資料2－7

7　安全保護回路

◇ソフトウェア管理方法、不正アクセス行為防止　ほか

適合のための基本方針

「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
（「実用発電用原子炉及びその附属施設の技術基準に関する規則」第三十五条）

設置許可基準	適合のための基本方針
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。	＜第24条　第１号への適合＞ （規制要求変更なし）
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。	＜第24条　第２号への適合＞ （規制要求変更なし）
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。	＜第24条　第３号への適合＞ （規制要求変更なし）
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。	＜第24条　第４号への適合＞ （規制要求変更なし）

適合のための基本方針

「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
（「実用発電用原子炉及びその附属施設の技術基準に関する規則」第三十五条）

設置許可基準	適合のための基本方針
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。	＜第24条　第５号への適合＞ （規制要求変更なし）
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。	＜第24条　第６号への適合＞ （追加要求事項） 安全保護回路（原子炉緊急停止系作動回路，工学的安全施設作動回路）を構成するデジタル計算機について，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。
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。	＜第24条　第７号への適合＞ （規制要求変更なし）

追加基準要求事項（第６号）の適合性について説明

柏崎6/7号炉，女川2号炉，島根２号炉と同様の方針

不正アクセス行為防止のための措置

■ 安全保護回路（原子炉緊急停止系作動回路,工学的安全施設作動回路）について，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ため，下記の対策を実施する。

（１）物理的及び電気的アクセスの制限対策

物理的アクセス（発電所の出入管理），電気的アクセス（制御盤及び保守ツールの接続部の施錠管理，保守ツールの保管及びパスワードによる変更管理）の制限を行う。

（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。また，ハードウェアを直接接続しない。

（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

外部ネットワークへ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。

（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

・「安全保護系へのディジタル計算機の適用に関する規程（ＪＥＡＣ4620）」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）」に基づき，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（Ｖ＆Ｖ）がなされたソフトウェアを使用している。
・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。
・入域制限や保守ツールの施錠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，サージ・ノイズ，電磁波障害等による擾乱に対して，制御盤へ入線する電源受電部や外部からの信号入出力部にラインフィルタや絶縁回路を設置，通信ラインにおける光ケーブルを適用している。

柏崎6/7号炉，女川2号炉，島根２号炉と同様の方針

不正アクセス行為防止のための措置

（６）ウイルス侵入防止について，供給者への要求事項及び供給者で実施している対策

・ウイルスの侵入防止対策も含め,当社の安全保護回路への妨害行為又は破壊行為を防止するため，下表のようなセキュリティ対策を安全保護回路の設計に反映するよう,供給者へ要求することとしている。

・供給者はこれを受けて,インターネットへの直接接続の禁止，保守のための当該システムへの接続は許可された機器のみに限定している等の対応を実施することとしている。

供給者への要求事項及び供給者で実施している対策

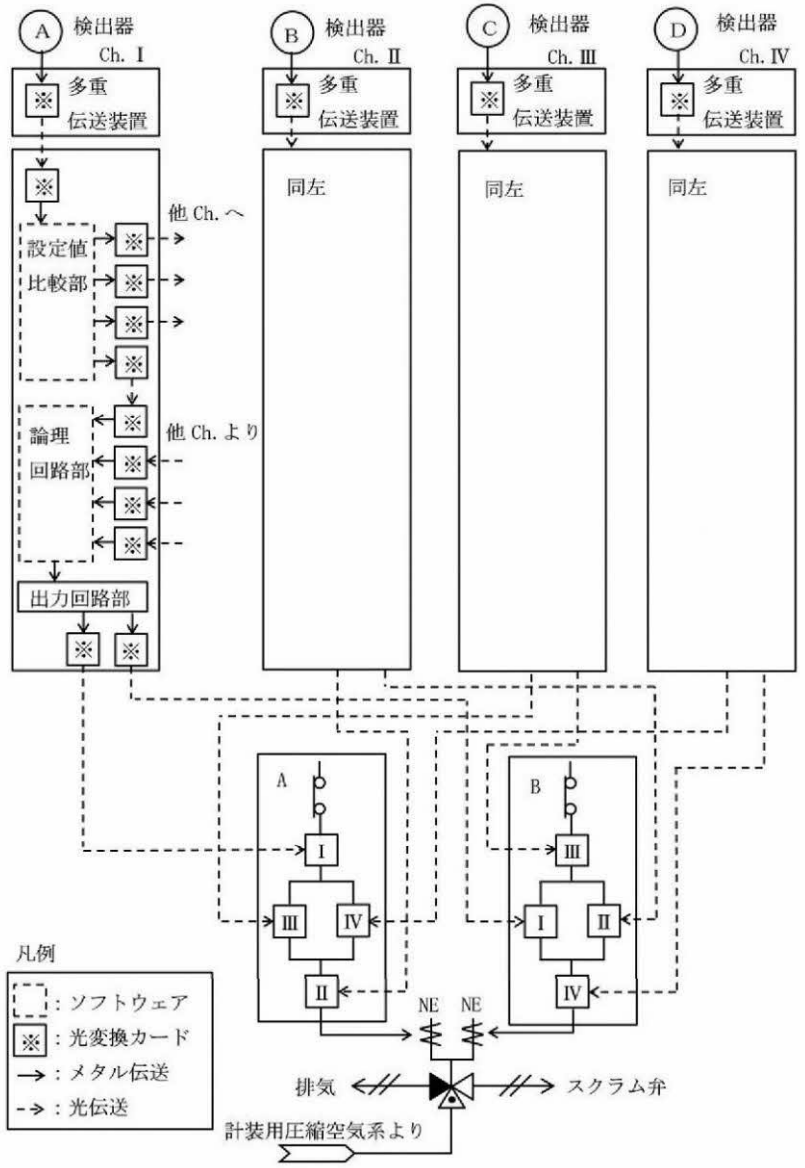
項目	当社の要求	供給者の対応
開発・改造に関する設計上の要求		
媒体の管理		
保守に関する要求		
教育		
設定及び設定変更管理		
作業実施		

本資料のうち，枠囲みの内容は機密に係る事項のため公開できません。

安全保護回路の概要

柏崎6/7号炉と同様の方針

- 安全保護回路は，原子炉緊急停止系を自動的に作動させる信号を発する原子炉緊急停止系作動回路と，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いる。
- 安全保護回路のソフトウェアは区分ごとにそれぞれ設けており，ソフトウェアの故障，異常等の単一故障又は使用状態からの単一の取り外しを行った場合でも，安全保護系機能を喪失することはない。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，区分ごとに論理回路部を設け，2 out of 4ロジック回路を構成している。



原子炉緊急停止系の構成例

柏崎6/7号炉，女川2号炉，島根２号炉と同様の方針

安全保護回路のソフトウェア管理方法

- 安全保護回路のソフトウェア変更に当たっては，施錠されたラック内に保管した保守ツールを使用して行い，使用時は安全保護回路の保守ツールの接続部の解錠を必要とし，管理されないソフトウェアの変更を防止する。
- 安全保護回路へソフトウェアをインストールする場合は，一連の作業は当社社員が立ち会い，正しくソフトウェア変更が行われたことを確認することとしている。

安全保護系盤及び保守ツール

本資料のうち，枠囲みの内容は機密に係る事項のため公開できません。

柏崎6/7号炉，女川2号炉，島根２号炉と同様の方針

外部からの不正アクセス行為防止

- 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データ等については，防護装置を介して接続している。
- 安全保護回路は固有のプログラム言語を使用するとともに，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等を防止している。
- 外部からの妨害行為又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。
  また，安全保護系盤については施錠を行い，関係者以外のアクセスを防止する。

外部ネットワークとの接続構成概要

本資料のうち，枠囲みの内容は機密に係る事項のため公開できません。

安全保護回路の検証及び妥当性確認

柏崎6/7号炉と同様の方針

■ 安全保護回路のソフトウェアは，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（Ｖ＆Ｖ）を適切に行うことで高い信頼性を実現している。

ライフサイクルプロセスにおける各段階での対策

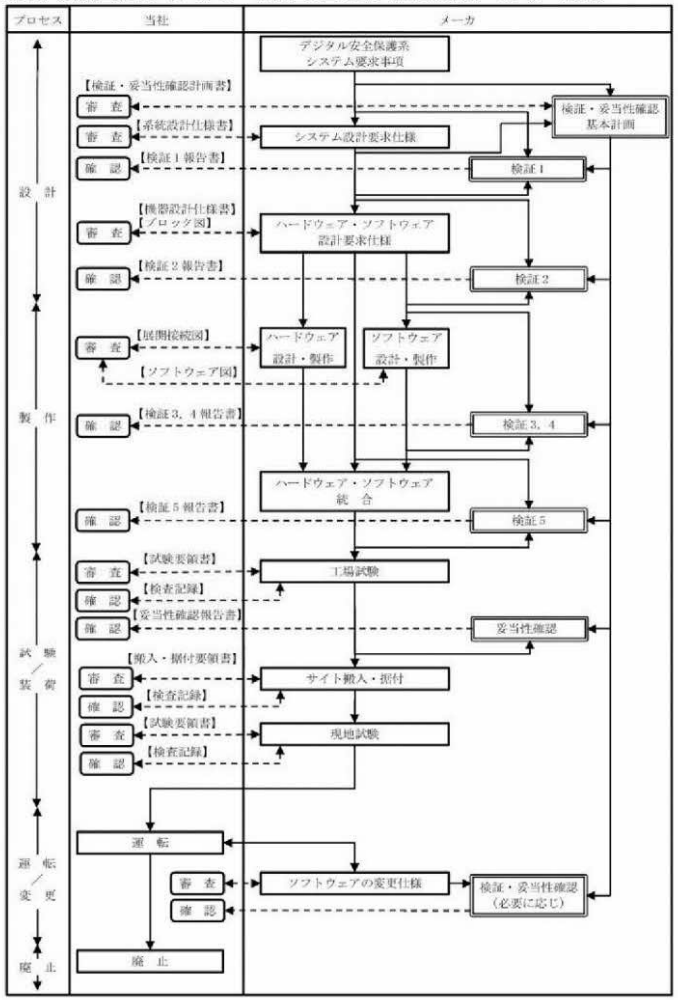
段階	内容	対策
設計プロセス	安全保護回路に対するシステムの要求事項からソフトウェア設計仕様を作成する。	・システム設計要求仕様及びソフトウェア設計要求仕様を文書化し，メーカ及び当社にてシステム要求事項を満足していることを確認する。 ・ＪＥＡＧ4609に基づいた検証及び妥当性確認（検証１と検証２）を実施し，ソフトウェア構成管理計画の下に適切に保存する。また，検証作業の合格基準及び不良結果等に対する措置を明確に文書化する。
製作プロセス	安全保護回路のソフトウェア設計要求仕様より安全保護系回路のソフトウェアを製作する。	・ＪＥＡＧ4609に基づいた検証及び妥当性確認（検証３から検証５）を実施し，ソフトウェア構成管理計画の下に適切に保存する。また，検証作業の合格基準及び不良結果等に対する措置を明確に文書化する。
試験プロセス	制作された安全保護回路のソフトウェアに対して，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制作されていることを試験により確認する。	・試験の対象範囲，実施要領及び判定基準を文章化し，メーカ及び当社にて上流の要求事項，設計要求仕様を満足する試験内容であることを確認する。また，試験を実施した結果を文章化する。 ・ＪＥＡＧ4609に基づいた検証及び妥当性確認（妥当性確認）を実施し，ソフトウェア構成管理計画の下に適切に保存する。また，検証作業の合格基準及び不良結果等に対する措置を明確に文書化する。

段階	内容	対策
装荷プロセス	実機へ安全保護回路のソフトウェアを実装する。	・各作業，試験内容を文書化し，メーカ及び当社にて上流の要求事項，設計要求仕様を満足する作業，試験内容であることを確認する。また実施した結果を文章化する。 ・工場出荷時のソフトウェアをローディングした後，コンペアチェックを実施し，相違ないことを確認する。 ・試験プロセスを完了し，運転プロセスに移行する前に，最終ソフトウェアをコンペアチェックで確認する。 ・最終ソフトウェアについて，ソフトウェア構成管理を実施し，結果を文書化する。
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する。	・各々のプロセスでの文書，ソフトウェアの変更を構成管理に基づき行う。 ・変更箇所及び変更の影響を受ける部分については，変更内容に応じて検証及び妥当性確認の必要な手順を再度実施する。

安全保護回路の検証及び妥当性確認

柏崎6/7号炉と同様の方針

■ 安全保護回路のソフトウェアは，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）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）に基づき，供給者による検証及び妥当性確認の各段階において，確実に実施されていることを確認している。



安全保護回路のソフトウェアに対する検証及び妥当性確認の流れ

検証項目及び検証内容

検証項目	検証内容
検証１	デジタル安全保護系システム要求事項が正しくシステム設計要求仕様に反映されていることを検証する。
検証２	システム設計要求仕様が正しくハードウェア・ソフトウェア設計要求仕様に反映されていることを検証する。
検証３	ソフトウェア設計要求仕様が正しくソフトウェア設計に反映されていることを検証する。
検証４	ソフトウェア設計どおりに正しくソフトウェアが製作されていることを検証する。
検証５	ハードウェア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どおりのシステムとなっていることを検証する。
妥当性確認	ハードウェアとソフトウェアを統合して検証されたシステムが，デジタル安全保護系システム要求事項を満たしていることを確認する。

想定脅威に対する対策

柏崎6/7号炉，女川2号炉，島根２号炉と同様の方針

- 安全保護回路のソフトウェアは，下表に示す想定脅威に対する対策を行っている。
- ソフトウェア更新時のセキュリティ対策として，保守ツール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［　　］の許可を得た上で貸し出しを行うことにより，許可された者のみアクセス可能とする。
- 保守ツールについては，施錠管理されたラック内に保管し，保守ツール使用には，［　　］の許可を得る必要があるとともに，パスワードの入力が必要である。

想定脅威に対する対策（工場製作及び出荷）

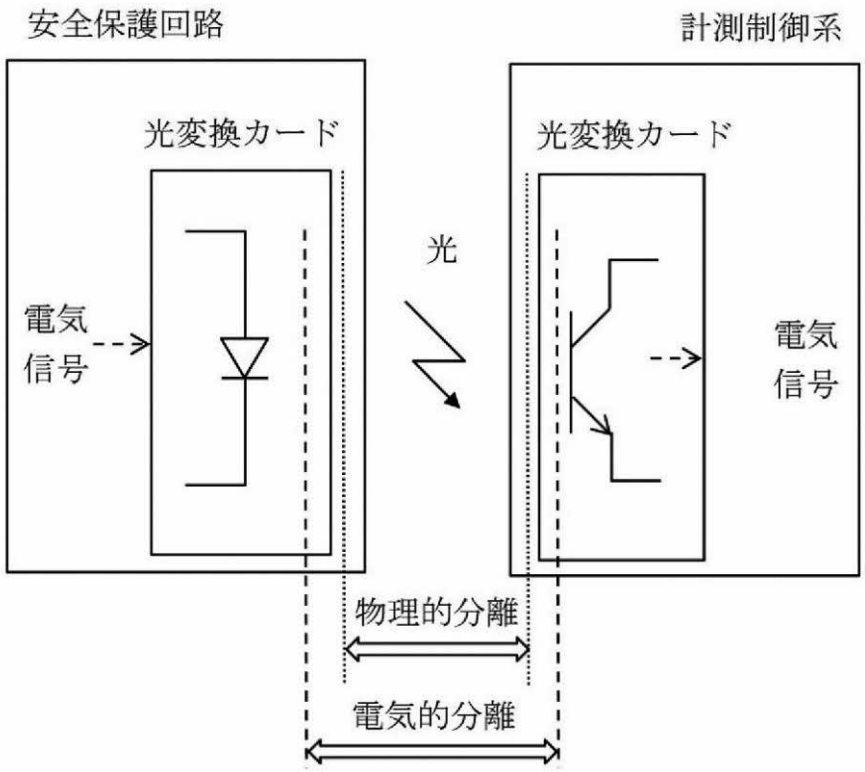
想定脅威	対策

本資料のうち，枠囲みの内容は機密に係る事項のため公開できません。

物理的分離及び電気的分離

柏崎6/7号炉と同様の方針

- 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，光変換カードによって送信側と受信側の物理的及び電気的分離を行っている。

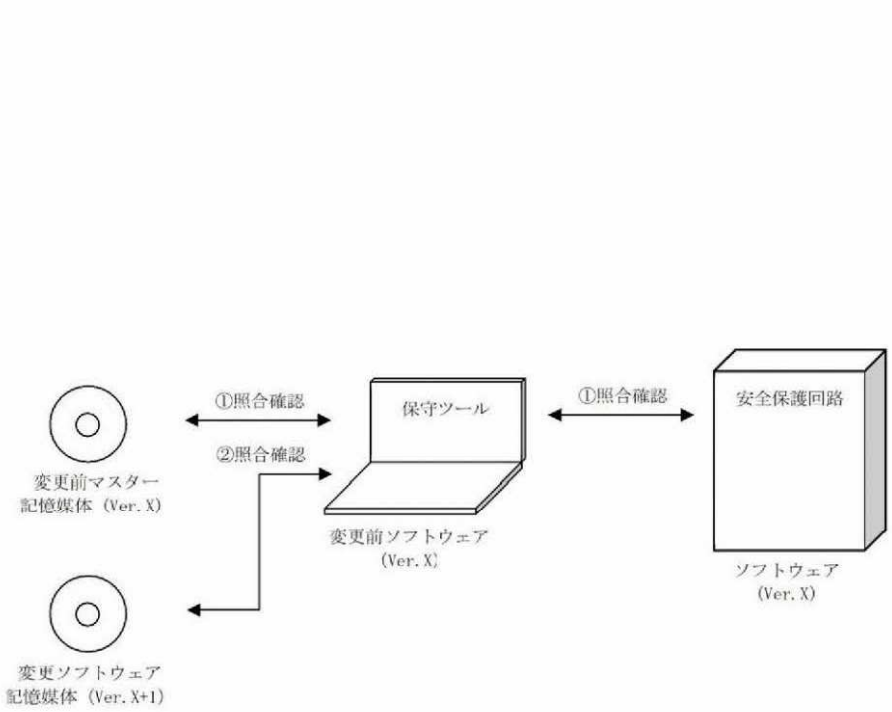


通信における分離概念図

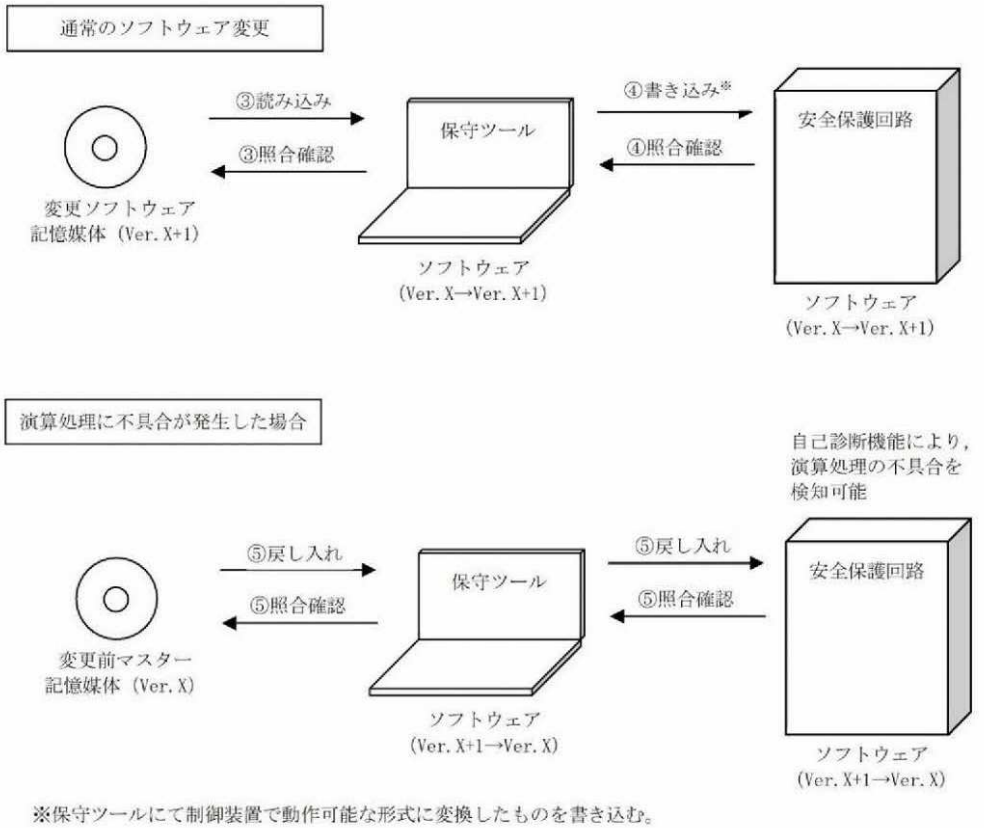
柏崎6/7号炉と同様の方針

ソフトウェア変更作業におけるソフトウェア不具合対応

- ソフトウェア変更作業において万が一，ウイルス，バグ等が安全保護回路に書き込まれることにより，ソフトウェアの演算処理に不具合が発生した場合は，自己診断機能により演算処理の不具合を検知することが可能。
- ウイルス，バグ等を発見した場合は，マスター用に保管している外部記憶媒体から変更作業前のバージョンのソフトウェアを安全保護回路に書き込み，変更作業前の状態に復元することが可能。



ソフトウェア変更作業の流れ（ソフトウェア変更前）



ソフトウェア変更作業の流れ（ソフトウェア変更）

女川２号炉と同様の方針

安全保護回路に変更を施している場合の基準適合性

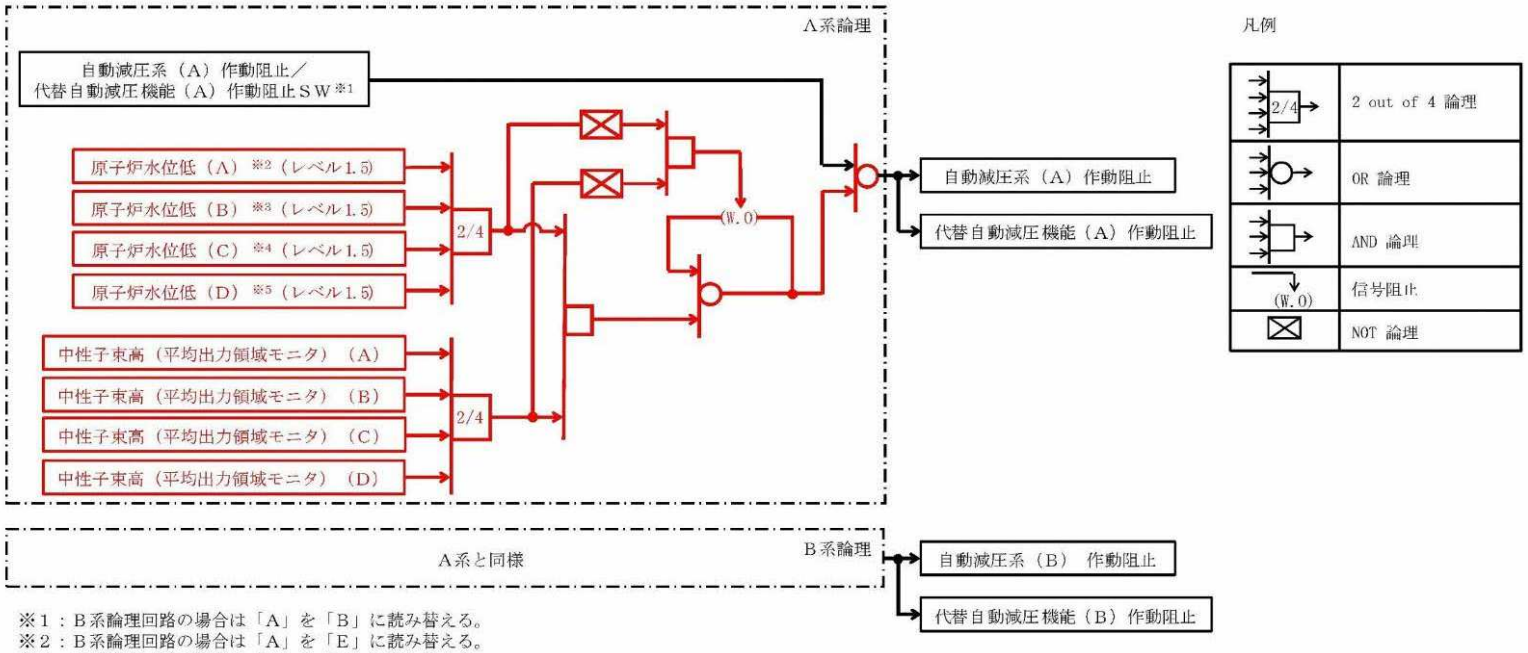
ＡＴＷＳ緩和設備（自動減圧系作動阻止機能）を追加（44条,46条）

■ 【目的】

原子炉停止機能喪失事象においては，原子炉が臨界状態にあるため，自動減圧系が作動すると，高圧炉心注水系及び低圧注水系から大量の冷水が注水され出力の急激な上昇につながる。このため原子炉停止機能喪失事象発生時に自動減圧系及び代替自動減圧ロジック（代替自動減圧機能）が作動しないように，ＡＴＷＳ緩和設備（自動減圧系作動阻止機能）を設置する。

■ 【安全保護回路への影響評価】

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ＡＴＷＳ緩和設備（自動減圧系作動阻止機能）を設置しており，単一故障による誤動作防止のため，２ out of 4論理により動作する設計とする。



※1：B系論理回路の場合は「A」を「B」に読み替える。
※2：B系論理回路の場合は「A」を「E」に読み替える。
※3：B系論理回路の場合は「B」を「F」に読み替える。
※4：B系論理回路の場合は「C」を「G」に読み替える。
※5：B系論理回路の場合は「D」を「H」に読み替える。

ＡＴＷＳ緩和設備（自動減圧系作動阻止機能）回路図