泊発電所３号炉審査資料	
資料番号	DB24　r.3.0
提出年月日	令和3年10月1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）

令和３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。

目　次

注：（　）内は重大事故等対処施設の該当条文

資料１

２４条：安全保護回路

＜目　次＞

＜概　要＞

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。

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。

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 24 条及び技術基準規則第 35 条において，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。	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 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

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。

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。

安全保護回路は，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。

安全保護回路の機能を果たす安全保護系のディジタル計算機は，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(2.1，2.2，2.3，2.4，2.5，2.6)】

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

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。

また，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，必要なものは記録できる設計とする。

(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。

(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。

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

工学的安全施設作動設備は，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．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設計とする。

(2)安全設計方針

1. 安全設計

1.1 安全設計の方針

1.1.5 安全保護回路設計の基本方針

原子炉停止系（トリップ機能）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回路は，原子炉保護設備及び工学的安全施設作動設備からなり，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。安全保護系は，原則として原子炉運転中に試験できる設計とする。また，安全保護系は，駆動源の喪失，系統の遮断等においても最終的に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。

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。

【説明資料（2.1，2.2，2.3，2.4，2.5，2.6）】

(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

安全保護系は，運転時の異常な過渡変化時に，中性子束，原子炉圧力等の変化を検出し，原子炉停止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ない設計とする。

なお，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，各チャンネルごと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）

第１項第６号について

安全保護系のディジタル計算機は，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) 安全保護系のディジタル計算機は，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) 安全保護系のディジタル計算機は，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) 安全保護系のディ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とともに，安全保護系のディ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。

【説明資料(2.1，2.2，2.3，2.4，2.5，2.6)】

第１項第７号について

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。

安全保護系の一部から計測制御系へ信号を取り出す場合には，信号の分岐箇所に絶縁回路

を設け，取り出し先の計測制御系での回路の短絡，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。

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，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。

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。

(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．設計基準事故時の監視

安全保護回路以外のプロセス計装は，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。

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，ディ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。

ディ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計測制御系に使用する場合には，計測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ため，絶縁回路により両者の間を絶縁する。

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，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，設計基準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，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。

j．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。

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。

1．プラント計算機

中央制御盤による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。

6.3.6　手順等

(1)　安全保護系のディ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)　発電所への出入については，出入管理方法を定め運用する。

(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)　適切に保守管理を実施するとともに，必要に応じ補修を行う。

(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。

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。

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。

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。

6.6.6　手順等

安全保護系の手順については，「6.3.6 手順等」に示す。

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。

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。

6.7.6 手順等

安全保護系の手順については，「6.3.6 手順等」に示す。

2.　安全保護回路

2.1　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，ディジタル化している安全保護設備（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，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。

2.2　安全保護設備の物理的分離

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。

安全保護設備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。

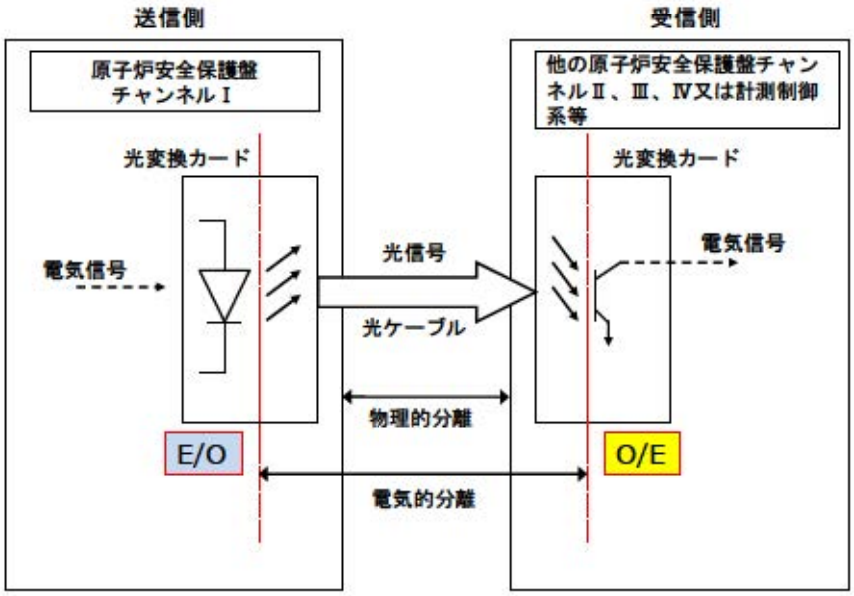


図１　光通信における分離概念図

2.3　安全保護設備の機能的分離

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，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。

2.4　コンピュータウイルスによる被害の防止

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。

さらに，ウイルスの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。

「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）

項目	確認項目
調達に係る対策	
システムの構成に係る対策	
システムの構成要素に係る対策	
アクセスの制御に係わる対策	
パスワードに係わる対策	
バックアップに係わる対策	
媒体に係わる対策	
セキュリティチェック	

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

□内の内容は機密事項に属しますので公開できません。

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

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関する規程に基づき適切に行うことで，高い信頼性を実現している。

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））

□内の内容は機密事項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。	
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

内の内容は機密事項に属しますので公開できません。

安全保護設備のディ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「安全保護系へのディ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（V＆V）を実施し，「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（V＆V）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。

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。

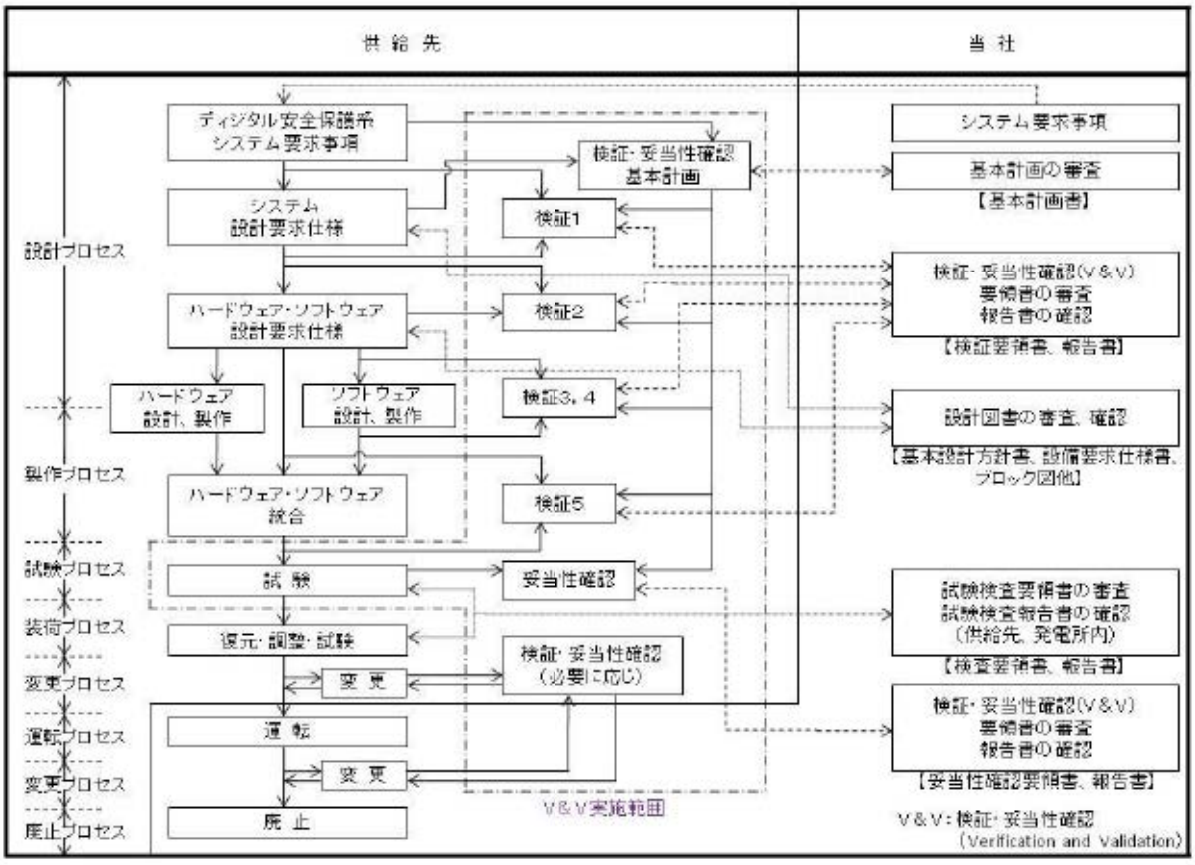


図２　安全保護設備の検証及び妥当性確認

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，ディ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

2.6　物理的及び電気的アクセスの制限

[redacted] 内の内容は機密事項に属しますので公開できません。

図３　不正アクセス防止の概念図

□内の内容は機密事項に属しますので公開できません。

2.7　安全保護設備の概要

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，原子炉停止信号を発信し，また，工学的安全施設作動に係わる信号を工学的安全施設作動盤へ発信する設備である。

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。

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。

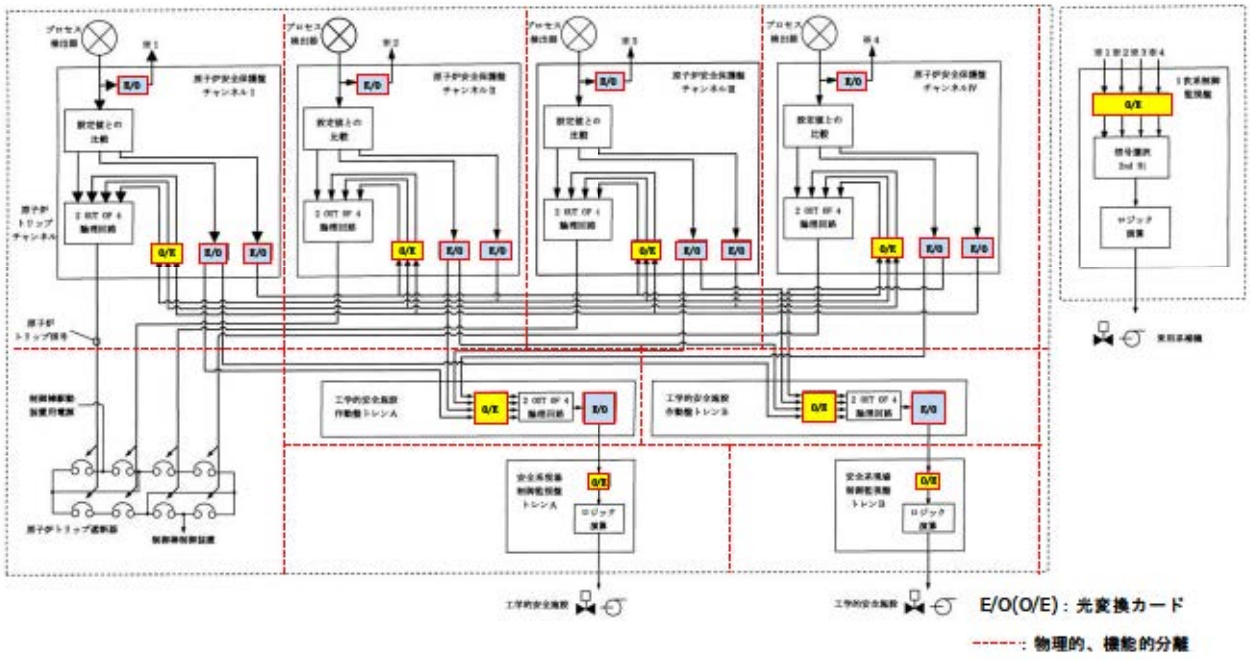
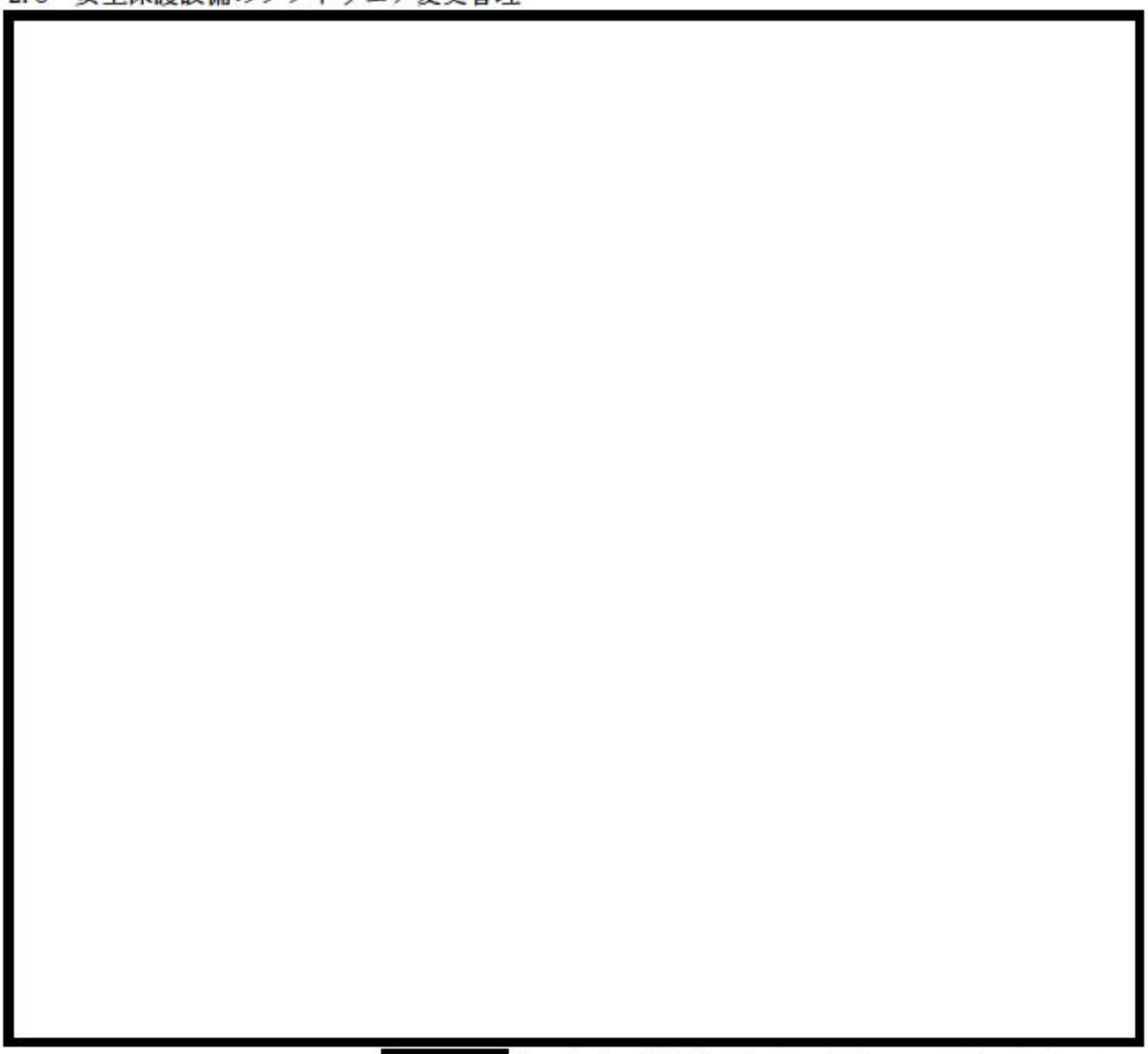


図４　安全保護設備の構成

2.8　安全保護設備のソフトウェア変更管理



内の内容は機密事項に属しますので公開できません。

2.9　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 1000-4-4，電波障害試験／参考規格 JIS C 1000-4-3 等）

別添１

泊発電所３号炉

技術的能力説明資料
安全保護回路

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。

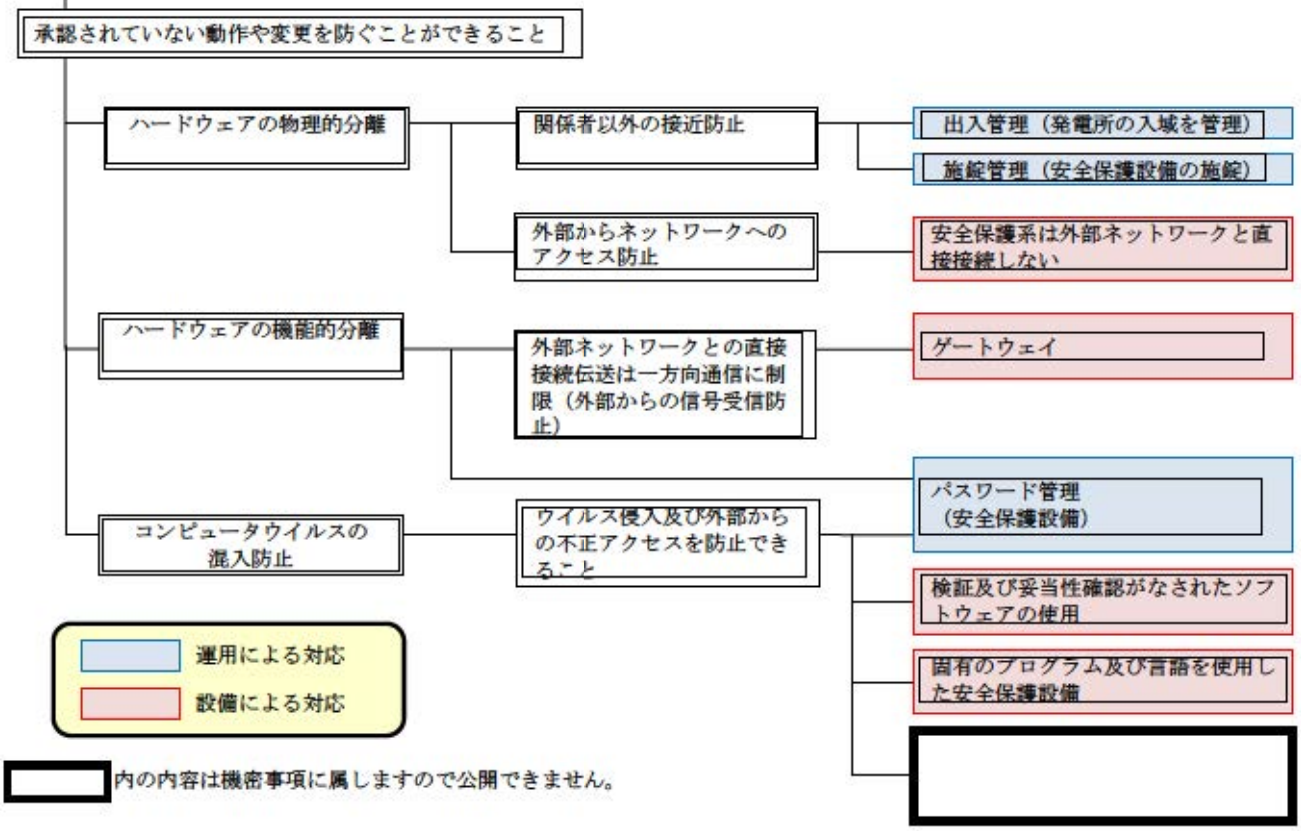
六　不正アクセス行為その他の電子計算機に使用目的に沿うべき動作をさせず、又は使用目的に反する動作をさせる行為による被害を防止することができるものとすること。

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。



技術的能力に係る運用対策等（設計基準）

【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	－
	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（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	－
	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。
	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。
ゲートウェイ	運用・手順	－
	体制	（保修課員によるゲートウェイの保守・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。