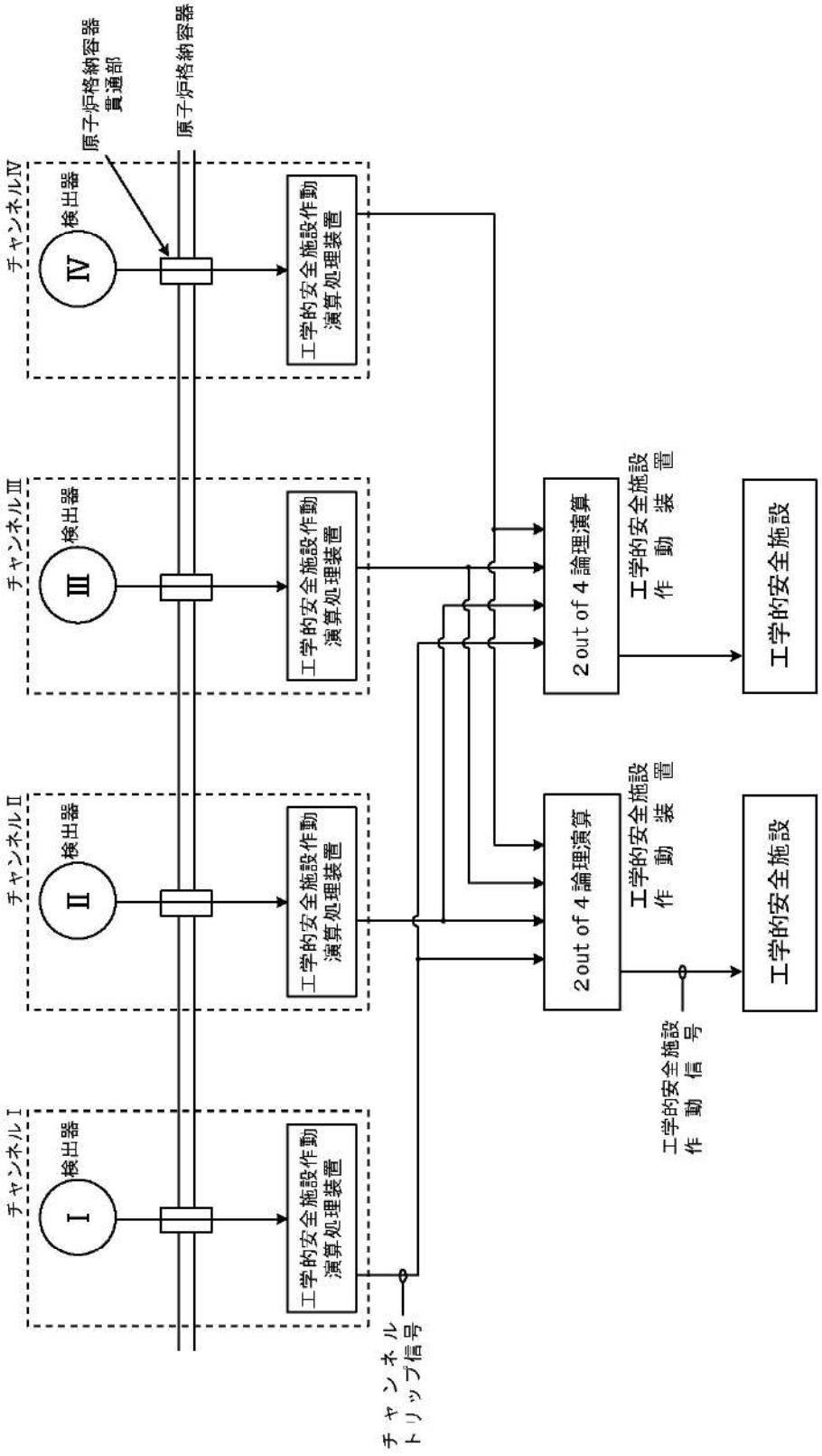
第 6.6.3 図　過大温度ΔＴ高及び過大出力ΔＴ高による保護限界図（代表例）

第 6.7.1 表　工学的安全施設作動信号一覧表

工学的安全施設作動信号		検　出　器	作動ロジック	インターロック	作動限界値又は計画設定値
非常用炉心冷却設備作動信号	a．原子炉圧力低と加圧器水位低の一致	加圧器圧力検出器 加圧器水位検出器	加圧器圧力低と加圧器水位低の一致の２／４	（Ｐ－１１）設定値以下で手動ブロック	12.04MPa[gage] (注1) 計器スパンの 0%水位 (注1)
	b．原子炉圧力異常低	加圧器圧力検出器	２／４	（Ｐ－１１）設定値以下で手動ブロック	11.36MPa[gage] (注1)
	c．主蒸気ライン圧力低	主蒸気ライン圧力検出器	各主蒸気ライン圧力低 ２／４	（Ｐ－１１）設定値以下で手動ブロック	3.35MPa[gage] (注1)
	d．原子炉格納容器圧力高	原子炉格納容器圧力検出器	２／４		0.034MPa[gage] (注1)
	e．手　動		１／２		－
主蒸気ライン隔離信号	a．原子炉格納容器圧力異常高	原子炉格納容器圧力検出器	２／４		0.083MPa[gage] (注2)
	b．主蒸気ライン圧力低	非常用炉心冷却設備作動信号ｃ．と同じ	非常用炉心冷却設備作動信号ｃ．と同じ	非常用炉心冷却設備作動信号ｃ．と同じ	非常用炉心冷却設備作動信号ｃ．と同じ
	c．主蒸気ライン圧力減少率高	主蒸気ライン圧力検出器	各主蒸気ライン圧力減少率高 ２／４	（Ｐ－１１）設定値以上で自動ブロック	-0.69MPa （時定数 50 秒の不完全微分演算において） (注2)
	d．手　動		１／２		－
原子炉格納容器スプレイ作動信号	a．原子炉格納容器圧力異常高	原子炉格納容器圧力検出器	２／４		0.136MPa[gage] (注1)
	b．手　動		（２／２）×１／２		－
原子炉格納容器隔離信号	a．非常用炉心冷却設備作動信号	非常用炉心冷却設備作動信号と同じ	非常用炉心冷却設備作動信号と同じ		非常用炉心冷却設備作動信号と同じ
	b．原子炉格納容器スプレイ作動信号	原子炉格納容器スプレイ作動信号と同じ	原子炉格納容器スプレイ作動信号と同じ		原子炉格納容器スプレイ作動信号と同じ
	c．手　動		１／２		－

（注１）　添付書類十で使用する作動限界値（実際のセット値は，本表の数値に基づき，詳細設計により決定する。）

（注２）　計画設定値（現段階での計器のセット値であり，実際のセット値は，本表の数値に基づき，詳細設計により決定する。）



第 6.7.1 図　工学的安全施設作動設備系統図

2.　追加要求事項に対する適合方針

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

「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こと。』が要求されている。

泊発電所３号炉の安全保護回路は，デジタル計算機で構成している。

安全保護回路（原子炉保護設備及び工学的安全施設作動設備）の不正アクセス行為による被害防止については，デジタル計算機に，下記の対策を実施している。

(1) 物理的及び電気的アクセスの制限対策

発電所への入域に対しては，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，安全保護回路のデジタル計算機が収納された盤（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）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すとともに，保守ツールをパスワード管理することにより，管理されない変更を防止している。

(2) ハードウェアの物理的な分離又は機能的な分離対策

安全保護回路の信号は，安全保護回路→防護装置（ソフトウェア的に一方向のみに通信を許可する装置）→防護装置（[redacted]※1）→データ収集計算機→防護装置（[redacted]※2）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。

(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

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（ソフトウェア的に一方向のみに通信を許可する装置），防護装置（[redacted]※1）及び防護装置（[redacted]※2）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。

(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

安全保護回路は，「安全保護系へのディジタル計算機の適用に関する規程」（JEAC4620-2008）及び「ディジタル安全保護系の検証及び妥当性確認に関する指針」（JEAG4609-2008）に準じて設計，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。

安全保護回路は，固有のプログラム及びプログラム言語を使用（一般的なコンビ

[redacted] 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。

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すとともに，保守ツールをパスワード管理することにより，関係者以外の不正な変更等を防止している。

また，安全保護系は，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）。

(5) 耐ノイズ・サージ対策

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，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。

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。

安全保護回路は，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）

※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

2.2 概要

「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こと。」に対して，安全保護回路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。

2.3 安全保護回路の物理的分離

安全保護回路は，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，安全保護回路にはＵＳＢポートを設けないことで，ＵＳＢメモリー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。

安全保護回路から計測制御系などへのデータ伝送には光信号を用いており，光変換カードによって電気信号を光信号に変換して送信することで，物理的分離及び電気的分離を行っている。

図１　安全保護回路の物理的分離

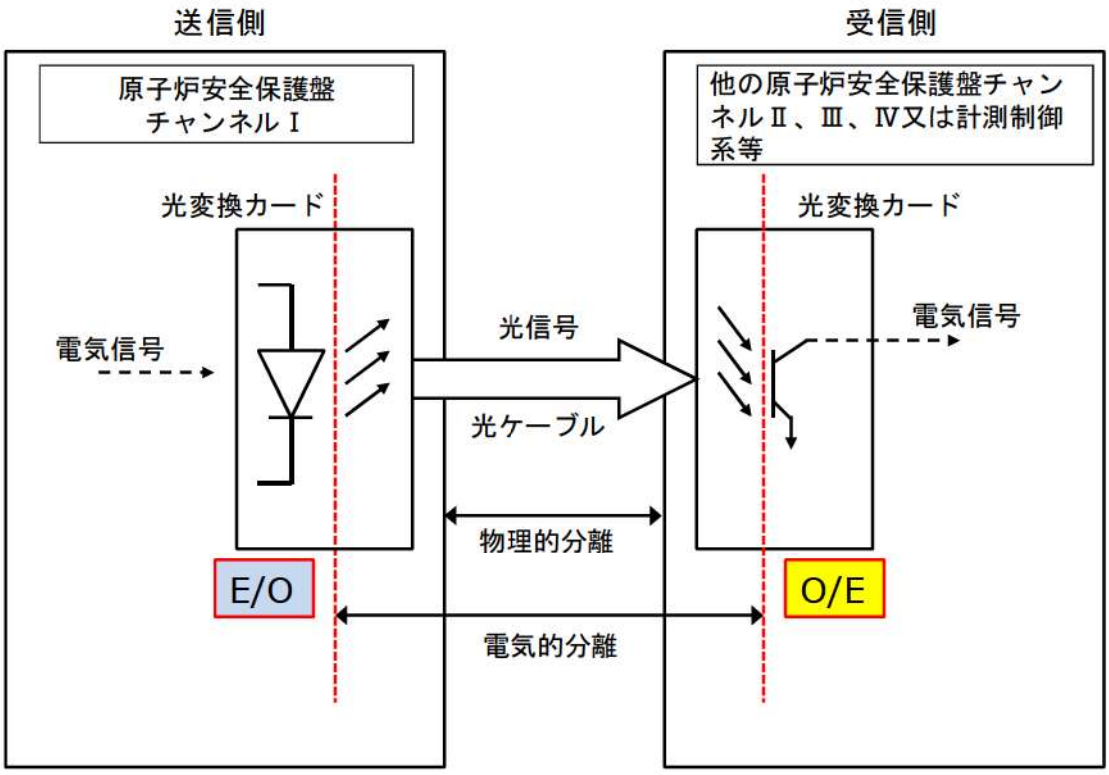


図２　光通信における分離概念図

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。

2.4 安全保護回路の機能的分離

安全保護回路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（ソフトウェア的に一方向のみに通信を許可する装置），防護装置（[redacted]）及び防護装置（[redacted]）を介した一方向通信に制限し，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。

2.5 コンピュータウイルスによる被害の防止

安全保護回路は，固有のプログラム及び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保守ツールの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。

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。

準拠規格

「安全保護系へのディジタル計算機の適用に関する規程」（JEAC4620-2008）

[redacted]

表１　情報システムセキュリティ計画の概要

出典元：泊発電所 情報システムセキュリティ計画

[redacted] 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。

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

安全保護回路は，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。安全保護回路の検証及び妥当性確認について別紙－８に示す。

安全保護回路のプログラムは，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。

準拠規格

「安全保護系へのディジタル計算機の適用に関する規程」（JEAC4620-2008）

「ディジタル安全保護系の検証及び妥当性確認に関する指針」（JEAG4609-2008）

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，安全保護系のシステムへ接続可能なアクセスについて別紙５に示す。

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	
	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	

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））

□ 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。

段階	内容	対策
設計プロセス	安全保護回路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。	
製作プロセス	安全保護回路ソフトウェア設計要求仕様から安全保護回路で実現するためのプログラムを作成する。	
試験プロセス	安全保護回路に対して，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	安全保護回路を発電所に搬入・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	安全保護回路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

安全保護回路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，「安全保護系へのディジタル計算機の適用に関する規程」（JEAC4620-2008）及び「ディジタル安全保護系の検証及び妥当性確認に関する指針」（JEAG4609-2008）に基づき，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。

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。

□ 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。

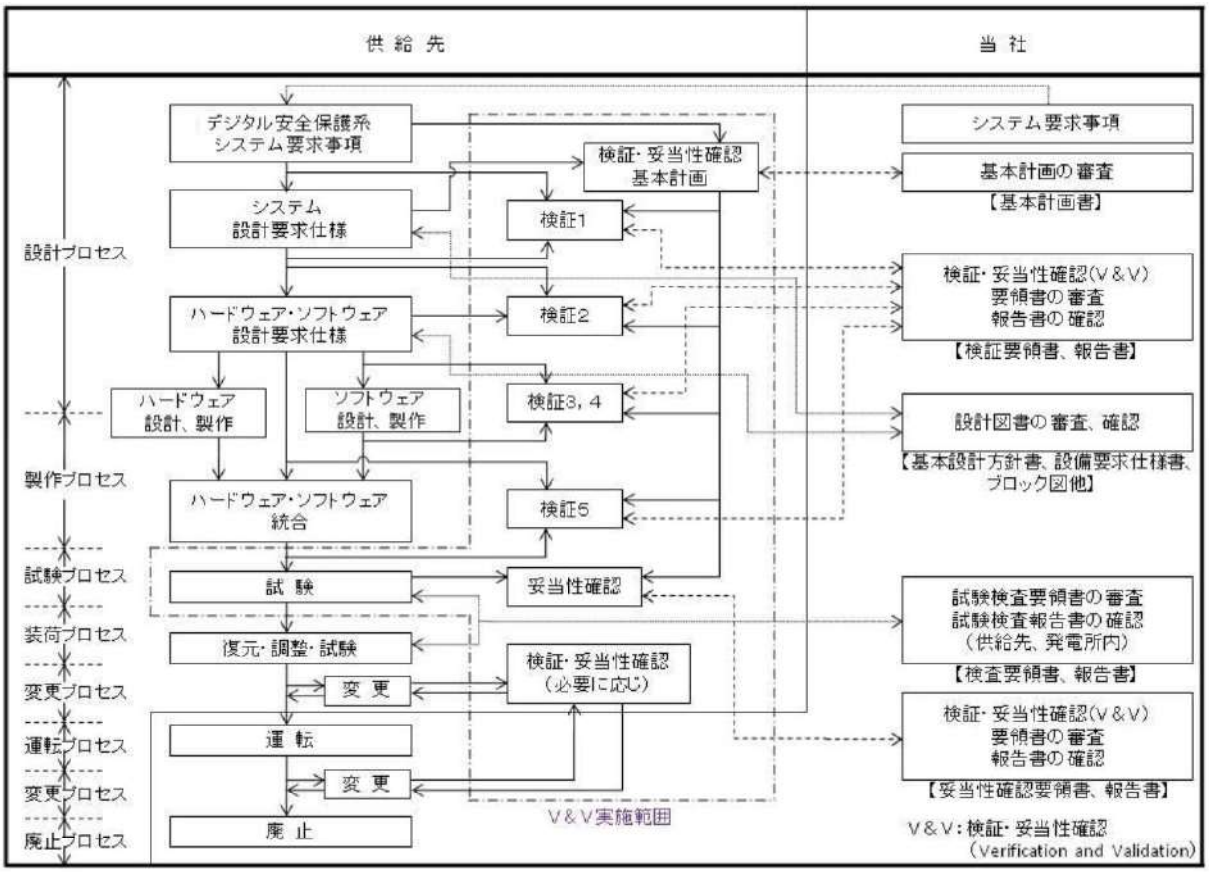


図３　安全保護回路の検証及び妥当性確認

検証項目	検証内容
検証１	システム設計要求仕様検証 安全保護系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，デジタル安全保護系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

2.7 物理的及び電気的アクセスの制限

発電所への入域に対する出入管理及び，安全保護回路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，安全保護回路の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，保守ツール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。

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のあるデータ等については，安全保護回路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，防護装置（ソフトウェア的に一方向のみに通信を許可する装置）により，信号の流れが安全保護回路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，安全保護回路とデータ収集計算機との間に設けた防護装置（[redacted]）により，ハードウェアレベルで信号の流れが安全保護回路から信号を送信するのみの一方向となっている。

加えて，データ収集計算機と外部システムとの間には，防護装置（[redacted]）を介して接続している。

また，安全保護系は，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。

[redacted]

図４　不正アクセス防止の概念図

[redacted] 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。

2.8 安全保護回路の概要

安全保護回路は，デジタル計算機で構成している。安全保護回路の構成を図５に示すとともに，詳細を別紙９に示す。

安全保護回路は，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。

安全保護系は，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。

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。

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も安全保護系へ影響を与えない設計とする。

また，安全保護回路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。

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。

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。

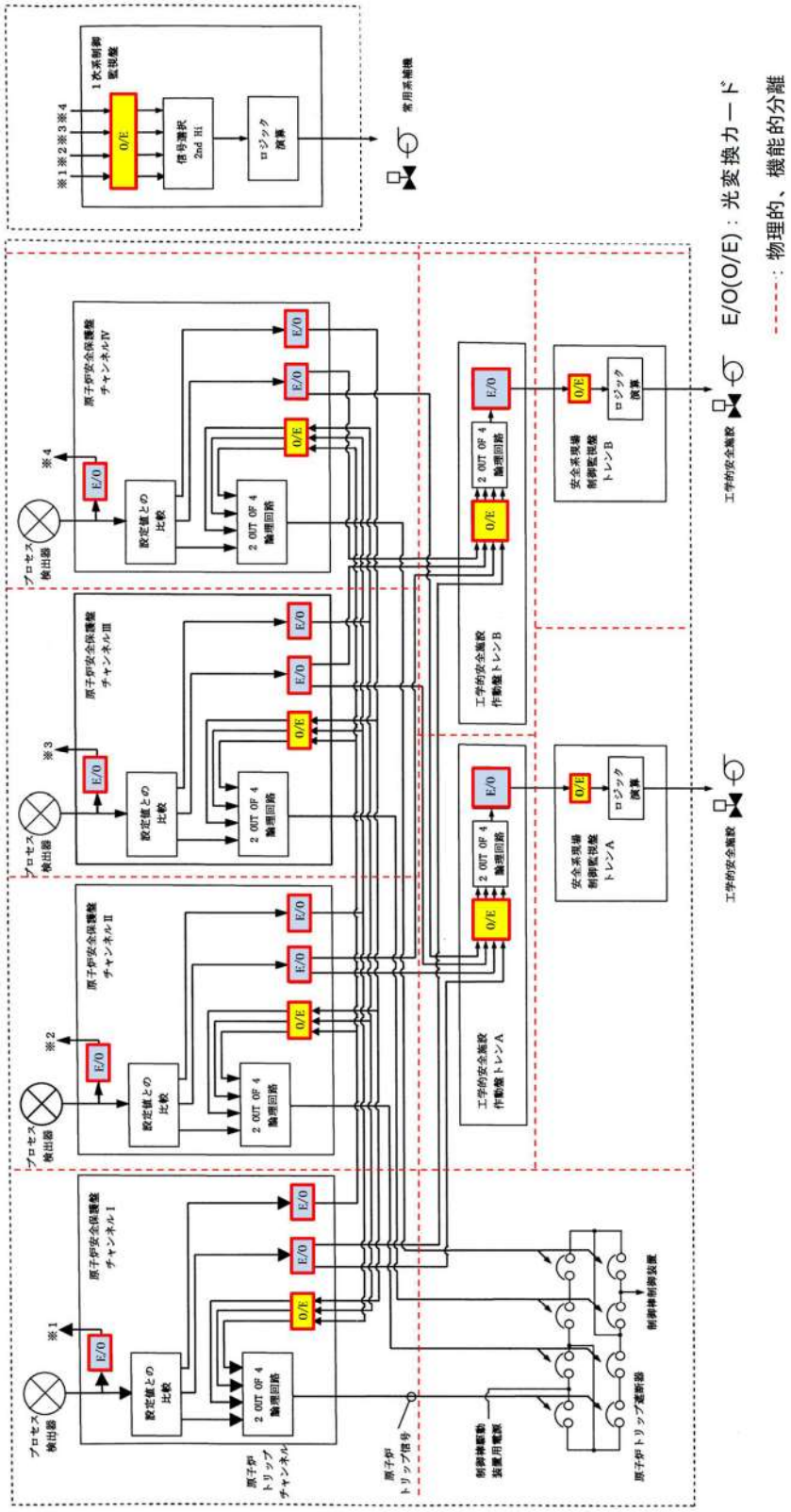


図５　安全保護回路の構成

2.9 安全保護回路のソフトウェア変更管理

2.10 耐ノイズ・サージ対策

安全保護回路は，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）

上記 2.1～2.10 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。

□ 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。

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

安全保護回路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。

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。

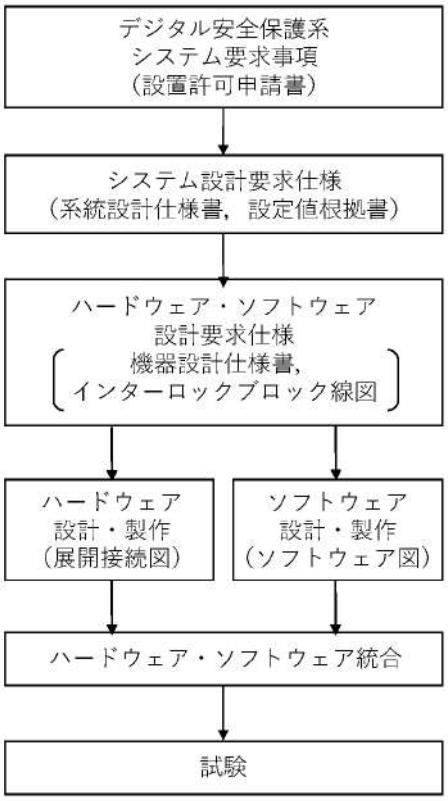
安全保護回路のソフトウェアは設計，製作，試験及び変更管理の各段階で検証と妥当性の確認を適切に行う。

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。

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。

安全保護系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。

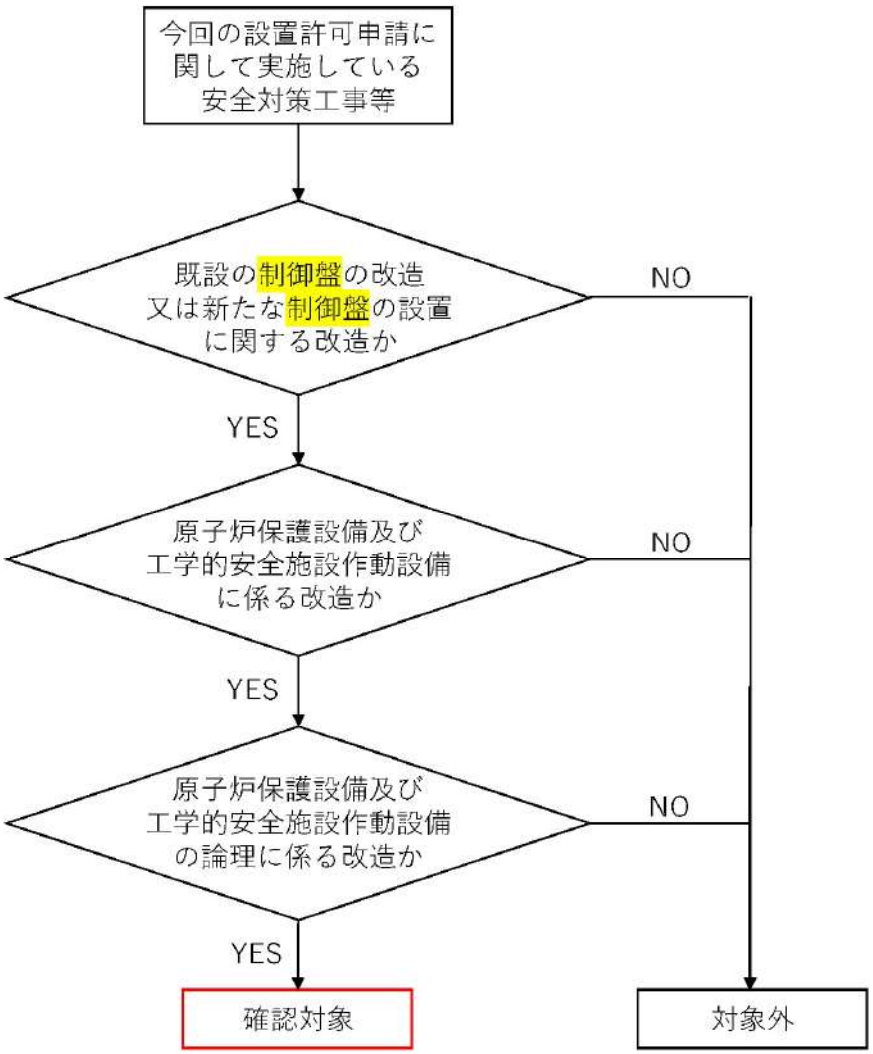
安全保護回路に係る現場作業を実施する際は，中央制御室にて発電課長（当直）の許可を得て，発電課長（当直）の管理する鍵を借用する必要があり，外部からの人的妨害行為又は破壊行為を防止している。



別紙 1-1 図 安全保護系の設計・製作・試験の流れ（例）

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

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，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。



別紙 2-1 図 安全保護回路の論理に係る改造抽出フロー

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

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下記のとおり抽出した。

(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

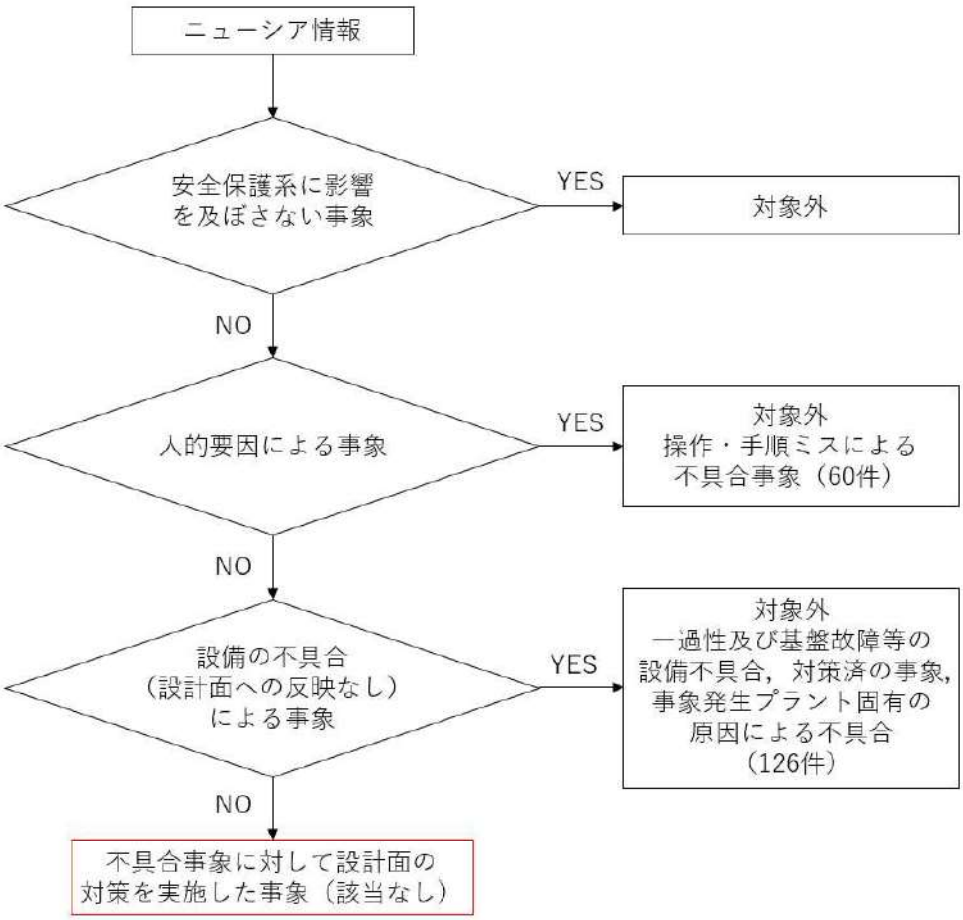
b. キーワード検索（安全保護系，原子炉保護系，工学的安全施設作動回路，雷，ノイズ，スクラム等）により抽出

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。）

(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号炉の安全保護系の設計面へ反映すべき事項は抽出されなかった。

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。



別紙 3-1 図 設計面へ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。

参考１

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

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。

泊発電所３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。

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。

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

安全保護回路について，以下の対策を実施する。

(1) 作業管理

a．安全保護回路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。

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，安全保護回路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。

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。

別紙５　安全保護回路のシステムへ接続可能なアクセスについて

安全保護回路は，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すとともに，保守ツールをパスワード管理しており，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。

別紙 5-1 図 安全保護回路に係るソフトウェア変更手順

□ 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。

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※１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	発電所の出入管理を社内手順に定め実施	左記手順に従い実施
	・盤の施錠管理 ・保守ツールの接続箇所を施錠管理された盤内で常時物理的に切り離すとともに，保守ツールをパスワード管理	鍵管理及びパスワード管理を社内手順に定め実施	左記手順に従い実施
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】	・安全保護回路の信号は防護装置（ソフトウェア的に一方向のみに通信を許可する装置），防護装置（[redacted]及び防護装置（[redacted]を介して外部に伝送 ・信号は一方向のみ（安全保護回路から発信）で，外部からの信号を受信しない設計	機器の設計管理プロセス※２により受注者の実施内容を管理	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※３
	保守ツールの接続箇所を施錠管理された盤内で常時物理的に切り離し	鍵管理を社内手順に定め実施	左記手順に従い実施
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】	防護装置・一方向通信により外部からのデータ書き込み機能を設けない設計	機器の設計管理プロセス※２により受注者の実施内容を管理	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※３
	ソフトウェアは，所定の手順に従わなければ変更できない設計	ソフトウェア変更管理を社内手順に定め実施	左記手順に従い実施

[redacted]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。

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※１の実施内容
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【2.1(4),2.3, 2.5, 2.6, 2.7, 2.9, 別紙５，８】	安全保護回路のソフトウェアは，JEAC4620，JEAG4609 に準じた管理	機器の設計管理プロセス※２により受注者の実施内容を管理	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※３
	固有のプログラム及びプログラム言語の使用，不要な機能を設けない設計	機器の設計管理プロセス※２により受注者の実施内容を管理	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※３
	発電所の出入管理	発電所の出入管理を社内手順に定め実施	左記手順に従い実施
	・保守ツールの接続箇所を施錠管理された盤内で常時物理的に切り離すとともに，保守ツールをパスワード管理 ・現場作業時の鍵管理	鍵管理及びパスワード管理を社内手順に定め実施	左記手順に従い実施
５．耐ノイズ・サージ対策【2.1(5), 2.10】	ノイズ対策の実施	機器の設計管理プロセス※２により受注者の実施内容を管理	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※３
６．安全保護回路の設計【2.8, 別紙１】	不正アクセス等の被害を受けない構成	機器の設計管理プロセス※２により受注者の実施内容を管理	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※３
	発電所の出入管理	発電所の出入管理を社内手順に定め実施	左記手順に従い実施
	現場作業時の鍵管理	鍵管理を社内手順に定め実施	左記手順に従い実施

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※１の実施内容
7．想定脅威に対する対策【2.6，別紙4】	(1)工場制作・出荷段階 ・外部脅威に対する対策（外部からの侵入）	機器の設計管理プロセス※２により受注者の実施内容を管理 具体的には，調達時に受注者に対し，不正アクセス対策，ウイルス対策，不正プログラム対策，教育等の情報セキュリティ対策を要求し，実施状況を確認。	防護装置（[redacted]及び[redacted]）による社外からの侵入防止対策
	・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）		ソフトウェアは，受注者独自のソフトウェア言語にて構築，作業専用端末のインストール管理，作業専用端末による作業，作業専用エリアへの作業関係者のみの入域管理
	・人的要因（知識不足による情報漏えい等）		左記手順に従い実施
	(2)現場据付以降 ・現場作業時の鍵管理	鍵管理を社内手順に定め実施	左記手順に従い実施
	・機器取り外し時の警報発生	機器の設計管理プロセス※２により受注者の実施内容を管理	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※３
	・作業要領書に基づく点検		
	・保守ツールの接続箇所を施錠管理された盤内で常時物理的に切り離し ・現場作業時の鍵管理	鍵管理を社内手順に定め実施	左記手順に従い実施
8．物理的分離・電気的分離【2.8】	電源・ケーブル等の物理的分離，光変換器，絶縁増幅器の使用	機器の設計管理プロセス※２により受注者の実施内容を管理	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※３

[redacted]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。

※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…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…要求事項に従い設計を行い，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…設計内容を調達仕様に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。

※3　受注者の設計管理

当社が提示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。

別紙７　安全保護回路について，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

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。

別紙８　安全保護回路の検証及び妥当性確認について

安全保護回路のソフトウェアは，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「安全保護系へのディジタル計算機の適用に関する規程」（JEAC4620-2008）及び「ディジタル安全保護系の検証及び妥当性確認に関する指針」（JEAG4609-2008（以下「JEAG4609」という。））に準じた検証及び妥当性確認を実施する。

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）。

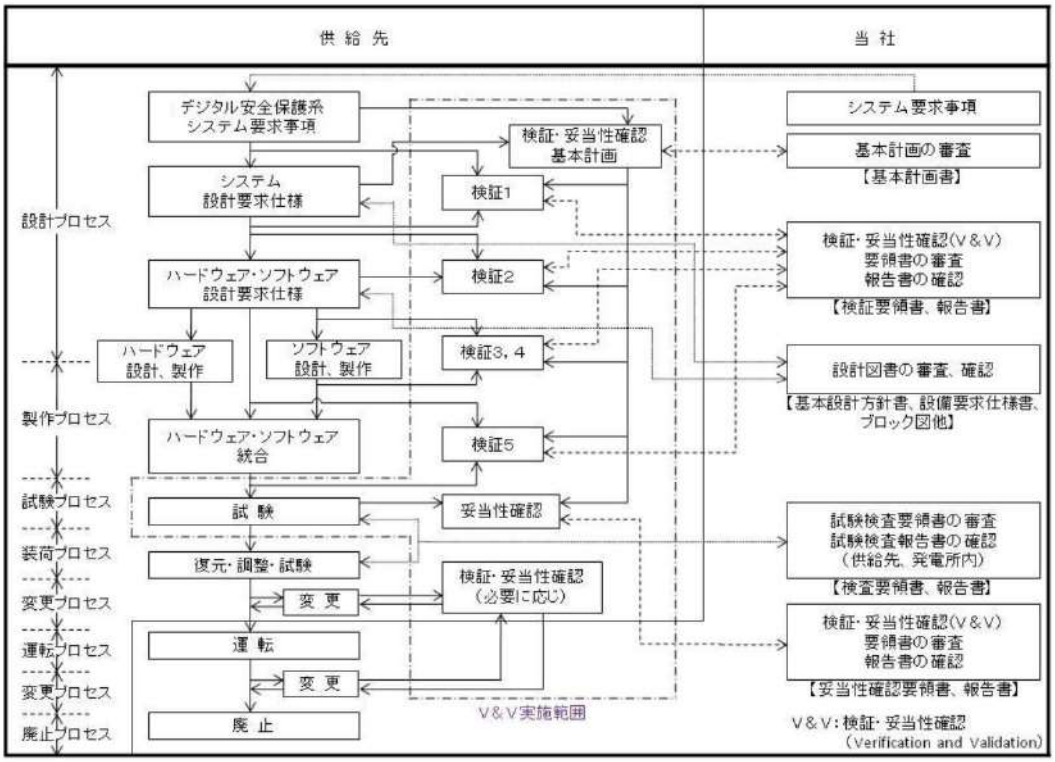
検証は，設計，製作過程のステップごとに上位仕様と下位仕様の整合性チェックを主体として，以下の観点から検証作業を行う。

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

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

ｃ．上記設計要求仕様に基づいてソフトウェアが製作されていること。

ｄ．検証及び妥当性確認が可能なソフトウェアとなっていること。必要な検証を経て製作されたソフトウェアをハードウェアと統合した後の全体システムについて，最終的に安全保護系システム要求事項が正しく実現されていることを確認するために妥当性確認を行う。



別紙 8-1 図　検証及び妥当性確認

別紙９　安全保護回路の構成

泊発電所３号炉の安全保護回路（安全保護系）は，原子炉停止回路（原子炉保護設備）及びその他の主要な安全保護回路（工学的安全施設作動設備）で構成している。

詳細は別紙 9-1 図のとおりであり，原子炉保護設備は，デジタル計算機である原子炉安全保護盤チャンネルⅠ～Ⅳにて構成され，工学的安全施設作動設備は，デジタル計算機である工学的安全施設作動盤トレンA，B及び安全系現場制御監視盤トレンA，Bにて構成される。

また，安全保護回路のプロセス計装の演算処理装置も，原子炉安全保護盤チャンネルⅠ～Ⅳにて構成されている。

泊発電所３号炉では，以上に示す安全保護回路のデジタル計算機に対して，「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設計」※とする。

※ 具体的には以下を意図している。

・不正アクセス行為

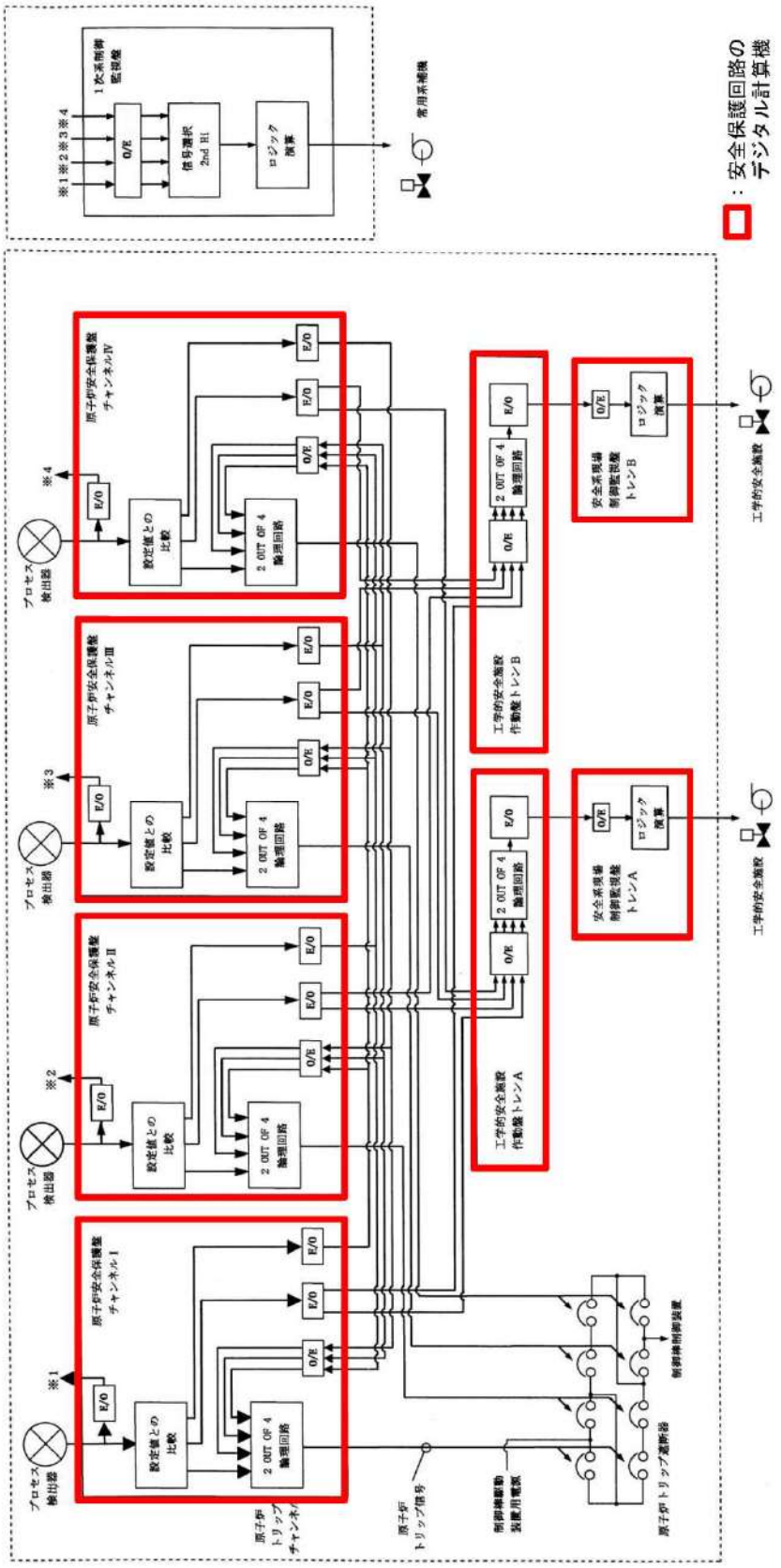
デジタル計算機に対して，管理されずに行われる物理的及び機能的アクセス行為のこと。

・電子計算機

デジタル計算機のこと。

・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

安全保護回路を不動作又は誤動作させる行為のこと。具体例として「不動作：プラントの異常時において，原子炉のトリップ動作を行う信号を発信させない行為」や「誤動作：プラントの正常運転時において，工学的安全施設の作動信号を発信させる行為」などがある。



別紙 9-1 図　安全保護回路の構成

別添

泊発電所３号炉

技術的能力説明資料
安全保護回路

第 24 条 安全保護回路

【追加要求事項】

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。

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。

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。

三　安全保護回路を構成する機械若しくは器具又はチャンネルは、単一故障が起きた場合又は使用状態からの単一の取り外しを行った場合において、安全保護機能を失わないよう、多重性を確保するものとすること。

四　安全保護回路を構成するチャンネルは、それぞれ互いに分離し、それぞれのチャンネル間において安全保護機能を失わないように独立性を確保するものとすること。

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。

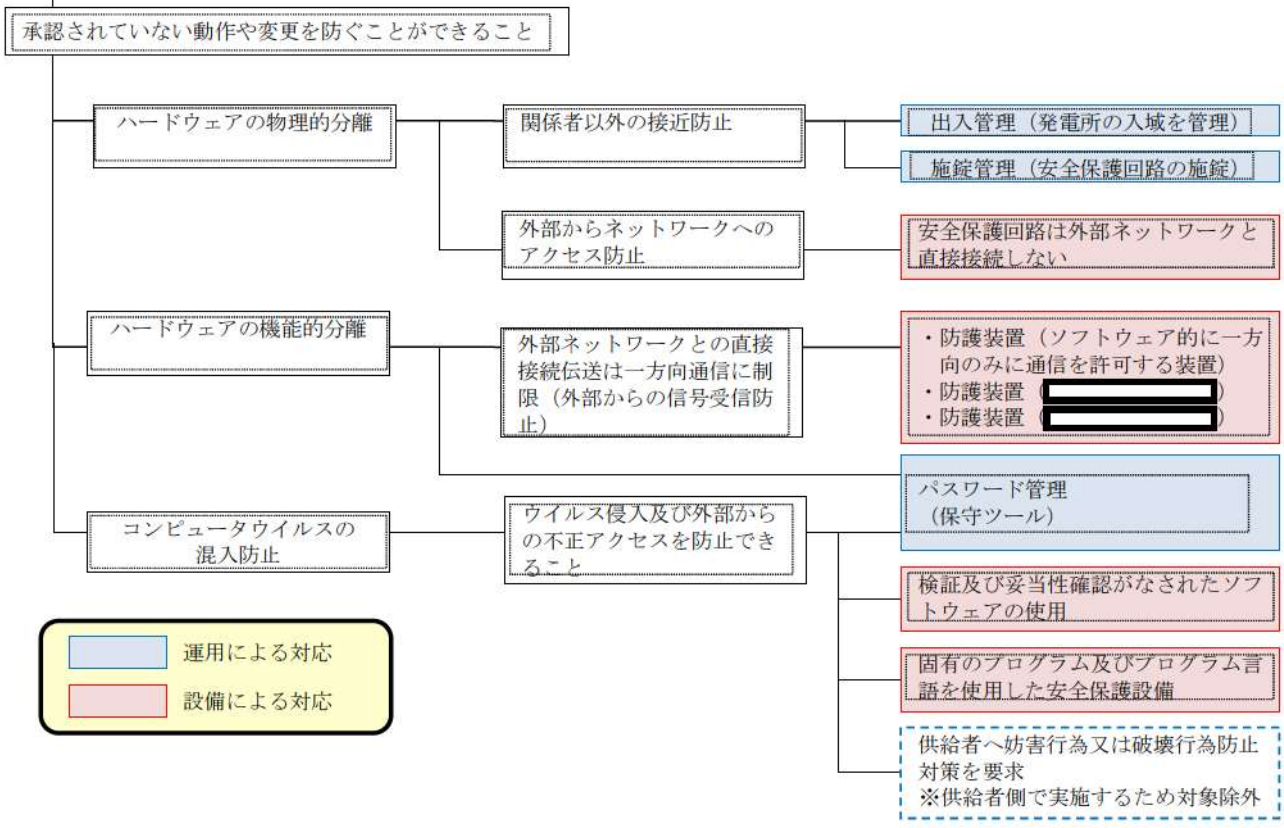
六　不正アクセス行為その他の電子計算機に使用目的に沿うべき動作をさせず、又は使用目的に反する動作をさせる行為による被害を防止することができるものとすること。

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。

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。

（解釈）

6　第６号に規定する「不正アクセス行為その他の電子計算機に使用目的に沿うべき動作をさせず、又は使用目的に反する動作をさせる行為による被害を防止すること」とは、ハードウェアの物理的分離、機能的分離に加え、システムの導入段階、更新段階又は試験段階でコンピュータウイルスが混入することを防止する等、承認されていない動作や変更を防ぐ設計のことをいう。



[redacted] 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。

技術的能力に係る運用対策等（設計基準）

【第 24 条 安全保護回路】

対象項目	区分	運用対策等
固有のプログラム及びプログラム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（安全保護回路の施錠）	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	－
	教育・訓練	施錠管理手順に関する教育を実施する。
パスワード管理（保守ツール）	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	パスワード管理及び入力操作に関する教育を実施する。
安全保護回路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。
	教育・訓練	補修に関する教育を実施する。
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。
・防護装置（ソフトウェア的に一方向のみに通信を許可する装置） ・防護装置（[redacted]） ・防護装置（[redacted]）	運用・手順	－
	体制	（保修課員による保守・点検）
	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。
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（検証及び妥当性確認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	（保修課員による管理）
	保守・点検	－
	教育・訓練	管理手順（検証及び妥当性確認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。

※外部からのアクセスができない対応を実施している。

[redacted] 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。