資料１－３－１

東海第二発電所

安全保護回路

平成 29 年 7 月

日本原子力発電株式会社

本資料のうち，□は商業機密又は核物質防護上の観点から公開できません。

第 24 条　安全保護回路

＜目　次＞

セキュリティ対策

別紙５　安全保護回路のうちデジタル部分のシステムへ接続可能なアクセスについて

別紙６　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

別紙７　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

3.　運用，手順説明資料

（別添資料）安全保護回路

＜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東海第二発電所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運用，手順等を抽出し，必要となる対策等を整理する。

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。（第1.1表）

第 1.1 表　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。	変更なし
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じる場合において，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。	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
—	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，及び原子炉緊急停止系その他系統と併せて機能することにより，燃料の許容設計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，原子炉緊急停止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。

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。

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ことで，不正アクセス行為をさせず，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-32,33）（2.2：P24 条-33,34）（2.3：P24 条-35）（2.4：P24 条-36）（2.5：P24 条-37）（2.6：P24-37,38）】

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。

ヘ　計測制御系統施設の構造及び設備

(2)　安全保護回路

安全保護回路（安全保護系）は，「原子炉停止回路（原子炉緊急停止系作動回路）」及び「その他の主要な安全保護回路（工学的安全施設作動回路）」で構成する。

安全保護回路は，不正アクセス行為をさせず，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-32,33）（2.2：P24条-33,34）（2.3：P24条-35）（2.4：P24条-36）（2.5：P24条-37）（2.6：P24-37,38）】

（ｉ）　原子炉停止回路の種類

原子炉停止回路（原子炉緊急停止系作動回路）は，次に示す条件により原子炉をスクラムさせるため，2つの独立のチャンネルが設けられ，これらの同時動作によって原子炉をスクラムさせる。

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．原子炉出力ペリオド短（起動領域計装）

ｅ．中性子束高（起動及び出力領域計装）

ｆ．中性子束指示低（出力領域計装）

ｇ．中性子計装動作不能（起動及び出力領域計装）

ｈ．スクラム・ディスチャージ・ボリューム水位高

ｉ．主蒸気隔離弁閉

ｊ．主蒸気管放射能高

ｋ．主蒸気止め弁閉

ｌ．蒸気加減弁急速閉（ＥＨＣ油圧低）

ｍ．地震加速度大

ｎ．原子炉モード・スイッチ「停止」の位置

ｏ．手　　動

なお，原子炉停止回路の電源喪失の場合にも原子炉はスクラムする。

（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回路）には，次のものを設ける。

ａ．原子炉水位異常低下，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，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

ｂ．ドライウェル圧力高，原子炉水位低，原子炉建屋放射能高のいずれかの信号による原子炉建屋常用換気系の閉鎖と原子炉建屋ガス処理系の起動

ｃ．原子炉水位異常低下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

ｄ．原子炉水位異常低下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

e．原子炉水位異常低下又はドライウェル圧力高の信号による非常用ディーゼル発電機の起動

f．原子炉水位低，原子炉水位異常低下，ドライウェル圧力高のいずれかの信号による主蒸気隔離弁以外の隔離弁の閉鎖

(2)　安全設計方針

1.1.5　計測制御系統施設設計の基本方針

1.1.5.1　原子炉出力制御系

運転及び制御保護動作に必要な中性子束，温度，圧力等を測定する核計装及び原子炉プラント・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出力制御系を設ける。

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，警報を発信する装置を設ける。

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　安全保護系

(1)　原子炉緊急停止系作動回路

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，原子炉スクラムを行うために原子炉緊急停止系を設ける。原子炉緊急停止系作動回路は，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，これらの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。

(2)　工学的安全施設作動回路

原子炉冷却材喪失等の設計基準事故時に，炉心及び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回路を設ける。工学的安全施設作動回路は，原子炉緊急停止系作動回路と同様に高い信頼性が得られるよう設計する。

1.1.5.4　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-32,33）（2.2：P24 条-33,34）（2.3：P24 条-35）（2.4：P24 条-36）（2.5：P24 条-37）（2.6：P24-37,38）】

(3)　適合性説明

（安全保護回路）

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。

適合のための設計方針

第１項第１号について

(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，原子炉緊急停止系を含む適切な系統の作動を自動的に開始させ，燃料の許容設計限界を超えることがないように設計する。

(2)　安全保護系は，偶発的な制御棒引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異常な反応度印加が生じた場合でも，燃料の許容設計限界を超えないよう，中性子束高スクラム及び原子炉出力ペリオド短スクラムにより原子炉を停止できるように設計する。

第１項第２号について

安全保護系は，設計基準事故時に異常状態を検知し，原子炉緊急停止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，原子炉建屋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。

(1)　発電用原子炉は，下記の条件の場合にスクラムする。

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．原子炉出力ペリオド短（起動領域計装）

ｅ．中性子束高（起動及び出力領域計装）

ｆ．中性子束指示低（出力領域計装）

ｇ．中性子計装動作不能（起動及び出力領域計装）

ｈ．スクラム・ディスチャージ・ボリューム水位高

ｉ．主蒸気隔離弁閉

ｊ．主蒸気管放射能高

ｋ．主蒸気止め弁閉

ｌ．蒸気加減弁急速閉（ＥＨＣ油圧低）

ｍ．地震加速度大

ｎ．原子炉モード・スイッチ「停止」の位置

ｏ．手　　動

(2)　その他主要な安全保護系（工学的安全施設作動回路）には，次のようなものを設ける。

ａ．原子炉水位異常低下，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，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

ｂ．ドライウェル圧力高，原子炉水位低，原子炉建屋放射能高のいずれかの信号による原子炉建屋常用換気系の閉鎖と原子炉建屋ガス処理系の起動

ｃ．原子炉水位異常低下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

ｄ．原子炉水位異常低下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

ｅ．原子炉水位異常低下又はドライウェル圧力高の信号による非常用ディ

ーゼル発電機の起動

ｆ．原子炉水位低，原子炉水位異常低下，ドライウェル圧力高のいずれかの信号による主蒸気隔離弁以外の隔離弁の閉鎖

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少なくとも2チャンネルの保護回路で構成し，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り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。

具体例は下記のとおりである。

(1) 原子炉緊急停止系作動回路は，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。

安全保護機能を維持するため，原子炉緊急停止系作動回路は，運転中すべて励磁状態であり，電源の喪失，継電器の断線及び検出器を取外した場合，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。

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。

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。

(2) 第１項第２号の(2)項に示す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。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。

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，独立性を持つ設計とする。

具体例は下記のとおりである。

(1) 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。

(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) 原子炉緊急停止系動作回路の電源は，分離・独立した母線から供給する。

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計器用空気を使用する。この系統に使用する弁等は，フェイル・セイフの設計とするか，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保護動作を行うことができる設計とする。

フェイル・セイフとなる主要なものは以下のとおりである。

(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)　計器用空気喪失

ａ．スクラム

ｂ．格納容器ベント弁閉

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。

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

安全保護系のアナログ回路は，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し，外部からの不正アクセスを防止する設計とする。

また，発電所での出入管理による物理的アクセスの制限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。

【説明資料（2.1：P24条-32,33）（2.2：P24条-33,34）（2.3：P24条-35）（2.4：P24条-36）（2.5：P24条-37）（2.6：P24-37,38）】

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，ケーブル・ルート及び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。

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。

また，核計装等の検出部が表示，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。

1.3　気象等

該当なし

1.4　設備等（手順等含む）

6.　計測制御系統施設

6.3　原子炉計測制御系

6.3.2　安全保護系

6.3.2.1　概　要

安全保護系は，原子炉の安全性を損なうおそれのある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は，原子炉及び発電所の保護のための制御棒の緊急挿入（スクラム）機能，その他の保護動作（非常用炉心冷却系起動等を含む。）を有する。また，安全保護系を構成するチャンネルは，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とともに，原子炉運転中においても試験が可能な設計とする。

6.3.2.2　設計方針

(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，原子炉緊急停止系を含む適切な系統を自動的に作動させ，燃料の許容設計限界を超えないようにする。

(2)　安全保護系は，偶発的な制御棒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対しても，燃料の許容設計限界を超えないようにする。

(3)　安全保護系は，事故時にあっては，直ちにこれを検知し，原子炉停止系及び工学的安全施設の作動を自動的に開始させる。

(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，機器の単一故障若しくは使用状態からの単一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。

(5)　安全保護系は，系統の遮断，駆動源の喪失においても，フェイル・セイフの設計とするか，又は故障と同時に現状維持（フェイル・アズ・イズ）とし，安全上許容される状態になるようにする。

(6)　安全保護系は，計測制御系とは極力分離し，部分的に共用した場合でも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。

(7)　安全保護系の電源は，原子炉保護系用Ｍ－Ｇ装置（はずみ車付）又は所内常設直流電源設備から給電する設計とする。

(8)　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。

(9)　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。

(10)　安全保護系は，不正アクセス行為その他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-32,33）（2.2：P24 条-33,34）（2.3：P24 条-35）
（2.4：P24 条-36）（2.5：P24 条-37）（2.6：P24-37,38）】

6.3.2.3　主要設備の仕様

(1)　原子炉緊急停止系　　第 6.3－1 表，第 6.3－2 図，第 6.3－3 図及び第 6.3－5 図

(2)　その他の主要な安全保護系　　第 6.3－2 表，第 6.3－6 図及び第 6.3－7 図

6.3.2.4　主要設備

(1)　原子炉緊急停止系の機能

原子炉緊急停止系は，第 6.3－2 図に示すように 2 チャンネルで構成され各チャンネルには，1 つの測定変数に対して少なくとも 2 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に対して，原子炉がスクラムされるようになっている。

原子炉は，下記の条件の場合にスクラムされる。

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．原子炉出力ペリオド短（起動領域計装）

ｅ．中性子束高（起動及び出力領域計装）

ｆ．中性子束指示低（出力領域計装）

ｇ．中性子計装動作不能（起動及び出力領域計装）

ｈ．スクラム・ディスチャージ・ボリューム水位高

ｉ．主蒸気隔離弁閉

ｊ．主蒸気管放射能高

ｋ．主蒸気止め弁閉

ｌ．蒸気加減弁急速閉（ＥＨＣ油圧低）

ｍ．地震加速度大

ｎ．原子炉モード・スイッチ「停止」の位置

ｏ．手　　動

検出器の形式，配置場所及びスクラム設定値は，第 6.3－1 表に示すとおりである。

この他，原子炉緊急停止回路の電源喪失の場合にも原子炉はスクラムする。

なお，原子炉モード・スイッチによって安全保護系の回路は以下のようにバイパスされる。

(a)　「停止」このモードでは，スクラム信号が出され，全制御棒が炉内に挿入される。このモードにしてから約 10 秒程度で自動的にスクラム信号のリセットが可能となる。また，主蒸気隔離弁閉のスクラム信号は原子炉圧力が約 4.13MPa［gage］以下のときには自動的にバイパスされ，スクラム・ディスチャージ・ボリューム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。

(b)　「燃料取替」このモードではスクラム回路は動作状態にあるが，主蒸気隔離弁閉のスクラム信号は原子炉圧力が約 4.13MPa［gage］以下のときは自動的にバイパスされる。さらに，スクラム・ディスチャージ・ボリューム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き抜くことはできない。

(c)　「起動」このモードは原子炉を起動し，最高で定格の約 5%まで出力をあげる場合に適用される。また，主蒸気隔離弁が閉で，かつタービン補機が動作している状態で，原子炉を臨界に保つ時にも適用される。このモードでは，主蒸気隔離弁閉のスクラム信号は原子炉圧力が約 4.13MPa［gage］以下のときには自動的にバイパスされる。

(d)　「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にのみ保守上の目的で，個々の計器をバイパスさせることができる。

(2)　その他の主要な安全保護系の種類

その他の主要な安全保護系には，次のようなものが設けられる。

a．原子炉水位異常低下，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，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

b．ドライウェル圧力高，原子炉水位低，原子炉建屋放射能高のいずれかの信号による原子炉建屋常用換気系の閉鎖と原子炉建屋ガス処理系の起動

c．原子炉水位異常低下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

d．原子炉水位異常低下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

e．原子炉水位異常低下又はドライウェル圧力高の信号による非常用ディーゼル発電機の起動

f．原子炉水位低，原子炉水位異常低下，ドライウェル圧力高のいずれかの信号による主蒸気隔離弁以外の隔離弁の閉鎖

(3)　原子炉緊急停止系の動作

原子炉緊急停止系は二重チャンネル，継電器方式の構成で，論理回路及びスクラム・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ている。

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，すべて運転中励磁状態にあり，コイルの断線又は短絡，あるいは導線の断線

等の継電器の故障の大部分は，継電器自体を非励磁状態に戻し，回路が不動作状態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・セイフ”になっている。

一方，接点の焼損又は溶着等“フェイル・セイフ”に反する方向の故障に対しては，各接点を流れる電流が定格の 50%以下であるように制限することによって，その発生を防止するようにしている。

第 6.3－2 図に示すように，論理回路の継電器接点はすべて直列につながれているので，どの継電器でも 1 個が非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阻止されることになる。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 2 つずつ直列につないで，継電器接点が 1 つ単独で故障して開かない場合でも，スクラム動作を妨げないようにしている。

主蒸気隔離弁の閉鎖及びそのほかの補助保護機能の作動開始には，別の継電器が使用されている。

主スクラム弁への計器用空気の制御には，ソレノイド作動スクラム・パイロット弁を使用する。このパイロット弁は，3 方向形で，各制御棒駆動機構のスクラム弁に対して，2 つのソレノイドの 1 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なっている。両パイロット弁のソレノイドが非励磁になれば，スクラム弁ダイヤフラムの空気圧がなくなって弁は開き，制御棒を挿入することになる。各駆動機構に 2 つずつあるソレノイドは，2 チャンネルに接続されるので，両チャンネルがトリップすれば，原子炉はスクラムされるが，単一チャンネルのトリップではスクラムされない。

緊急停止系統の試験は，一度に 1 つずつのチャンネルを各検出器でトリップさせることによって，原子炉運転中でも定期的に行うことができる。

この試験によって，スクラム・パイロット弁までのあらゆる機能をチェックすることができる。

(4)　リセット及び警報

いずれか一方のチャンネルがトリップすれば，ロック・アウトされ警報が出る。この場合スクラム・パイロット弁を再励磁するためには，手動でリセットしなければならない。個々のトリップ信号の警報によって，運転員はチャンネル・トリップあるいはスクラムの原因を確認することが可能であり，また運転監視補助装置が，各検出器トリップの時間的順序を記録する。

(5)　後備緊急停止系統

スクラム・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，制御棒が確実に挿入されるように，計器用空気系統に 2 個の 3 方向ソレノイド後備緊急停止弁を設けている。このソレノイドは直流回路に接続されていて，通常時は無励磁状態にある。原子炉緊急停止系の 2 チャンネルの主トリップ継電器の消勢によって，2 個の後備緊急停止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は，後備緊急停止弁の動作によってスクラム弁への空気圧がなくなる。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が原子炉を停止させる場合，1 本の制御棒の挿入が遅れても，他の制御棒が挿入できれば十分なので，たとえ後備緊急停止弁がなくても安全に停止することができる。

(6)　原子炉緊急停止系の電源回路

原子炉緊急停止系の電源回路は，第 6.3－3 図に示されている。原子炉緊急停止系の各チャンネルは，原子炉保護系用Ｍ－Ｇ装置（はずみ車付）に接続されていて，各電動機は所内電気系の別々の 480V 交流電源に接続されている。はずみ車の保有エネルギが大きいので，瞬間的な電圧降下で

は原子炉スクラムは生じない。

ＭＧセットを保守のため取り外すことができるように，バイパス変圧器からも電力を供給できるようになっている。

6.3.2.5　試験検査

(1)　原子炉緊急停止系は，原則として原子炉運転中でも次の試験ができ，定期的にその機能が喪失していないことを確認できる。

ａ．手動スクラム・パイロット弁作動試験：各チャンネルの手動スクラム・スイッチによるスクラム・パイロット弁の作動の確認

ｂ．自動スクラム・パイロット弁作動試験：各チャンネルごとの鍵付テスト・スイッチによるスクラム・パイロット弁の作動の確認

ｃ．検出器作動試験：各検出器の校正用タップ及び各検出器の信号入力回路から校正用模擬信号を入れることによるスクラム・パイロット弁の作動の確認

また，各制御棒のスクラム時間の確認のための制御棒スクラム試験は，原子炉停止時に行うことができる。

(2)　その他の主要な安全保護系は，原則として原子炉運転中でも各検出器の校正用タップ及び各検出器の信号入力回路から校正用模擬信号を入れることにより，各チャンネルの作動の確認を行うことができ，その機能が喪失していないことを確認できる。なお，論理回路を含む全系統の試験については，原子炉停止時に行うことができる。

6.3.4　原子炉プラント・プロセス計装

6.3.4.1　概　　要

原子炉の適切かつ安全な運転のため，核計装のほかに，原子炉施設の重要

な部分には，すべ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，すべて中央制御室に設置する。

原子炉プラント・プロセス計装は，原子炉圧力容器計装，再循環回路計装，原子炉給水系及び蒸気系計装，制御棒駆動機構計装及びそのほかの計装から構成されている。

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。

6.3.4.2　設計方針

(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プロセス計装を設ける。

(2)　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に，プロセス計装を設ける。

(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，「6.3.2　安全保護系」に記載する設計方針(4)～(10)を満足するように設計する。

(4)　原子炉冷却材圧力バウンダリからの原子炉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。

6.3.4.3　主要設備

(1)　原子炉圧力容器計装

原子炉圧力容器について計測する必要のある項目は，水位，圧力，容器

胴部の温度及びフランジ・シール漏えいである。

原子炉水位は差圧形検出器で連続的に測定され，指示及び記録される。水位高及び水位低で警報が出され，水位低下が更に大きい場合には，原子炉スクラム信号が出される。原子炉圧力は圧力検出器で測定され，指示及び記録される。原子炉圧力高でスクラム信号が出される。

原子炉圧力容器壁の温度は熱電対によって測定され，記録される。この記録を基にして，原子炉冷却材の加熱及び冷却を行う。

原子炉容器上蓋のフランジ部シールの漏えいは，2個のOリング間のフランジ面に接続されたドレン・ラインで連続的にモニタされる。通常ドレン・ラインは閉鎖されているが，内側Oリングからの漏えい水は，レベル・スイッチ・チェンバに集められ，水位高で警報が出される。また，ドレン・ラインの圧力が測定及び指示され，圧力高で警報が出される。

(2)　再循環回路計装

外部の再循環回路では，再循環流量，冷却材温度，ポンプ出入口差圧及び流量制御弁開度が連続的に測定され指示される。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って測定される。再循環ポンプについては，シール漏えい量，冷却水流量及び温度が計測され，シール漏えい流量高及び低，並びに原子炉補機冷却系流量低で警報が出される。

(3)　原子炉給水系及び蒸気系計装

原子炉給水流量及び蒸気流量は，フロー・ノズルによって連続的に測定され，指示及び記録される。これらは温度及び圧力補償が行われた後，三要素式原子炉水位制御用の信号として用いられる。

そのほか，給水温度，タービン第一段圧力などが測定され，指示及び記録される。

(4)　制御棒駆動機構計装

制御棒駆動機構計装は，駆動冷却材の供給系，通常の駆動水圧系，スクラム・アキュムレータ及びスクラム・ディスチャージ・ボリューム，並びに制御棒位置の指示に対して，それぞれ適当なプロセス計装が設けられている。

駆動冷却材の供給系では，駆動ポンプ出口圧力，フィルタでの圧力降下などが計測される。

通常の駆動水圧系では，原子炉と駆動水圧系との差圧，駆動ヘッダの流量と制御棒駆動機構の温度（位置指示用計器ウェル内）などが計測される。

スクラム・アキュムレータ及びディスチャージ・ボリューム系では，アキュムレータ窒素圧力，アキュムレータの漏えい水量，ディスチャージ・ボリューム水位などが計測され，アキュムレータの圧力低と水位高，ディスチャージ・ボリュームの水位高で警報が出される。ディスチャージ・ボリュームの水位が更に高くなれば，原子炉はスクラムされる。

制御棒位置は，駆動機構の中心部に設けられた計器ウェル内のリード・スイッチによって測定指示される。

(5)　漏えい検出系計装

原子炉冷却材圧力バウンダリからの原子炉冷却材の漏えいは，ドライウェル内ガス冷却装置のドレン量，格納容器内サンプ水量の測定により約3.8L／min の漏えいを 1 時間以内に検出できるようにする。また，格納容器内雰囲気中の核分裂生成物の放射性物質濃度の測定によっても漏えいを検出できるようにする。測定値は，指示するとともに，原子炉冷却材の漏えい量が多い場合には警報を出す。

(6)　燃料貯蔵設備計装

使用済燃料プール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プールの状態を示す事項を監視できる設計とする。

(7) その他の原子炉プラント・プロセス計装

ドライウェル及びサプレッション・チェンバ系では，ドライウェル圧力及びサプレッション・プールの水温及び水位が計測され，ドライウェル圧力高で原子炉はスクラムされる。

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が計測され，タンク水位低，ポンプ出口圧力低等で警報が出される。

高圧炉心スプレイ系，低圧炉心スプレイ系及び残留熱除去系では，ポンプ出口圧力及びサプレッション・プール水位が計測される。

(8) 記録及び保存

安全保護系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。

(9) プロセス計算機

中央制御室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ロセス計算機を設け，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。

6.3.4.4 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。

6.3.2.5　手順等

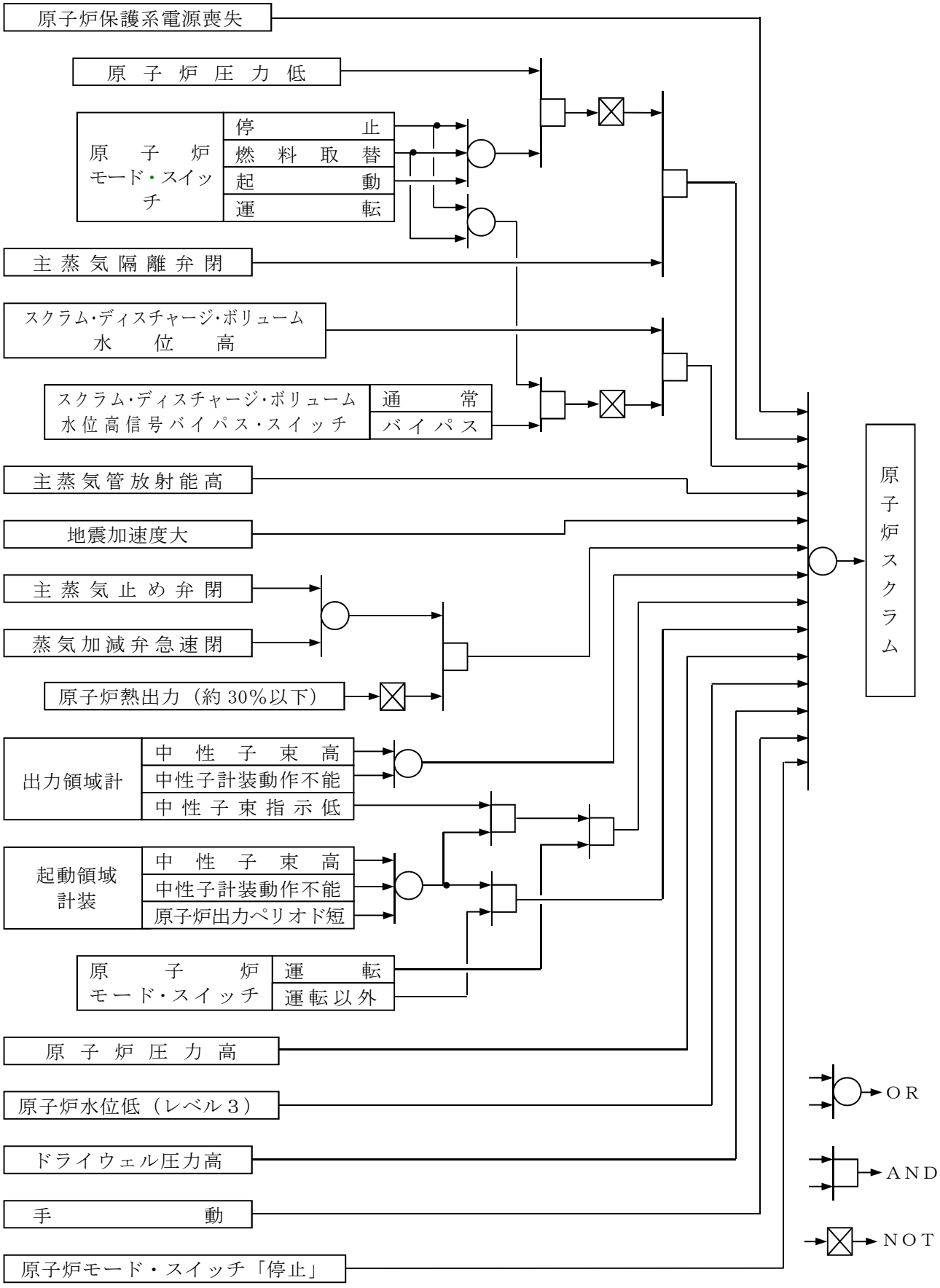
安全保護系に関して，以下の内容を含む手順等を定める。

(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る。

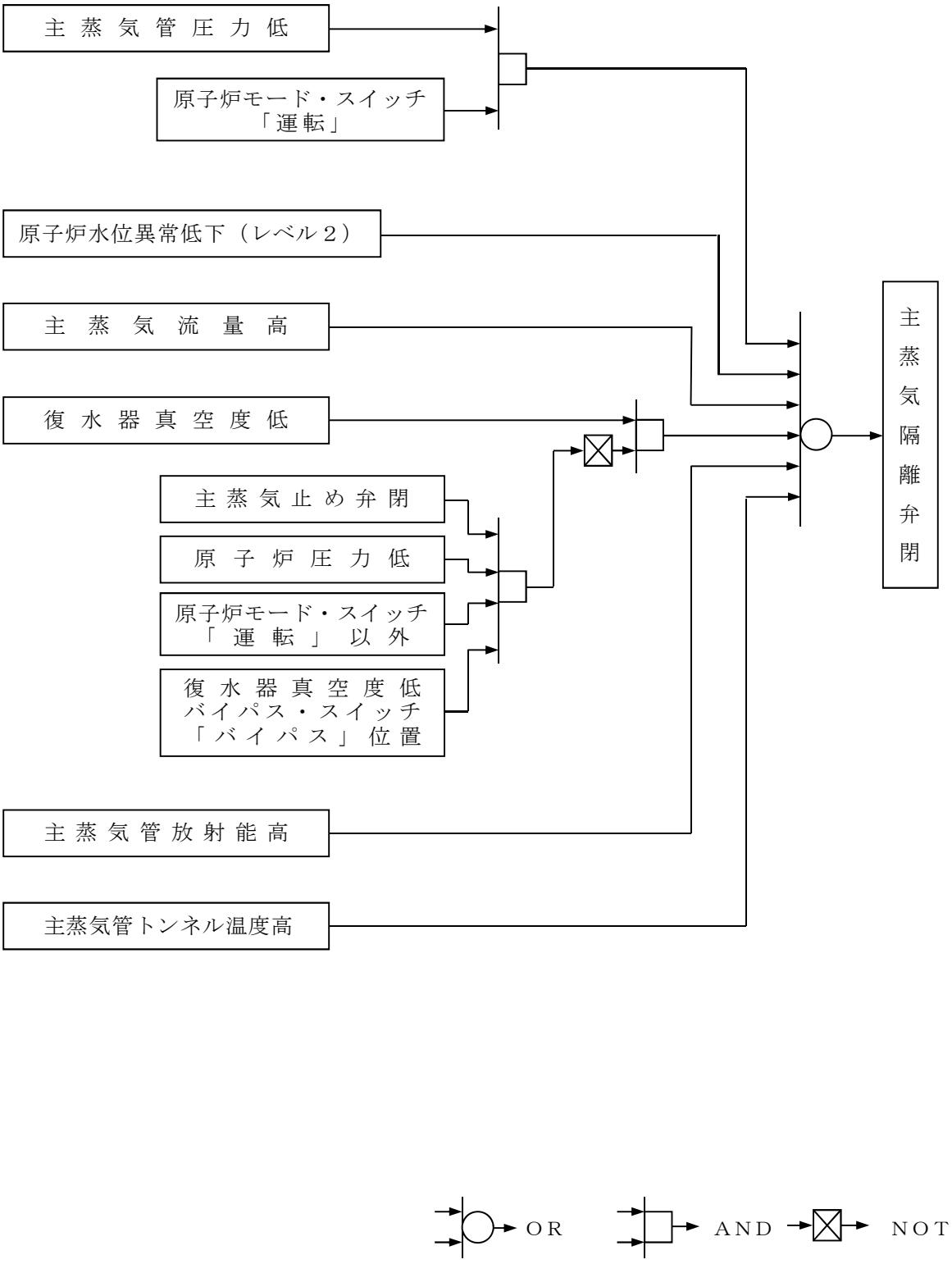
(2)　発電所の出入管理方法については，「1.1　安全設計の方針　1.1.1.5 人の不法な侵入等の防止(3)手順等」に示す。

第 6.3－2 表　その他の主要な安全保護系作動信号一覧表

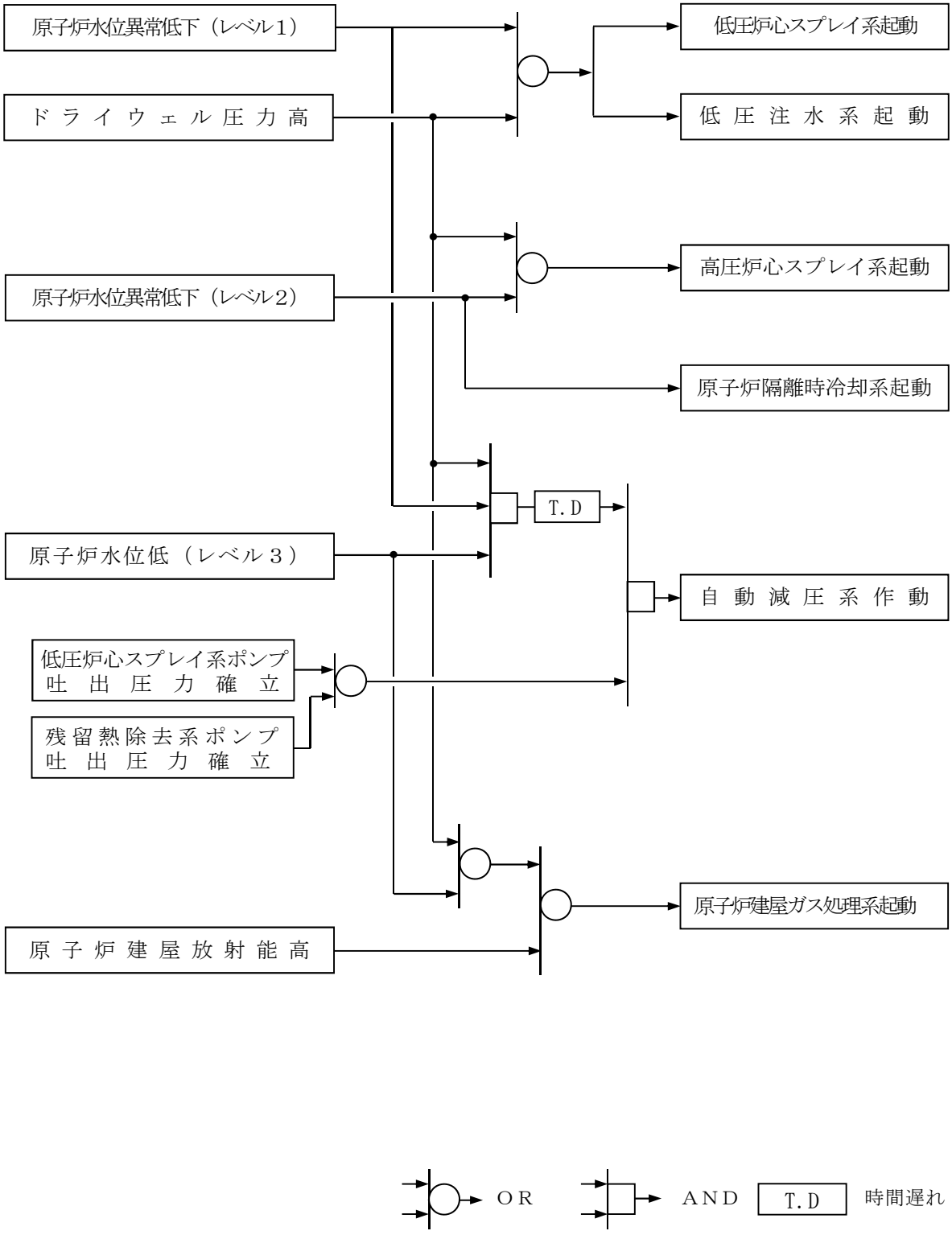
信　号　の　種　類	保護機能の種類	設　定　値
原　子　炉　水　位　低	原子炉建屋ガス処理系起動	1,370cm （ベッセルゼロより上） （レベル３）
原子炉水位異常低下	主蒸気隔離弁閉鎖 高圧炉心スプレイ系起動 原子炉隔離時冷却系起動	1,245cm （ベッセルゼロより上） （レベル２）
	低圧炉心スプレイ系起動 低圧注水系起動 自動減圧系作動	960cm （ベッセルゼロより上） （レベル１）
ドライウェル圧力高	低圧炉心スプレイ系起動 低圧注水系起動 高圧炉心スプレイ系起動 自動減圧系作動 原子炉建屋ガス処理系起動	13.7kPa［gage］
主　蒸　気　管　圧　力　低	主蒸気隔離弁閉鎖	5.89MPa［gage］
主　蒸　気　流　量　高	主蒸気隔離弁閉鎖	定格流量の 140％相当
復　水　器　真　空　度　低	主蒸気隔離弁閉鎖	真空度 24.0kPa
主蒸気管放射能高	主蒸気隔離弁閉鎖	通常運転時の放射能の 10 倍以下
主蒸気管トンネル温度高	主蒸気隔離弁閉鎖	93℃
原子炉建屋放射能高	原子炉建屋ガス処理系起動	通常運転時の放射能の 10 倍以下



第 6.3－5 図　原子炉緊急停止系機能説明図



第 6.3－6 図　その他の主要な安全保護系機能説明図（その１）



第 6.3－7 図　その他の主要な安全保護系機能説明図（その２）

2.　安全保護回路

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（原子炉緊急停止系，工学的安全施設作動回路）のうちデジタル処理部のある機器については，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し，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とし，デジタル処理部を持つ機器からデータを採取するデータ収集端末にはデジタル処理を行う演算回路からのデータ受信機能のみを設けるとともに，データ収集端末を施錠管理された場所に保管することで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→プロセス計算機・データ伝送装置→防護装置→緊急時対策支援システム伝送装置→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，安全保護回路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。

(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。

※データダイオード装置（ハードウェアレベルでダイオードのように片方向のみ通信を許可する装置）により一方向通信に制限する。

(4)　システムの導入段階，更新段階または試験段階で承認されていない動作や変更を防ぐ対策

安全保護回路のうちデジタル処理部を持つ機器は，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や設定値変更作業での鍵管理及びパスワード管理を行い，関係者以外の不正な変更等を防止している。

(5)　耐ノイズ・サージ対策

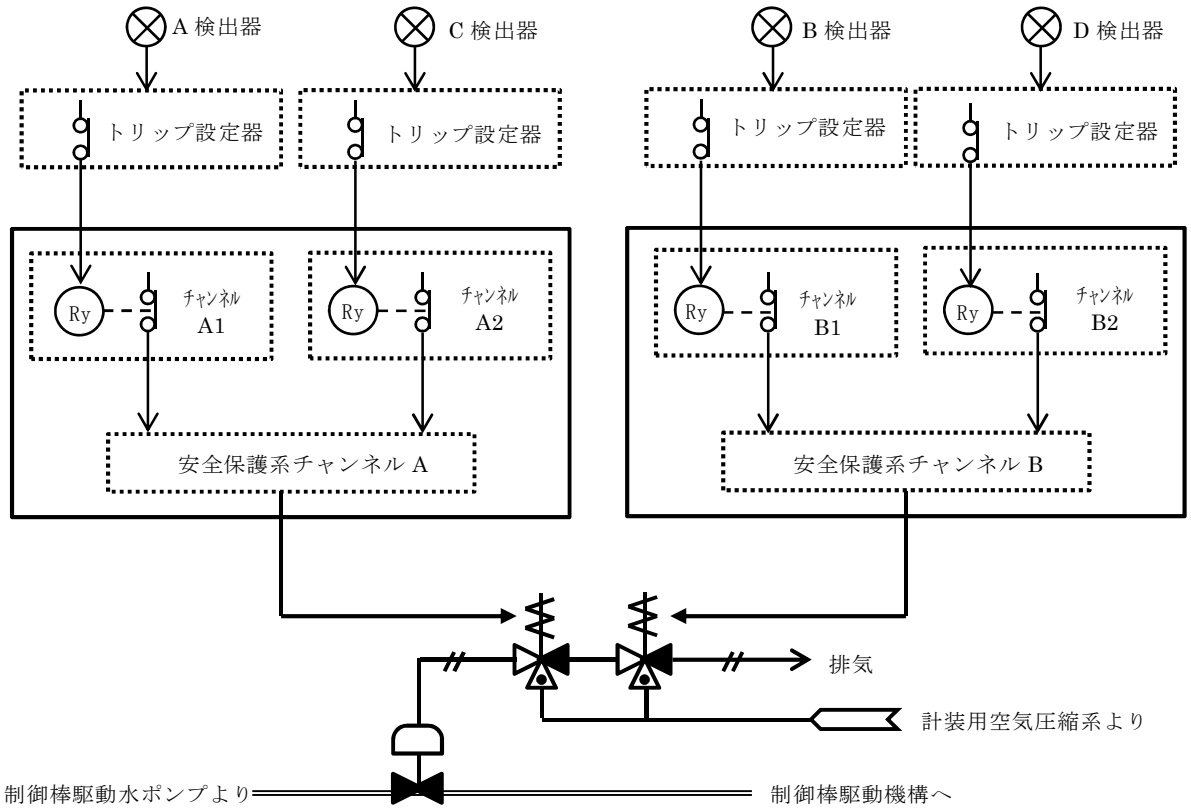
安全保護回路は，雷・誘導サージ・電磁波障害等による擾乱に対して，制御盤へ入線する電源受電部及びケーブルからの信号入出力部にラインフィルタや絶縁回路を設置している。

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。

2.2　安全保護回路の概要

安全保護回路の検出器はアナログ機器，論理回路はハードワイヤーロジック（補助継電器や配線等）で構成されており，ソフトウェアを用いないアナログ回路である。従って，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。例として，原子炉緊急停止系の構成例を第2.2図に示す。

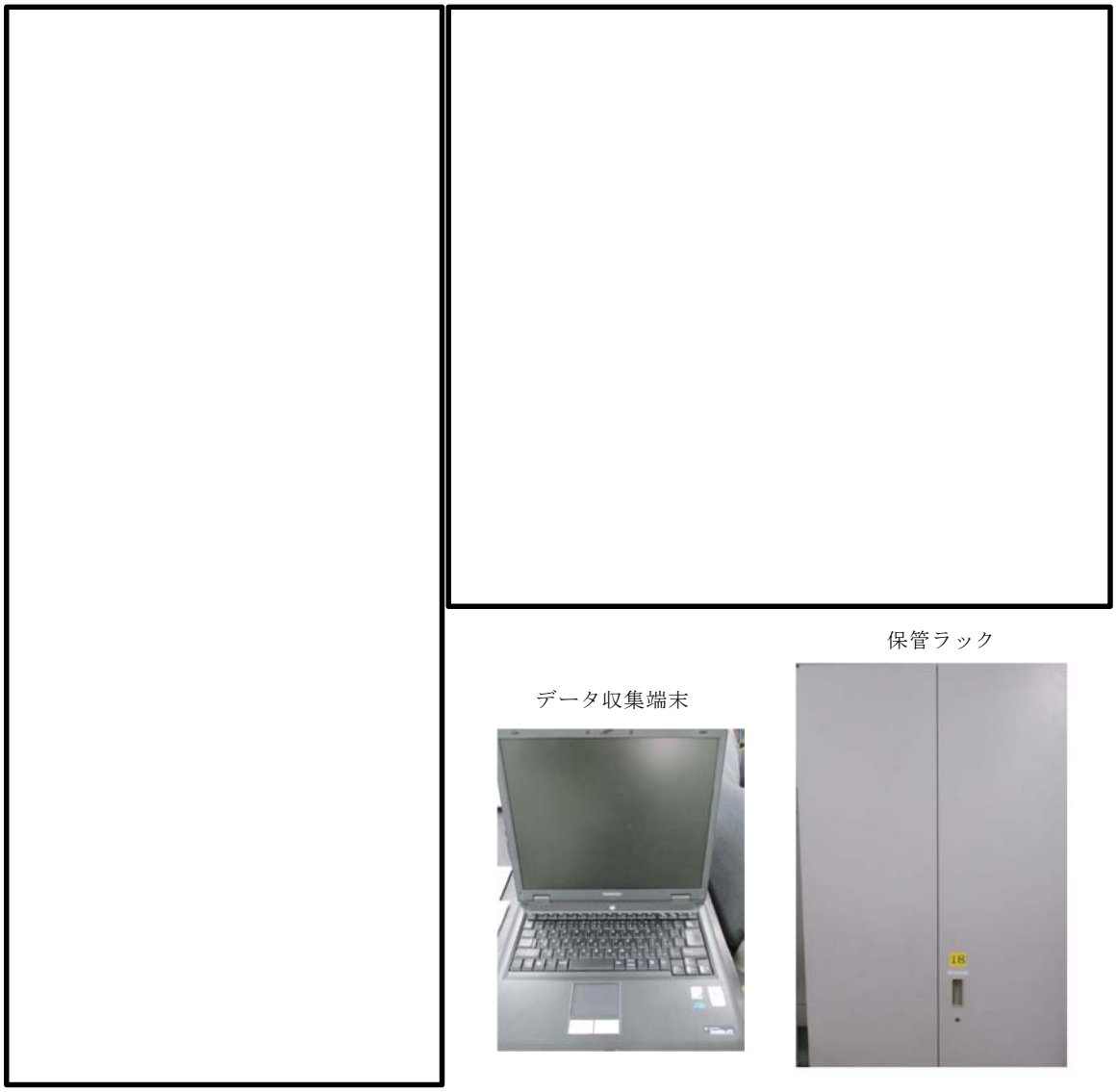
安全保護回路は，検出器からの信号を受信し，原子炉緊急停止系を自動的に作動させる回路と，工学的安全施設を作動させる信号を発する工学的安全施設作動回路で構成しており，多重性及び電気的・物理的な独立性を持たせている。



第2.2図　原子炉緊急停止系の構成例

2.3　安全保護回路の物理的分離対策

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。



安全保護系盤等は，社内規程に定める発電長による扉の鍵管理を行っている。
データ収集端末は，作業担当箇所により鍵管理されたラック内に保管しており，許可されない者のアクセスを防止している。また，情報セキュリティに関する教育を行っている。

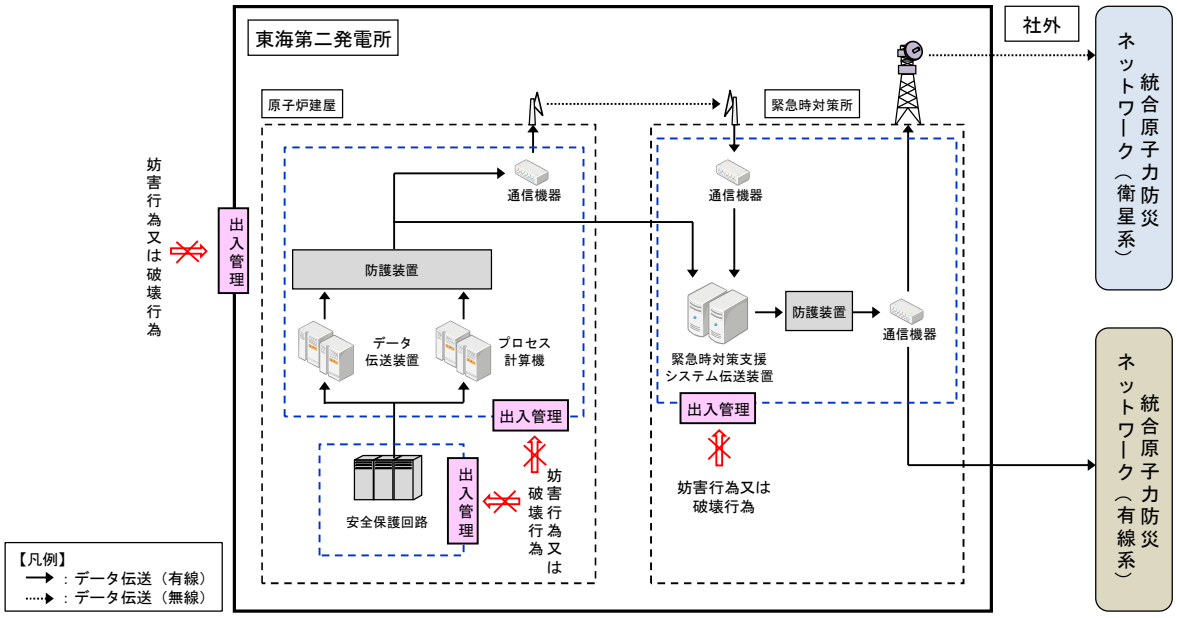
第 2.3 図　安全保護系盤及びデータ収集端末

2.4　外部からの不正アクセス防止について

安全保護回路は，外部ネットワークと直接接続は行っていない。外部システムと接続する必要のある計算機については，防護装置を介して接続され，外部からのデータ書き込み機能を設けないことでコンピュータウイルスの侵入等を防止している。

また，外部からの妨害行為または破壊行為については，出入管理により関係者以外の接近を防止している。

外部ネットワークとの接続構成概略図を第 2.4 図に示す。



第 2.4 図　外部ネットワークとの接続構成概略図

2.5　想定脅威に対する対策について

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 2.5 表に示す想定脅威に対する対策を行っている。

第 2.5 表　想定脅威に対する対策（工場製作及び出荷）

想定脅威		対策
外部脅威	外部からの侵入	ソフトウェアの設計データの製作環境は外部に接続しない環境で製作
内部脅威	設備の脆弱性	安全保護系のソフトウェアは供給者独自ソフトウェアにて構築
	不正ソフトウェア利用	不正ソフトウェアが無いことを確認した環境で，ソフトウェア設計を実施
	持込機器・媒体による改ざん・漏えい	作業専用端末による作業
	作業環境からの不正アクセス	作業環境での第三者のソフトウェアへの不正アクセスを防止
人的要因	作業ミス，知識不足による情報漏えい等	情報セキュリティ教育の実施

2.6　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，ケーブル・ルート及び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。

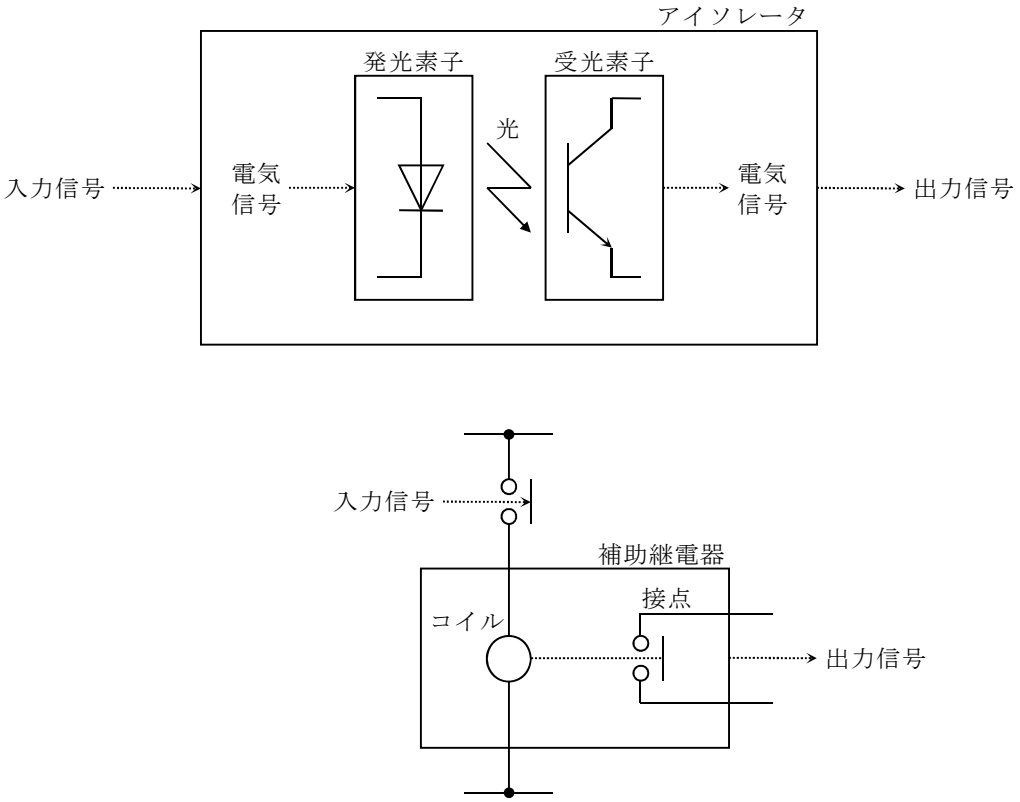
安全保護回路と計測制御系で計装配管を共用する場合は，安全保護回路の計装配管として設計する。

(2)　電気的分離について

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2.6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も安全保護回路に影響を与えない）を行う。

核計装系等の検出部が表示，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。



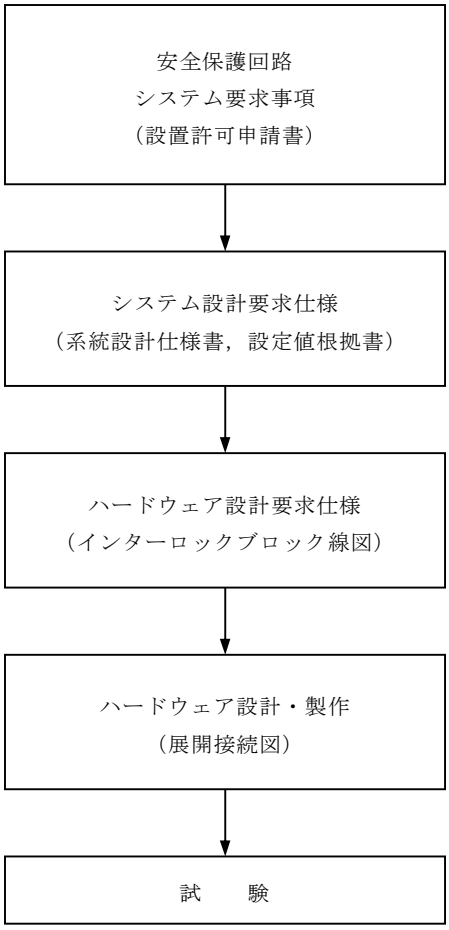
第 2.6 図　隔離装置（アイソレータ及び補助継電器）

別紙 1　アナログ型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設計方針

アナログ型の安全保護回路は，論理回路がハードワイヤーロジック（補助継電器や配線によるアナログ回路）で構成され制御盤内に設置している。

当該回路に対し，承認されていない動作及び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（第 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。
・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。
・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。
・安全保護回路及び設定値を変更するには，中央制御室にて発電長の許可を得て，発電長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。



第１図　安全保護回路の設計・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 月の運転停止以降の安全性向上対策工事等（新規制対応工事含む）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。第 1 図の抽出フローに基づき抽出した結果，SA 対策で実施する自動減圧系及び過渡時自動減圧機能の起動阻止スイッチ設置が抽出された。

安全保護回路の変更に係る設備の抽出結果を第 1 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。また，過渡時自動減圧機能及びＡＴＷＳ緩和設備（代替制御棒挿入機能）については，安全保護回路に変更を施しておらず，安全保護回路と電気的・物理的に分離されており安全保護回路に悪影響を与えない設計とする（参考 1)。

(1)　自動減圧系の起動阻止スイッチについて

ａ．目的

原子炉停止機能喪失事象においては，原子炉が臨界状態であるため，高圧炉心スプレイ系及び低圧注水系の急激な流量増加は，正の反応度印加を引き起こし，原子炉出力の急上昇につながる。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過渡時自動減圧機能が作動しないように，起動阻止スイッチを設置する。

ｂ．起動阻止スイッチ

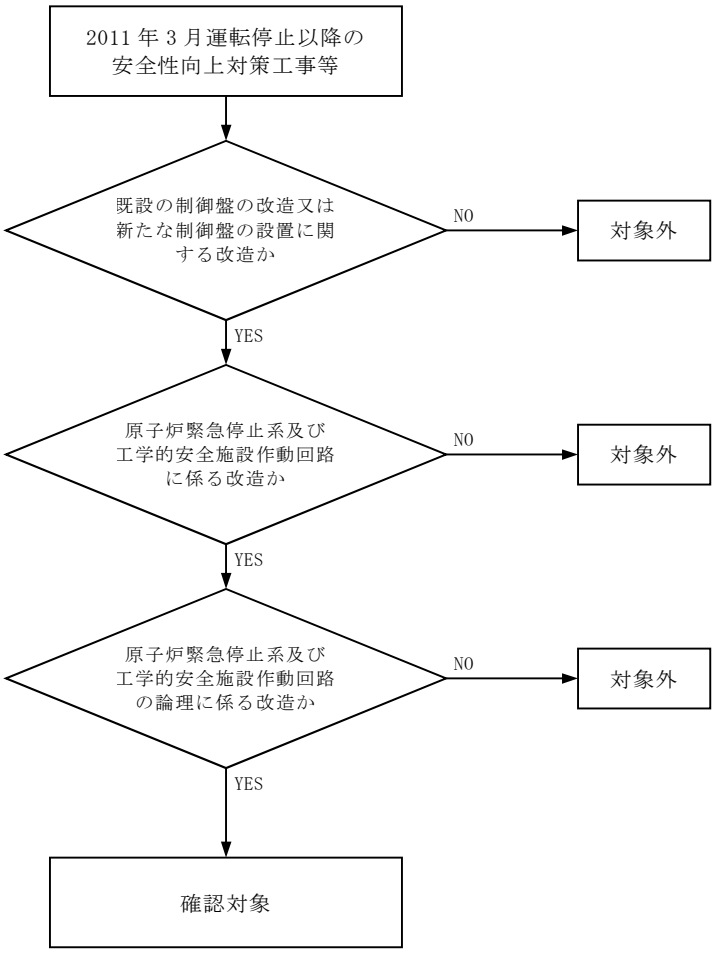
自動減圧系及び過渡時自動減圧機能の作動回路を第2図に示す。この起動阻止スイッチは，単一故障により，自動減圧系の機能を阻害しないように，また，多重化された自動減圧系の独立性に悪影響がないように自動減圧系の論理回路ごとに設ける設計としている。

ｃ．自動減圧系への影響について

追加設置する自動減圧系の起動阻止スイッチが，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。

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。	起動阻止スイッチは，原子炉停止機能喪失事象時に手動で自動減圧系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。	自動減圧系の多重性，独立性に悪影響を与えないよう，区分ごとに起動阻止スイッチを設置しているため問題ない。
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。	自動減圧系の多重性，独立性に悪影響を与えないよう，区分ごとに起動阻止スイッチを設置しているため問題ない。
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。	自動減圧系の多重性，独立性に悪影響を与えないよう，区分ごとに起動阻止スイッチ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。	自動減圧系は，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，独立性をもつことで原子炉を十分に安全な状態に導くようにしている。追加する起動阻止スイッチはこの安全保護動作を阻害するものではない。
六　不正アクセス行為その他の電子計算機に使用目的に沿うべき動作をさせず，又は使用目的に反する動作をさせる行為による被害を防止することができるものとすること。	阻止回路はアナログで構成しており，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。	計測制御系とは共用していないため，影響はない。

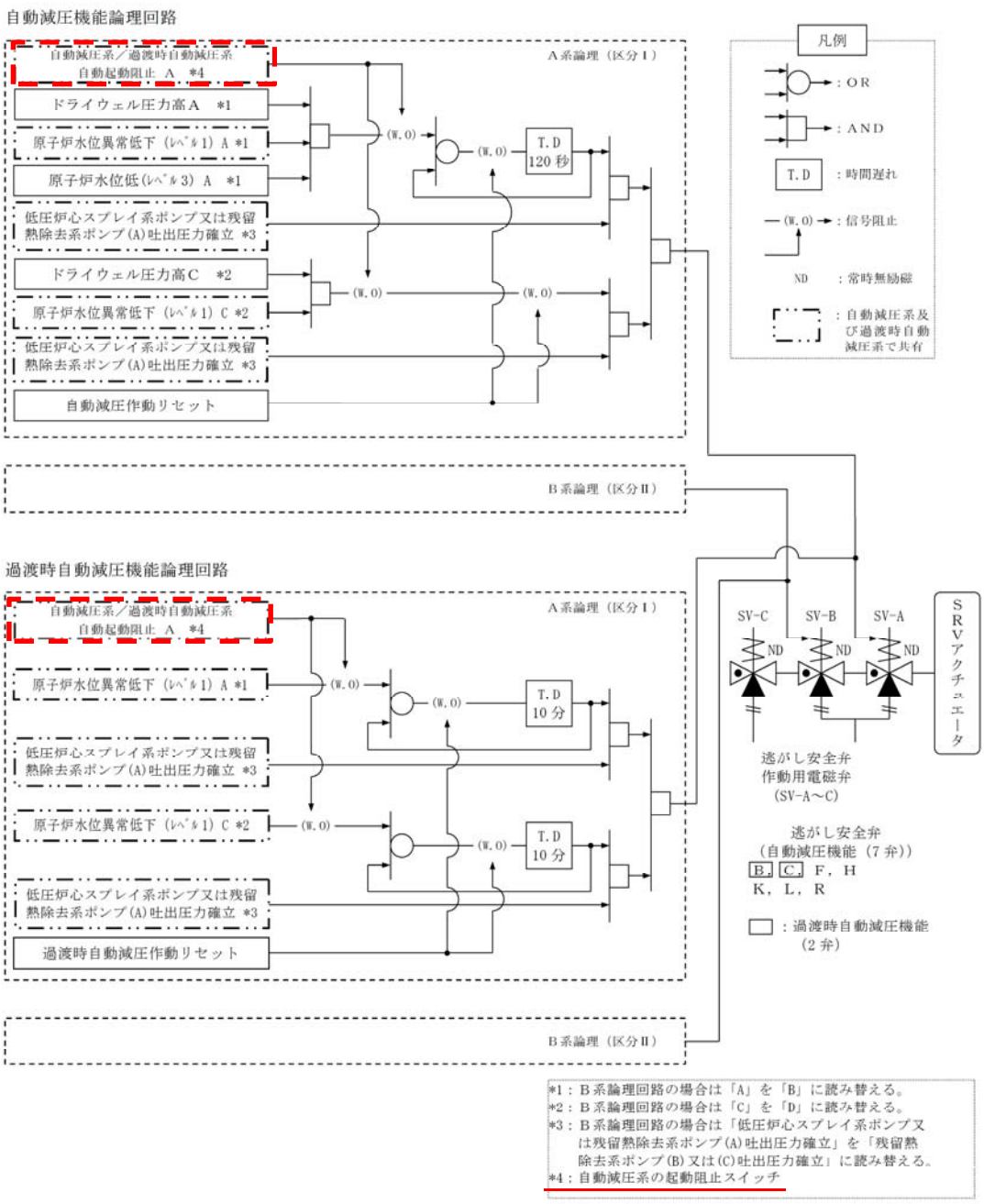
設置許可基準規則 第 12 条（安全施設）	自動減圧系への影響
4　安全施設は，その健全性及び能力を確認するため，その安全機能の重要度に応じ，発電用原子炉の運転中又は停止中に試験又は検査ができるものでなければならない。	起動阻止スイッチを設置することで自動減圧系の試験に影響を与えることはない。



第 1 図　安全保護回路の変更に係る改造抽出フロー

第１表　安全保護回路の変更に係る設備の抽出結果

改造概要	条文	安全保護回路への 影響評価
ＡＴＷＳ時に自動減圧系及び過渡時自動減圧機能の作動を阻止する手動阻止回路を追加する。	44 条	自動減圧系及び過渡時自動減圧機能の起動阻止スイッチは自動減圧機能論理回路の関連回路として安全保護回路と同等に扱うものとする。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。



第 2 図　自動減圧系及び過渡時自動減圧機能の作動回路図

参考１　新規制対応設備の安全保護回路への影響について

1.　過渡時自動減圧機能について

(1)　目的

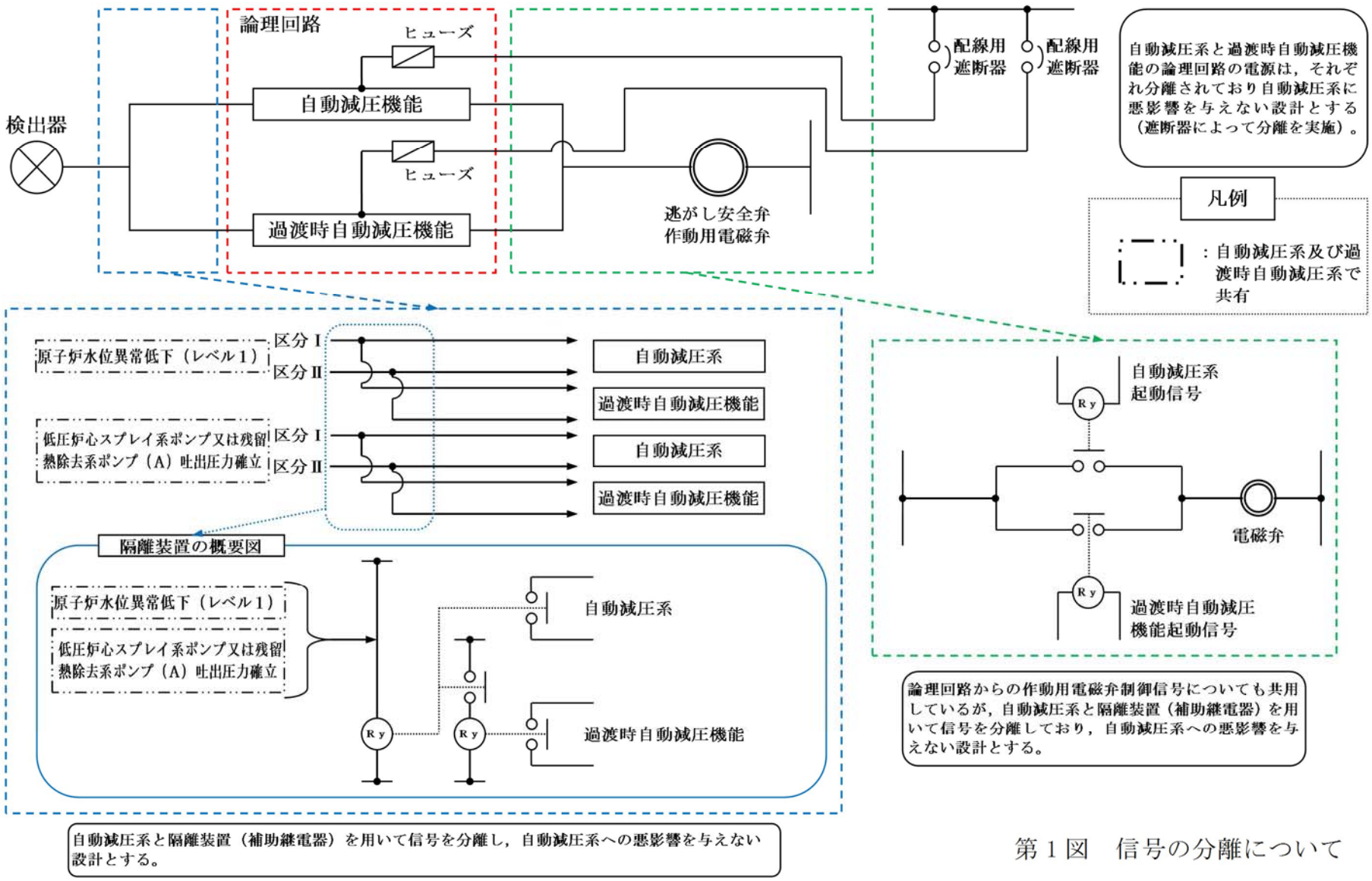
過渡時自動減圧機能は，原子炉冷却材圧力バウンダリが高圧の状態であって，設計基準事故対処設備が有する原子炉の自動減圧機能が喪失した場合においても，原子炉冷却材圧力バウンダリを減圧し，炉心の著しい損傷及び原子炉格納容器の破損を防止することを目的とする。

(2)　自動減圧系への影響について

過渡時自動減圧機能の論理回路は別紙2（第2図）のとおりであり，論理回路を自動減圧系に対して独立した構成としており，自動減圧系に悪影響を与えない設計としている。

第1図のとおり，原子炉水位異常低下（レベル１），低圧炉心スプレイ系ポンプ吐出圧力確立，及び残留熱除去系ポンプ吐出圧力確立信号については共有しているが，自動減圧系と隔離装置を用いて電気的に分離しており，自動減圧系への悪影響を与えない設計としている。

また，論理回路からの作動用電磁弁制御信号についても共用しているが，自動減圧系と隔離装置を用いて電気的に分離しており，自動減圧系への悪影響を与えない設計としている。



第１図　信号の分離について

2．ＡＴＷＳ緩和設備（代替制御棒挿入機能）について

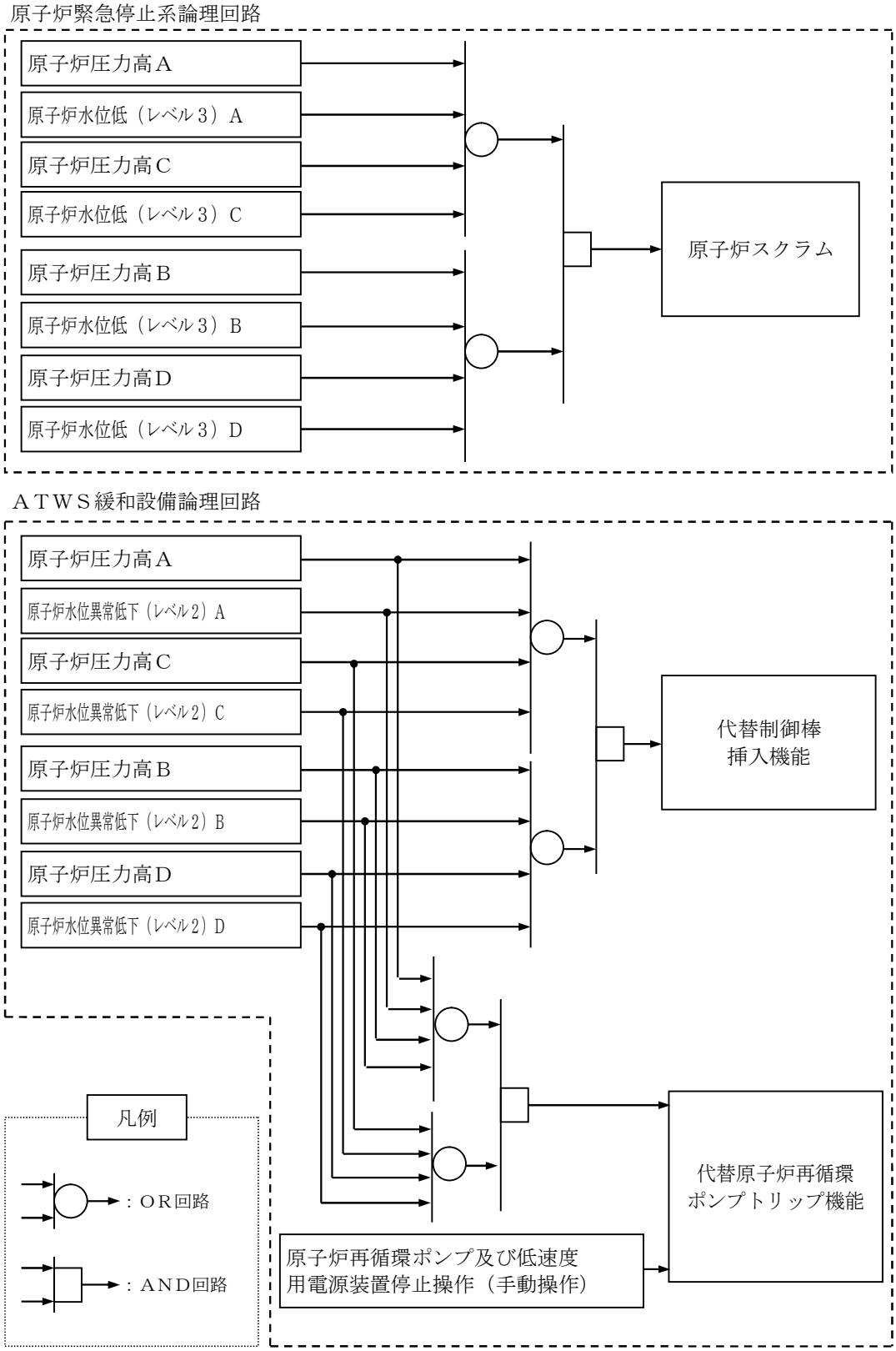
(1)　目的

代替制御棒挿入機能は，運転時の異常な過渡変化時において，原子炉の運転を緊急に停止することができない事象が発生するおそれがある場合又は当該事象が発生した場合において，原子炉緊急停止系から独立した回路により，計器用空気配管上に設置したスクラム・パイロット弁とは別のソレノイドが励磁され排気弁を開放し，全制御棒を挿入することにより原子炉出力を低下させることを目的とする。

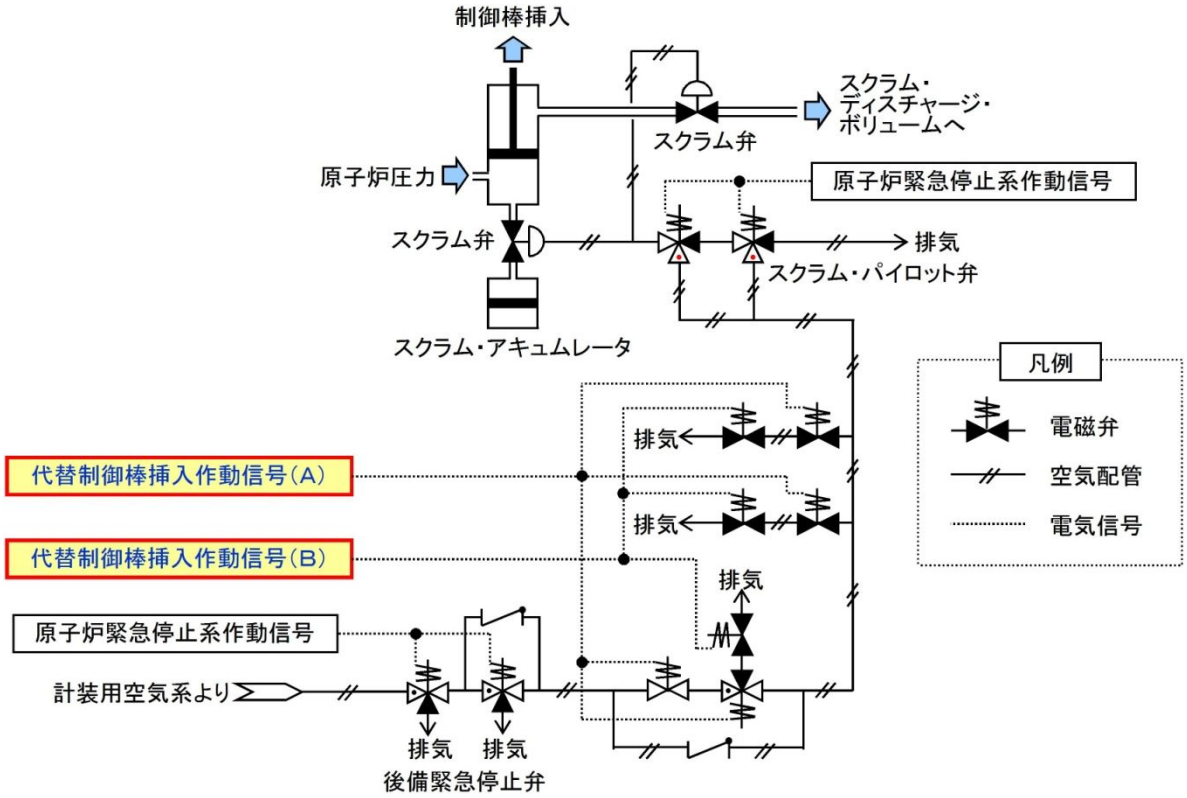
(2)　原子炉緊急停止系への影響について

代替制御棒挿入機能の論理回路は第2図のとおり，検出器から論理回路まで，原子炉緊急停止系とは独立した構成となっており，原子炉緊急停止系に悪影響を与えない設計としている。

なお，代替制御棒挿入機能の作動電磁弁についても，第3図のとおり代替制御棒挿入機能と原子炉緊急停止系では独立した構成となっている。



第２図　原子炉緊急停止系及び代替制御棒挿入機能の論理回路図



第 3 図　作動電磁弁について

別紙３　アナログ型安全保護回路の不正アクセス行為等の防止対策

アナログ型安全保護回路の検出器はアナログ機器，論理回路はハードワイヤーロジック（補助継電器や配線によるアナログ回路）で構成しているが，一部の安全保護回路への出力信号処理でデジタル装置を使用している。安全保護回路（原子炉緊急停止系，工学的安全施設作動回路）について，検出器から論理回路の入口までの構成機器に対しアナログ・デジタルの有無を抽出した。安全保護系構成概略図を第１図，抽出結果を第１表，第２表に示す。安全保護回路にはプロセス放射線モニタ盤の演算処理装置及び中性子束計装モニタ盤の演算処理装置にデジタル回路が含まれる。ただし，当該演算処理装置は外部ネットワークと直接接続しないことにしている。さらに，出入管理により外部からの妨害行為または破壊行為を防止していることから不正アクセス行為による被害を受けることはない。

(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し，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とし，デジタル処理部を持つ機器からデータを採取するデータ収集端末にはデジタル処理を行う演算回路からのデータ受信機能のみを設けるとともに，データ収集端末を施錠管理された場所に保管することで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→プロセス計算機・データ伝送装置→防護装置→緊急時対策支援システム伝送装置→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，安全保護回路からは発信され

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。

(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。

※データダイオード装置（ハードウェアレベルでダイオードのように片方向のみ通信を許可する装置）により一方向通信に制限する。

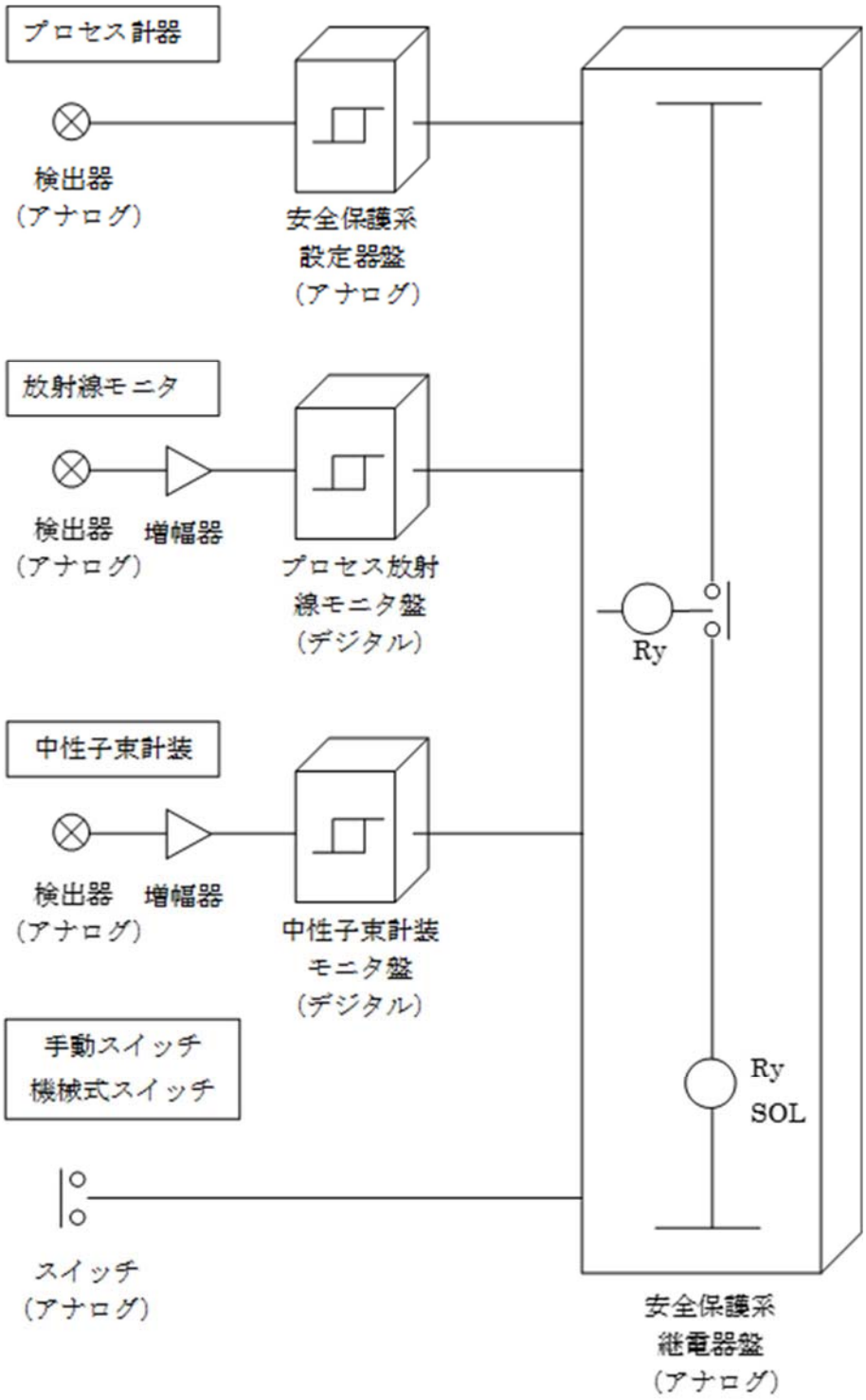
(4)　システムの導入段階，更新段階または試験段階で承認されていない動作や変更を防ぐ対策

安全保護回路のうちデジタル処理部を持つ機器は，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や設定値変更作業での鍵管理及びパスワード管理を行い，関係者以外の不正な変更等を防止している。

(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，制御盤へ入線する電源受電部及びケーブル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。

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。



第 1 図　安全保護系構成概略図

第１表　原子炉緊急停止系の構成機器

原子炉スクラム信号の種類	構成機器	
	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
ドライウェル圧力高	アナログ	アナログ
原子炉出力ペリオド短（起動領域計装）	アナログ	デジタル
中性子束高（起動及び出力領域計装）	アナログ	デジタル
中性子束指示低（出力領域計装）	アナログ	デジタル
中性子計装動作不能（起動及び出力領域計装）	アナログ	デジタル
スクラム・ディスチャージ・ボリューム水位高	アナログ（接点）	
主蒸気隔離弁閉	アナログ（接点）	
主蒸気管放射能高	アナログ	デジタル
主蒸気止め弁閉	アナログ（接点）	
蒸気加減弁急速閉（ＥＨＣ油圧低）	アナログ（接点）	
地震	アナログ（接点）	
原子炉モード・スイッチ「停止」の位置	アナログ（接点）	
手動	アナログ（接点）	

第 2 表　工学的安全施設作動回路の構成機器

機能	信号の種類	構成機器	
		検出器	設定器
主蒸気隔離弁閉	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
	主蒸気流量高	アナログ	アナログ
	原子炉水位異常低下	アナログ	アナログ
	主蒸気管トンネル温度高	アナログ	アナログ
	復水器真空度低	アナログ	アナログ
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	ドライウェル圧力高	アナログ	アナログ
	原子炉水位異常低下	アナログ	アナログ
自動減圧系の作動	ドライウェル圧力高	アナログ	アナログ
	原子炉水位異常低下	アナログ	アナログ
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	ドライウェル圧力高	アナログ	アナログ
	原子炉水位異常低下	アナログ	アナログ
原子炉建屋常用換気系の閉鎖と原子炉建屋ガス処理系の起動	ドライウェル圧力高	アナログ	アナログ
	原子炉水位低	アナログ	アナログ
	原子炉建屋放射能高	アナログ	デジタル
主蒸気隔離弁以外の主要な隔離弁閉鎖	ドライウェル圧力高	アナログ	アナログ
	原子炉水位低	アナログ	アナログ
	原子炉水位異常低下	アナログ	アナログ

別紙 4　ソフトウェア更新時の立会における，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，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処理部がある機器は，プロセス放射線モニタ盤，中性子束計装モニタ盤である。これらについては以下の対策を実施する。

データ収集端末については，デジタル処理を行う演算回路からのデータ受信機能のみを設けることとし，施錠管理されたラック内に保管する。また，データ収集端末は，当社保修員が許可した者に限定して貸し出しを行うこととする。

データ収集端末接続のためには制御盤の解錠が必要であり，制御盤の鍵は発電長の許可を得た上で貸し出しを行う。

これらにより，許可された者のみアクセス可能とする。

別紙 5　安全保護回路のうちデジタル部分のシステムへ接続可能なアクセスについて

安全保護回路のうちデジタル部分のシステムへの接続可能なアクセスとして，データ収集端末の接続がある。こちらについては以下のとおり対策する。

(1)　データ収集端末による不正アクセスの防止対策

データ収集端末は，中性子束計装モニタ盤に接続することによりデジタル処理を行う演算回路からデータを受信する機能がある。この場合において，中性子束計装モニタ盤からはデータを発信するだけであり，データ収集端末には自身から中性子束計装モニタ盤に向けて通信する機能は持たせていない。

(2)　物理的アクセスの制限

データ収集端末は通常時接続はせず，接続のためには制御盤の解錠を必要とする。また，施錠管理された場所に保管することで管理されない使用及び変更を防止している。

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し，管理されない変更を防止している。

別紙 6　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

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処理部がある機器は，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。

別紙７　安全保護系の過去のトラブルの反映事項

安全保護系に関わる過去のトラブル情報を抽出し，東海第二発電所の安全保護系の設計面へ反映すべき事項を下記の通り確認した。

(1)　過去の不具合事象の抽出

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

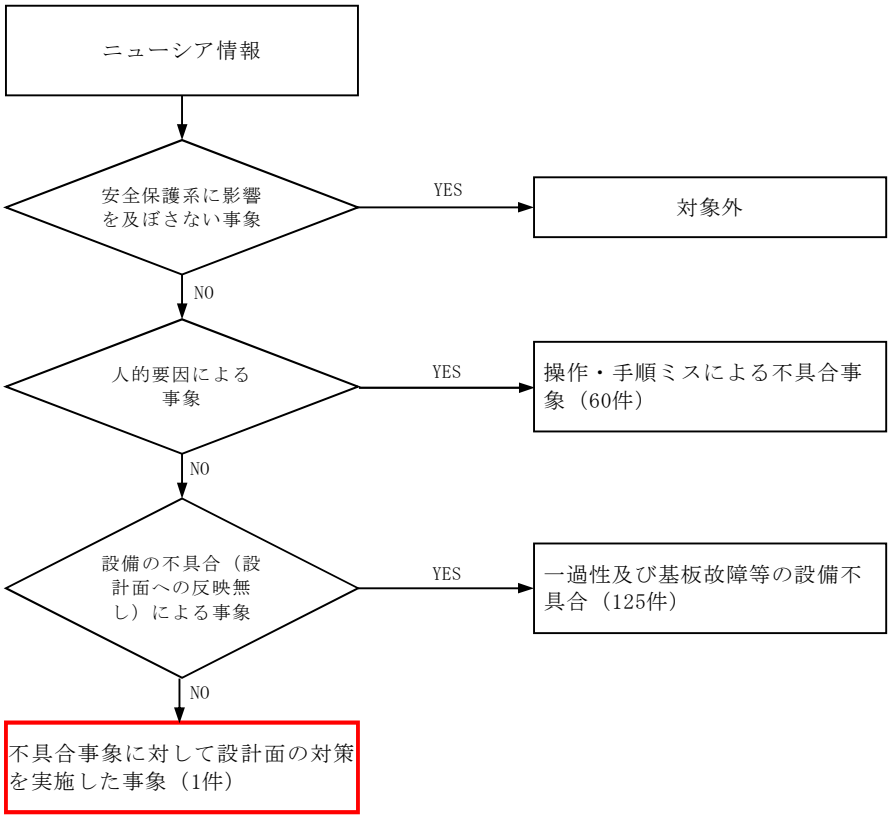
ｃ．間接的な影響（他設備のトラブル）によって安全保護系へ影響を与えた事象（安全保護系の正動作は除く）

(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，第1図及び第1表に基づき抽出した。抽出された過去の不具合事象を第2表に示す。

(3)　過去の不具合事象への対応について

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1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。



第1図　設計面へ反映すべき事項の抽出フロー

第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。
設備の不具合（設計面への反映無し）による事象	計器・部品の単体故障，一過性故障，偶発故障等	故障した部品の交換等の対策を図ることが基本であり，設計面へ反映すべき事項ではない。

第2表　抽出された過去の不具合事象

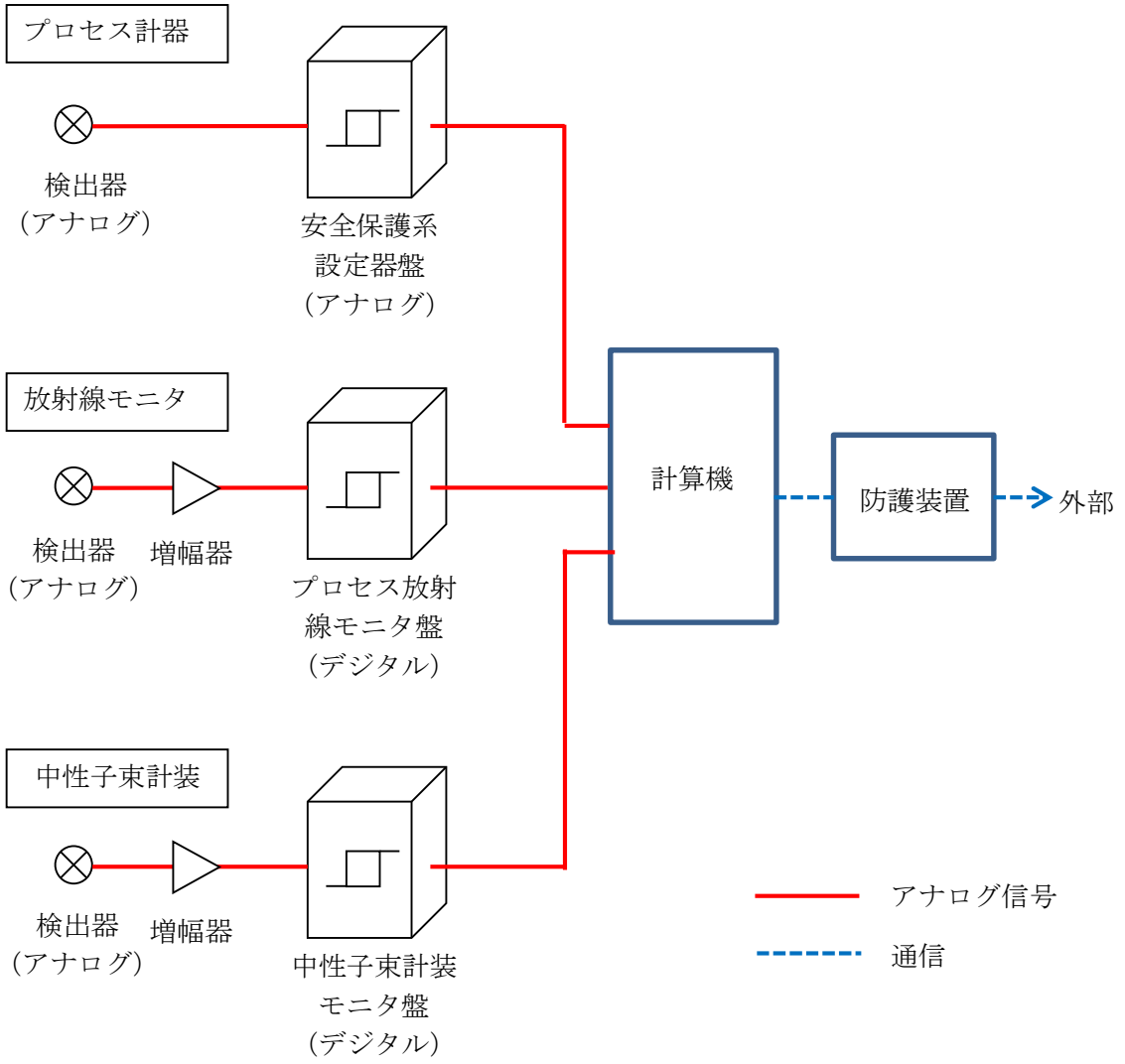
件名	原子炉保護系チャンネルＡのトリップについて
会社名・プラント	日本原子力発電株式会社　東海第二発電所
発生日	1982年3月18日
事象発生時の状況	出力１，１００MWで定常運転中の３月１８日１６時５６分，原子炉保護系チャンネルＡが，原子炉圧力高（Ａ２）の動作によりトリップした。 関連パラメータには，異常が認められなかったので，チャンネルＡトリップをリセットして，運転を継続した。
原因調査の概要	当該圧力スイッチ（Ｂ２２－Ｎ０２３Ｃ）の較正確認試験を実施した結果，セット値７３．３ｋｇ／ｃｍ^{2}ｇ（原子炉施設保安規定に定める設定値は７４．０ｋｇ／ｃｍ^{2}ｇ）に対し，動作値は７２．１ｋｇ／ｃｍ^{2}ｇであり，動作値がセット値に対し１．２ｋｇ／ｃｍ^{2}ｇ低い（ドリフト）ことが判明した。 なお，当該圧力スイッチ（Ｂ２２－Ｎ０２３Ｃ）は，昨年７月２８，２９日にも同じ事象が発生しており，その後，再現性テスト，配管・サポートの点検，圧力スイッチの固有振動数並びに運転中の圧力変動（脈動）及び振動値（加速度）の測定等の結果，当該圧力スイッチの検出管は，他の検出管に比べ圧力変動（脈動）が大きい（変動巾最大値１．３５ｋｇ／ｃｍ^{2}ｇ）現象が認められた。しかし，動作に至るほどの変動ではなかった。このため，定検後の原子炉起動時（昨年１２月）には，検出配管内のフラッシング及び空気抜きを十分に行っていた。
事象の原因	当該圧力スイッチの動作値がドリフトしていたこと及び検出配管内の圧力脈動等を瞬時に検出して，動作したものと考えられる。
再発防止対策	（１）当該圧力スイッチは動作値がドリフトしていたので，予備の圧力スイッチと交換した。 （２）次回定検時，検出方式を現在の現場圧力スイッチ方式から，圧力変動（脈動）等の影響（誤動作）及びドリフトの少ない，アナログ方式に変更する。 （３）中間停止（今年６月）から次回定検（今年１１月開始）までの運転中，関連パラメータをイベントレコーダに接続して，誤動作が生じるような事象の連続監視を行う。

参考

サイバー攻撃（ランサムウェア）による安全保護回路への影響について

チェルノブイリ原子力発電所周辺において，ランサムウェアによる攻撃により，ウィンドウズ・システムを使う放射線センサが作動しなくなったため手動に切り替えたとの報道がある。

東海第二発電所の安全保護回路はアナログ回路で構成しており，また外部ネットワークへ直接接続されておらず，外部からのランサムウェア等のサイバー攻撃に対して安全保護回路が影響を受けることはないと考える。



別 添

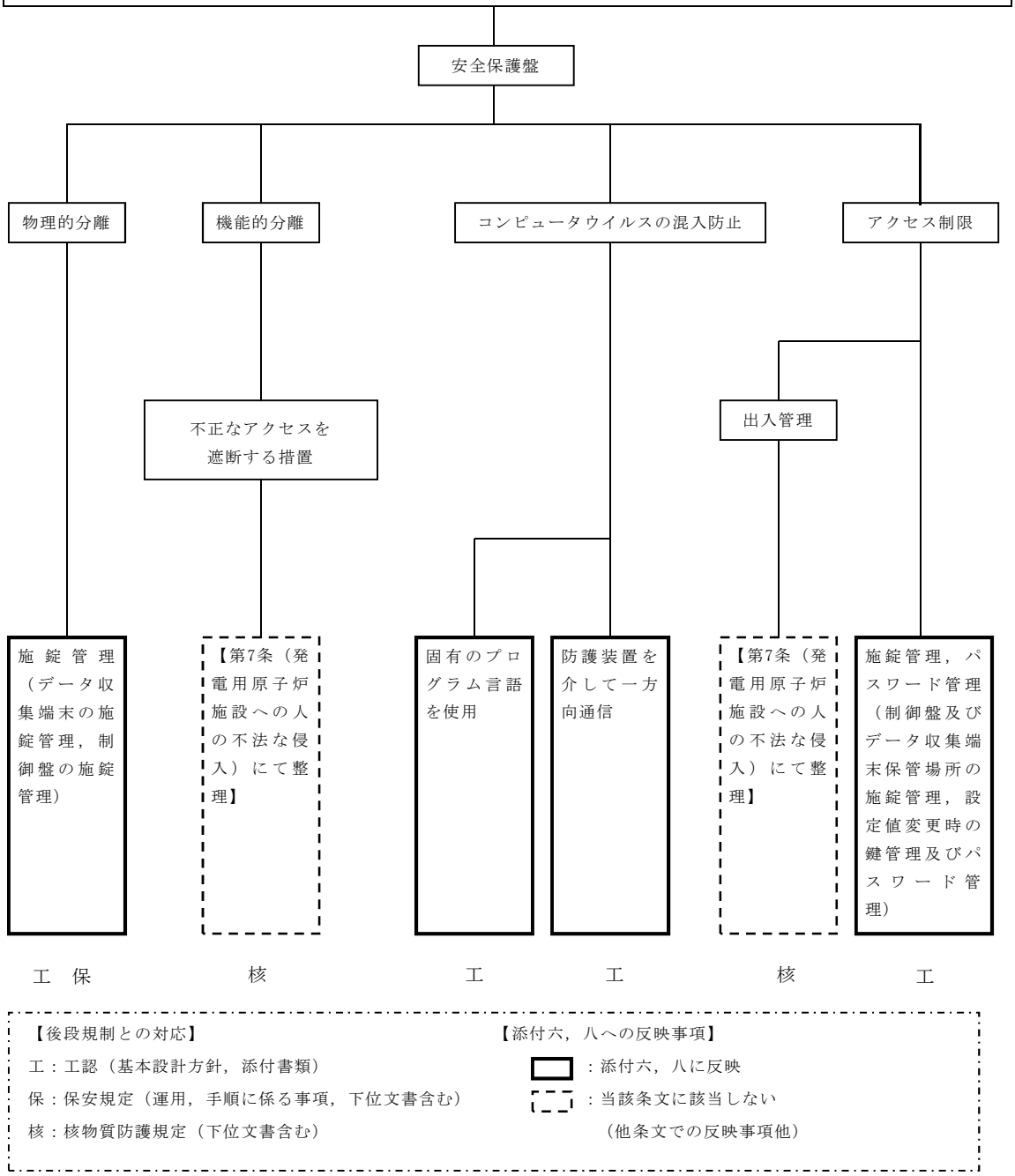
東海第二発電所

運用，手順説明資料

安全保護回路

第 24 条　安全保護回路

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）
　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。



【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）
核：核物質防護規定（下位文書含む）

【添付六，八への反映事項】
：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）

第 1 表　運用，手順に係る対策等（設計基準）

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	－
	パスワード管理	運用・手順	・管理（設定値変更時のパスワード管理の手順整備含む） ・操作（パスワード入力手順の整備含む）
		体制	（保修員によるパスワード管理）
		保守・点検	－
		教育・訓練	－