

島根原子力発電所 2 号炉 審査資料	
資料番号	EP-024 改 06 (比)
提出年月日	令和 2 年 9 月 30 日

島根原子力発電所 2 号炉

安全保護回路

比較表

令和 2 年 9 月

中国電力株式会社

実線・・・設備運用又は体制等の相違（設計方針の相違）
波線・・・記載表現，設備名称の相違（実質的な相違なし）

まとめ資料比較表　〔第 24 条　安全保護回路〕

柏崎刈羽原子力発電所　6／7号炉　（2017. 12. 20 版）	東海第二発電所（2018. 9. 18 版）	島根原子力発電所　2号炉	備考																												
比較表において、相違理由を類型化したものについて以下にまとめて記載する。下記以外の相違については、備考欄に相違理由を記載する。 <table><tr><th>相違No.</th><th>相違理由</th></tr><tr><td>①</td><td>島根 2 号炉は、追加要求事項への適合性については、「2. 追加要求事項に対する適合方針」以降に記載している</td></tr><tr><td>②</td><td>島根 2 号炉は、安全保護回路のうち論理回路はアナログのため</td></tr><tr><td>③</td><td>島根 2 号炉は、安全保護回路のうち一部デジタル演算処理を行う機器があり、ソフトウェアの検証及び妥当性確認について記載</td></tr><tr><td>④</td><td>島根 2 号炉の安全保護回路は一部デジタル演算処理を行う機器がある他は、アナログ回路で構成している</td></tr><tr><td>⑤</td><td>設備構成の相違による運用の相違（島根 2 号炉は保守ツールの接続部の施錠管理については、接続部は盤内にあるため盤を施錠管理している。他については同様）</td></tr><tr><td>⑥</td><td>島根 2 号炉で使用する保守ツールは送信機能もある</td></tr><tr><td>⑦</td><td>島根 2 号炉で使用するアナログ型安全保護回路は、 J E A C 4620、 J E A G 4609の適用対象外</td></tr><tr><td>⑧</td><td>柏崎6/7は光ケーブルの耐性の説明であり、島根 2 号炉は金属シールド付ケーブルを使用しノイズ等の対策を図っている</td></tr><tr><td>⑨</td><td>島根 2 号炉は、アナログ型安全保護回路による設備構成であり、一部のデジタル部については、保守ツール及び小型記憶媒体からのウィルス侵入が考えられることから供給者に対して要求し対策を図っている</td></tr><tr><td>⑩</td><td>デジタル型・アナログ型安全保護回路による論理回路の相違（島根 2 号炉はソフトウェアを使用していないハードワイヤの論理回路であるため）</td></tr><tr><td>⑪</td><td>島根 2 号炉は、アナログ型安全保護回路による設備構成であり、一部のデジタル部については、保守ツールから不正アクセスが考えられることから、保守ツールと安全保護系盤等の施錠管理を行っている</td></tr><tr><td>⑫</td><td>デジタル化している設備の相違</td></tr><tr><td>⑬</td><td>東海第二の設備の一部は、海外製であり、米国の基準に準拠して、検証及び妥当性確認を行っている</td></tr></table>				相違No.	相違理由	①	島根 2 号炉は、追加要求事項への適合性については、「2. 追加要求事項に対する適合方針」以降に記載している	②	島根 2 号炉は、安全保護回路のうち論理回路はアナログのため	③	島根 2 号炉は、安全保護回路のうち一部デジタル演算処理を行う機器があり、ソフトウェアの検証及び妥当性確認について記載	④	島根 2 号炉の安全保護回路は一部デジタル演算処理を行う機器がある他は、アナログ回路で構成している	⑤	設備構成の相違による運用の相違（島根 2 号炉は保守ツールの接続部の施錠管理については、接続部は盤内にあるため盤を施錠管理している。他については同様）	⑥	島根 2 号炉で使用する保守ツールは送信機能もある	⑦	島根 2 号炉で使用するアナログ型安全保護回路は、 J E A C 4620、 J E A G 4609の適用対象外	⑧	柏崎6/7は光ケーブルの耐性の説明であり、島根 2 号炉は金属シールド付ケーブルを使用しノイズ等の対策を図っている	⑨	島根 2 号炉は、アナログ型安全保護回路による設備構成であり、一部のデジタル部については、保守ツール及び小型記憶媒体からのウィルス侵入が考えられることから供給者に対して要求し対策を図っている	⑩	デジタル型・アナログ型安全保護回路による論理回路の相違（島根 2 号炉はソフトウェアを使用していないハードワイヤの論理回路であるため）	⑪	島根 2 号炉は、アナログ型安全保護回路による設備構成であり、一部のデジタル部については、保守ツールから不正アクセスが考えられることから、保守ツールと安全保護系盤等の施錠管理を行っている	⑫	デジタル化している設備の相違	⑬	東海第二の設備の一部は、海外製であり、米国の基準に準拠して、検証及び妥当性確認を行っている
相違No.	相違理由																														
①	島根 2 号炉は、追加要求事項への適合性については、「2. 追加要求事項に対する適合方針」以降に記載している																														
②	島根 2 号炉は、安全保護回路のうち論理回路はアナログのため																														
③	島根 2 号炉は、安全保護回路のうち一部デジタル演算処理を行う機器があり、ソフトウェアの検証及び妥当性確認について記載																														
④	島根 2 号炉の安全保護回路は一部デジタル演算処理を行う機器がある他は、アナログ回路で構成している																														
⑤	設備構成の相違による運用の相違（島根 2 号炉は保守ツールの接続部の施錠管理については、接続部は盤内にあるため盤を施錠管理している。他については同様）																														
⑥	島根 2 号炉で使用する保守ツールは送信機能もある																														
⑦	島根 2 号炉で使用するアナログ型安全保護回路は、 J E A C 4620、 J E A G 4609の適用対象外																														
⑧	柏崎6/7は光ケーブルの耐性の説明であり、島根 2 号炉は金属シールド付ケーブルを使用しノイズ等の対策を図っている																														
⑨	島根 2 号炉は、アナログ型安全保護回路による設備構成であり、一部のデジタル部については、保守ツール及び小型記憶媒体からのウィルス侵入が考えられることから供給者に対して要求し対策を図っている																														
⑩	デジタル型・アナログ型安全保護回路による論理回路の相違（島根 2 号炉はソフトウェアを使用していないハードワイヤの論理回路であるため）																														
⑪	島根 2 号炉は、アナログ型安全保護回路による設備構成であり、一部のデジタル部については、保守ツールから不正アクセスが考えられることから、保守ツールと安全保護系盤等の施錠管理を行っている																														
⑫	デジタル化している設備の相違																														
⑬	東海第二の設備の一部は、海外製であり、米国の基準に準拠して、検証及び妥当性確認を行っている																														

柏崎刈羽原子力発電所 6／7号炉 (2017.12.20版)	東海第二発電所 (2018.9.18版)	島根原子力発電所 2号炉	備考
第24条：安全保護回路	第 24 条 安全保護回路	第 24 条：安全保護回路	
＜目 次＞	＜目 次＞	＜目 次＞	
1. 基本方針	1. 基本方針	1. 基本方針	
1.1 要求事項の整理	1.1 要求事項の整理	1.1 要求事項の整理	
2. 追加要求事項に対する適合方針	<u>1.2 追加要求事項に対する適合性</u>	<u>2. 追加要求事項に対する適合方針</u>	・資料構成の相違 【東海第二】 島根2号炉は、追加要求事項への適合性については、「2.追加要求事項に対する適合方針」以降に記載している（以下、①の相違）
	<u>(1) 位置、構造及び設備</u>		
	<u>(2) 安全設計方針</u>		
	<u>(3) 適合性説明</u>		
	<u>1.3 気象等</u>		
	<u>1.4 設備等（手順等含む）</u>		
	2. 安全保護回路		
2.1 <u>安全保護系の不正アクセス行為防止のための措置について</u>	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	2.1 <u>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</u>	
2.2 <u>安全保護系盤の概要</u>	2.2 安全保護回路の概要	2.2 <u>安全保護回路の概要</u>	・設備の相違 【柏崎 6/7】 島根2号炉は、安全保護回路のうち論理回路はアナログのため（以下、②の相違）
<u>2.3 安全保護系制御装置のソフトウェア管理方法について</u>	2.3 安全保護回路の物理的分離対策	2.3 <u>安全保護回路の物理的分離対策</u>	
2.4 外部からの不正アクセス行為防止について	2.4 外部からの不正アクセス行為防止について	2.4 外部からの不正アクセス行為防止について	
<u>2.5 安全保護系の検証及び妥当性確認について</u>	2.5 想定脅威に対する対策について	2.5 想定脅威に対する対策について	・設備の相違 【柏崎 6/7】 ②の相違
2.6 想定脅威に対する対策について	2.6 物理的分離及び電気的分離について	2.6 物理的分離及び電気的分離について	
2.7 物理的分離及び電気的分離について			
<u>2.8 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</u>			・設備の相違 【柏崎 6/7】 ②の相違
3. 別紙		3. <u>別紙</u>	
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	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設計方針	別紙1 <u>アナログ型</u> 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	
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	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	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	
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	別紙3 安全保護回路の不正アクセス行為等の防止対策	別紙3 <u>アナログ型</u> 安全保護回路の不正アクセス行為等の防	

柏崎刈羽原子力発電所 6／7号炉 (2017.12.20版)	東海第二発電所 (2018.9.18版)	島根原子力発電所 2号炉	備考
対策 別紙4 ソフトウェア更新時の立会において、インサイダー等に対するセキュリティ対策 別紙5 <u>デジタル型安全保護回路</u>のシステムへ接続可能なアクセスについて 別紙6 <u>デジタル型安全保護回路</u>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 4. 別添 別添 運用，手順説明資料 安全保護回路	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 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 安全保護回路のうち一部デジタル演算処理を行う機器のソフトウェアの検証及び妥当性確認について 別紙8 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. <u>運用，手順説明資料</u> <u>(別添資料)</u> 安全保護回路	止対策 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 別紙5 <u>安全保護回路のうちデジタル部分</u>のシステムへ接続可能なアクセスについて 別紙6 <u>安全保護回路のうちデジタル部分</u>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 別紙8 <u>安全保護回路のうち一部デジタル演算処理を行う機器のソフトウェアの検証及び妥当性確認について</u> 4. <u>別添</u> 別添 <u>島根原子力発電所2号炉</u> 運用，手順説明資料 安全保護回路	・設備の相違 【柏崎6/7】 島根2号炉は，安全保護回路のうち一部デジタル演算処理を行う機器があり，ソフトウェアの検証及び妥当性確認について記載（以下，③の相違）

柏崎刈羽原子力発電所 6 / 7 号炉 (2017.12.20 版)	東海第二発電所 (2018.9.18 版)	島根原子力発電所 2 号炉	備考
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）。	<u><概 要></u> <u>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。</u> <u>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。</u> <u>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。</u> 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）	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 1.1－1 表）。	・資料構成の相違 【東海第二】 ①の相違

柏崎刈羽原子力発電所 6／7号炉 (2017.12.20版)	東海第二発電所 (2018.9.18版)	島根原子力発電所 2号炉	備考																																																
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	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	第 1.1－1 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																																																	
<table><tr><th>設置許可基準規則 第 24 条（安全保護回路）</th><th>技術基準規則 第 35 条（安全保護装置）</th><th>備 考</th></tr><tr><td>発電用原子炉施設には、次に掲げるところにより、安全保護回路（安全施設に属するものに限る。以下この条において同じ。）を設けなければならない。</td><td>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。</td><td>変更なし</td></tr><tr><td>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。</td><td>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。</td><td>変更なし</td></tr><tr><td>二 設計基準事故が発生する場合において、その異常な状態を検知し、原子炉停止系統及び工学的安全施設を自動的に作動させるものとする。</td><td>—</td><td>変更なし</td></tr><tr><td>三 安全保護回路を構成する機械若しくは器具又はチャンネルは、単一故障が起きた場合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。</td><td>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。</td><td>変更なし</td></tr></table>	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。	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。	—	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。	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	<table><tr><th>設置許可基準規則 第 24 条（安全保護回路）</th><th>技術基準規則 第 35 条（安全保護装置）</th><th>備 考</th></tr><tr><td>発電用原子炉施設には、次に掲げるところにより、安全保護回路（安全施設に属するものに限る。以下この条において同じ。）を設けなければならない。</td><td>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。</td><td>変更なし</td></tr><tr><td>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。</td><td>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。</td><td>変更なし</td></tr><tr><td>二 設計基準事故が発生する場合において、その異常な状態を検知し、原子炉停止系統及び工学的安全施設を自動的に作動させるものとする。</td><td>—</td><td>変更なし</td></tr><tr><td>三 安全保護回路を構成する機械若しくは器具又はチャンネルは、単一故障が起きた場合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。</td><td>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。</td><td>変更なし</td></tr><tr><td>四 安全保護回路を構成するチャンネルは、それぞれ互いに分離し、それぞれのチャンネル間において安全保護機能を失わないように独立性を確保するものとする。</td><td>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。</td><td>変更なし</td></tr></table>	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。	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。	—	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。	二 系統を構成する機械若しくは器具又はチャンネルは、単一故障が起きた場合又は使用状態からの単一の取り外しを行った場合において、安全保護機能を失わないよう、多重性を確保すること。	変更なし	四 安全保護回路を構成するチャンネルは、それぞれ互いに分離し、それぞれのチャンネル間において安全保護機能を失わないように独立性を確保するものとする。	三 系統を構成するチャンネルは、それぞれ互いに分離し、それぞれのチャンネル間において安全保護機能を失わないように独立性を確保すること。	変更なし	<table><tr><th>設置許可基準規則 第 24 条（安全保護回路）</th><th>技術基準規則 第 35 条（安全保護装置）</th><th>備考</th></tr><tr><td>発電用原子炉施設には、次に掲げるところにより、安全保護回路（安全施設に属するものに限る。以下この条において同じ。）を設けなければならない。</td><td>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。</td><td>変更なし</td></tr><tr><td>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。</td><td>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。</td><td>変更なし</td></tr><tr><td>二 設計基準事故が発生する場合において、その異常な状態を検知し、原子炉停止系統及び工学的安全施設を自動的に作動させるものとする。</td><td>—</td><td>変更なし</td></tr><tr><td>三 安全保護回路を構成する機械若しくは器具又はチャンネルは、単一故障が起きた場合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。</td><td>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。</td><td>変更なし</td></tr></table>	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。	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。	—	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。	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	
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。	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。	—	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。	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																																																	
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。	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。	—	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。	二 系統を構成する機械若しくは器具又はチャンネルは、単一故障が起きた場合又は使用状態からの単一の取り外しを行った場合において、安全保護機能を失わないよう、多重性を確保すること。	変更なし																																																	
四 安全保護回路を構成するチャンネルは、それぞれ互いに分離し、それぞれのチャンネル間において安全保護機能を失わないように独立性を確保するものとする。	三 系統を構成するチャンネルは、それぞれ互いに分離し、それぞれのチャンネル間において安全保護機能を失わないように独立性を確保すること。	変更なし																																																	
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。	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。	—	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。	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																																																	

柏崎刈羽原子力発電所 6／7号炉 (2017. 12. 20 版)			東海第二発電所 (2018. 9. 18 版)			島根原子力発電所 2号炉			備考
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	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	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	
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	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	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	
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				
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 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				
—	七 発電用原子炉の運転中に、その能力を確認するための必要な試験ができるものである こと。 八 運転条件に応じて作動設定値を変更できるものである こと。	変更なし	—	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				

柏崎刈羽原子力発電所 6／7号炉 (2017.12.20版)	東海第二発電所 (2018.9.18版)	島根原子力発電所 2号炉	備考
	<u>1.2. 追加要求事項に対する適合性</u> <u>(1) 位置、構造及び設備</u> <u>ロ 発電用原子炉施設の一般構造</u> <u>(3) その他の主要な構造</u> <u>(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。</u> <u>a. 設計基準対象施設</u> <u>(s) 安全保護回路</u> <u>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。</u> <u>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。</u> <u>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。</u> <u>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。</u> <u>安全保護回路のうち、一部デジタル演算処理を行う機器は、不正アクセス行為に対する安全保護回路の物理的分離及び機能的分離を行うとともに、ソフトウェアは設計、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。</u> <u>【説明資料 (2.1:P24条-37,38) (2.2:P24条-39) (2.3:P24条-40) (2.4:P24条-41) (2.5:P24条-42) (2.6:P24条-42,43)】</u> <u>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</u>		・資料構成の相違 【東海第二】 ①の相違

柏崎刈羽原子力発電所 6／7号炉 (2017.12.20版)	東海第二発電所 (2018.9.18版)	島根原子力発電所 2号炉	備考
	<u>離した設計とする。</u> <u>へ 計測制御系統施設の構造及び設備</u> <u>発電用原子炉の適切かつ安全な運転のため、中性子束を測定する炉内核計装設備と水位、圧力、再循環流量等を測定する計装設備、安全保護回路及び制御設備を設ける。また、通常運転中の原子炉圧力を一定に保つために、圧力制御装置を設ける。</u> <u>発電用原子炉の出力制御は、再循環流量の調整及び制御棒位置の調整の2方式により行われる。</u> <u>(1) 計 装</u> <u>(i) 核計装の種類</u> <u>中性子束は以下のように2つの領域に分けて原子炉内で計測する。</u> <u>起動領域：固定型計数方式及び 8チャンネル</u> <u>キャンベル方式計装</u> <u>出力領域：固定型直流方式計装 172チャンネル</u> <u>(ii) その他の主要な計装の種類</u> <u>原子炉水位、原子炉圧力、再循環流量、給水流量、蒸気流量、制御棒位置、制御棒駆動用冷却材圧力等の計装装置を設ける。</u> <u>(2) 安全保護回路</u> <u>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。</u> <u>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。</u> <u>【説明資料（2.1：P24条-37,38）（2.2：P24条-39）（2.3：P24条-40）（2.4：P24条-41）（2.5：P24条-42）（2.6：P24条-42,43）】</u> <u>(i) 原子炉停止回路の種類</u> <u>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発電用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発電用原子炉をスクラムさせる。</u> <u>a. 原子炉圧力高</u> <u>b. 原子炉水位低</u> <u>c. ドライウェル圧力高</u>		

柏崎刈羽原子力発電所 6／7号炉 (2017.12.20版)	東海第二発電所 (2018.9.18版)	島根原子力発電所 2号炉	備考
	<u>d. 原子炉出力ペリオド短 (起動領域計装)</u> <u>e. 中性子束高 (起動及び平均出力領域計装)</u> <u>f. 中性子束低 (平均出力領域計装)</u> <u>g. 中性子束計装動作不能 (起動及び平均出力領域計装)</u> <u>h. スクラム水排出容器水位高</u> <u>i. 主蒸気隔離弁閉</u> <u>j. 主蒸気管放射能高</u> <u>k. 主蒸気止め弁閉</u> <u>l. 蒸気加減弁急速閉</u> <u>m. 地震加速度大</u> <u>n. 原子炉モード・スイッチ「停止」</u> <u>o. 手 動</u> <u>なお、原子炉緊急停止系作動回路の電源喪失の場合にも発電用原子炉はスクラムする。</u> <u>(ii) その他の主要な安全保護回路の種類</u> <u>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。</u> <u>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</u> <u>b. ドライウエル圧力高、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</u> <u>c. 原子炉水位異常低下又はドライウエル圧力高の信号による高圧炉心スプレイ系、低圧炉心スプレイ系及び残留熱除去系 (低圧注水系) の起動</u> <u>d. 原子炉水位異常低下及びドライウエル圧力高の同時信号による自動減圧系の作動</u> <u>e. 原子炉水位異常低下又はドライウエル圧力高の信号による高圧炉心スプレイ系ディーゼル発電機及び非常用ディーゼル発電機の起動</u> <u>f. 原子炉水位低、原子炉水位異常低下、ドライウエ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</u> <u>また、その他保護動作としては次のようなものがある。</u> <u>a. 原子炉水位異常低下信号による原子炉隔離時冷却系の起動</u> <u>(2) 安全設計方針</u>		

柏崎刈羽原子力発電所 6／7号炉 (2017.12.20版)	東海第二発電所 (2018.9.18版)	島根原子力発電所 2号炉	備考
	<u>1.1.3 安全保護系の設計方針</u> <u>反応度制御系（制御棒）及び工学的安全施設の作動を開始させるための安全保護系は、多重性と独立性を有する設計とし、実際に起こると考えられる、いかなる単一故障によってもその安全保護機能が妨げられないような設計とする。また、安全保護系は系の遮断、駆動源の喪失等においても安全上許容される状態（フェイル・セイフ又はフェイル・アズ・イズ）になるよう設計する。</u> <u>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。</u> <u>【説明資料（2.1：P24条-37,38）（2.2：P24条-39）（2.3：P24条-40）（2.4：P24条-41）（2.5：P24条-42）（2.6：P24条-42,43）】</u> <u>(3) 適合性説明</u> <u>(安全保護回路)</u> <u>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。</u> <u>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。</u> <u>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。</u> <u>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。</u> <u>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。</u> <u>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。</u> <u>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</u>		

柏崎刈羽原子力発電所 6／7号炉 (2017.12.20版)	東海第二発電所 (2018.9.18版)	島根原子力発電所 2号炉	備考
	<u>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。</u> <u>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。</u> <u>適合のための設計方針</u> <u>第1項第1号について</u> <u>(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、燃料要素の許容損傷限界を超えることがない設計とする。</u> <u>(2) 安全保護系は、偶発的な制御棒引抜きのような原子炉停止系のいかなる単一誤動作に起因する異常な反応度印加が生じた場合でも、燃料要素の許容損傷限界を超えないよう、中性子束高スクラム及び原子炉出力ペリオド短スクラムにより発電用原子炉を停止できる設計とする。</u> <u>第1項第2号について</u> <u>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。</u> <u>(1) 発電用原子炉は、下記の条件の場合にスクラムする。</u> <u>a. 原子炉圧力高</u> <u>b. 原子炉水位低</u> <u>c. ドライウエル圧力高</u> <u>d. 原子炉出力ペリオド短（起動領域計装）</u> <u>e. 中性子束高（起動及び平均出力領域計装）</u> <u>f. 中性子束低（平均出力領域計装）</u> <u>g. 中性子束計装動作不能（起動及び平均出力領域計装）</u> <u>h. スクラム水排出容器水位高</u> <u>i. 主蒸気隔離弁閉</u> <u>j. 主蒸気管放射能高</u> <u>k. 主蒸気止め弁閉</u> <u>l. 蒸気加減弁急速閉</u> <u>m. 地震加速度大</u>		

柏崎刈羽原子力発電所 6／7号炉 (2017.12.20版)	東海第二発電所 (2018.9.18版)	島根原子力発電所 2号炉	備考
	<u>n. 原子炉モード・スイッチ「停止」</u> <u>o. 手 動</u> <u>(2) その他の主要な安全保護系（工学的安全施設作動回路）には、次のようなものを設ける設計とする。</u> <u>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</u> <u>b. ドライウエル圧力高，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</u> <u>c. 原子炉水位異常低下又はドライウエル圧力高の信号による高圧炉心スプレイ系，低圧炉心スプレイ系及び残留熱除去系（低圧注水系）の起動</u> <u>d. 原子炉水位異常低下及びドライウエル圧力高の同時信号による自動減圧系の作動</u> <u>e. 原子炉水位異常低下又はドライウエル圧力高の信号による高圧炉心スプレイ系ディーゼル発電機及び非常用ディーゼル発電機の起動</u> <u>f. 原子炉水位低，原子炉水位異常低下，ドライウエ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</u> <u>また，その他保護動作としては次のようなものがある。</u> <u>a. 原子炉水位異常低下信号による原子炉隔離時冷却系の起動</u> <u>第1項第3号について</u> <u>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。</u> <u>具体例は下記のとおりである。</u> <u>(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。</u> <u>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り外した場合，回路が無励磁状態で，チャンネル・トリップになるようにする。</u>		

柏崎刈羽原子力発電所 6／7号炉 (2017.12.20版)	東海第二発電所 (2018.9.18版)	島根原子力発電所 2号炉	備考
	<u>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。</u> <u>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。</u> <u>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。</u> <u>(2) 工学的安全施設を作動させるチャンネル（検出器を含む）は、多重性をもった構成とする。</u> <u>したがって、これらの単一故障、使用状態からの単一の取外しを行った場合においても、その安全保護機能を維持できる。</u> <u>第1項第4号について</u> <u>安全保護系は、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。</u> <u>具体例は下記のとおりである。</u> <u>(1) 原子炉格納容器を貫通する計装配管は、物理的に独立した貫通部を有する2系列を設ける。</u> <u>(2) 検出器からのケーブル及び電源ケーブルは、独立に中央制御室の各盤に導く。各トリップチャンネルの論理回路は、盤内で独立して設ける。</u> <u>(3) 原子炉緊急停止系作動回路の電源は、分離・独立した母線から供給する。</u> <u>第1項第5号について</u> <u>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・セーフの設計とするか、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。</u> <u>フェイル・セーフとなるものの主要なものをあげると以下のとおりである。</u> <u>(1) 電源喪失</u> <u>a. スクラム</u>		

柏崎刈羽原子力発電所 6／7号炉 (2017.12.20版)	東海第二発電所 (2018.9.18版)	島根原子力発電所 2号炉	備考
	<u>b. 主蒸気隔離弁閉</u> <u>c. 格納容器ベント弁閉</u> <u>(2) 計器用空気喪失</u> <u>a. スクラム</u> <u>b. 格納容器ベント弁閉</u> <u>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。</u> <u>系統の遮断やその他、火災、浸水等不利な状況が発生した場合でも、この工学的安全施設作動回路及び工学的安全施設自体が多重性、独立性を持つことで発電用原子炉施設を十分に安全な状態に導くよう設計する。</u> <u>第1項第6号について</u> <u>安全保護系のうち、一部デジタル演算処理を行う機器は、これが収納された盤の施錠等により、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（片方向のみの通信を許可する装置）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するとともに、固有のプログラム言語の使用による一般的なコンピュータウイルスが動作しない環境等によりウイルス等の侵入を防止することでソフトウェアの内部管理の強化を図り、外部からの不正アクセスを防止する設計とする。</u> <u>また、「安全保護系へのデジタル計算機の適用に関する規程」（JEAC4620-2008）及び「デジタル安全保護系の検証及び妥当性確認に関する指針」（JEAG4609-2008），又は米国Regulatory Guide 1.152「原子力発電所安全関連システムのプログラマブルデジタル計算機システムソフトウェアの基準」に準じて設計、製作、試験及び変更管理の各段階で検証及び妥当性確認（コンピュータウ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とともに、発電所での出入管理による物理的アクセスの制限並びに設定値変更作業での鍵管理及びパスワード管理により、不正な変更等による承認されていない動作や変更を防止する設計とする。</u> <u>【説明資料（2.1：P24条-37,38）（2.2：P24条-39）（2.3：P24</u>		

柏崎刈羽原子力発電所 6／7号炉 (2017.12.20版)	東海第二発電所 (2018.9.18版)	島根原子力発電所 2号炉	備考
	<u>条-40) (2.4:P24条-41) (2.5:P24条-42) (2.6:P24条-42,43)】</u> <u>第1項第7号について</u> <u>安全保護系と計測制御系とは、電源、検出器、ケーブル・ルート及び原子炉格納容器を貫通する計装配管を、原則として分離する設計とする。</u> <u>安全保護系は、原子炉水位及び原子炉圧力を検出する計装配管ヘッダの一部を計測制御系と共用すること及び核計装等の検出部が表示、記録計用検出部と共用される以外は計測制御系とは完全に分離する等、計測制御系での故障が安全保護系に影響を与えない設計とする。</u> <u>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。</u> <u>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。</u> <u>1.3 気象等</u> <u>該当なし</u> <u>1.4 設備等（手順等含む）</u> <u>6. 計測制御系統施設</u> <u>6.3 原子炉プラント・プロセス計装</u> <u>6.3.1 概 要</u> <u>発電用原子炉の適切かつ安全な運転のため、核計装のほかに、発電用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。</u> <u>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他の計装から構成されている。</u> <u>発電用原子炉の停止、炉心冷却及び放射性物質の閉じ込めの機能の状況を監視するために必要なパラメータは、設計基準事故時においても監視でき確実に記録及び保存ができる。</u>		

柏崎刈羽原子力発電所 6／7号炉 (2017.12.20版)	東海第二発電所 (2018.9.18版)	島根原子力発電所 2号炉	備考
	<u>6.3.2 設計方針</u> <u>(1) 通常運転時及び運転時の異常な過渡変化時において、炉心、原子炉冷却材圧力バウンダリ及び原子炉格納容器バウンダリ並びにそれらに関連する系統の健全性を確保するために必要なパラメータは、予想変動範囲内での監視が可能であるようにプロセス計装を設ける設計とする。</u> <u>(2) 設計基準事故時において、事故の状態を知り対策を講じるのに必要なパラメータを監視できるようにプロセス計装を設ける設計とする。</u> <u>(3) 安全保護系に関連する原子炉プラント・プロセス計装は、「6.6 安全保護系」に記載する設計方針(4)～(9)を満足するように設計する。</u> <u>(4) 原子炉冷却材圧力バウンダリからの冷却材の漏えいがあった場合、その漏えいを検出するのに必要なプロセス計装を設ける設計とする。</u> <u>(5) 安全確保上最も重要な原子炉停止、炉心冷却及び放射能閉じ込めの3つの機能の状況を監視するのに必要な炉心の中性子束、原子炉水位及び原子炉冷却材系の圧力及び温度等は、設計基準事故時においても記録されるとともに事象経過後に参照できるように当該記録が保存できる設計とする。</u> <u>6.3.3 主要設備の仕様</u> <u>原子炉プラント・プロセス計装の一覧を第6.3-1表に示す。</u> <u>6.3.4 主要設備</u> <u>(1) 原子炉圧力容器計装</u> <u>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。</u> <u>原子炉水位は、連続的に測定され、指示及び記録される。原子炉水位低又は水位高で警報を出す。原子炉水位低下が更に大きい場合には、原子炉緊急停止系及び工学的安全施設を作動させるとともに再循環系ポンプをトリップする信号を出す。また、原子炉水位上昇が更に大きい場合にはタービン・トリップを行わせるための信号を出す（第6.3-1図参照）。</u> <u>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。</u>		

柏崎刈羽原子力発電所 6／7号炉 (2017.12.20版)	東海第二発電所 (2018.9.18版)	島根原子力発電所 2号炉	備考
	<u>原子炉压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。</u> <u>原子炉压力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、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。</u> <u>(2) 再循環回路計装</u> <u>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。再循環系ポンプについては、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。</u> <u>(3) 原子炉給水系及び蒸気系計装</u> <u>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。</u> <u>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。</u> <u>(4) 制御棒駆動機構計装</u> <u>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、水圧制御ユニットアキュムレータ及びスクラム水排出容器、並びに制御棒位置指示に対して、それぞれ適当なプロセス計装が設けられている。</u> <u>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。</u> <u>通常の駆動水圧系では、発電用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）等が計測される。</u> <u>水圧制御ユニットアキュムレータ及びスクラム水排出容器系では、アキュムレータ窒素圧力、アキュムレータの漏えい水量、スクラム水排出容器水位等が計測され、アキュムレータの圧力低と水位高、スクラム水排出容器の水位高で警報が出される。スクラム水排出容器の水位が更に高くなれば、発電用原子炉はスクラムされる。</u>		

柏崎刈羽原子力発電所 6／7号炉 (2017.12.20版)	東海第二発電所 (2018.9.18版)	島根原子力発電所 2号炉	備考
	<u>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。</u> <u>(5) 原子炉格納容器内雰囲気計装</u> <u>原子炉格納容器（以下6.では「格納容器」という。）について計測する主要な項目は、格納容器内の圧力、温度、湿度、水素濃度、酸素濃度及び放射線レベルである。</u> <u>格納容器内の圧力、温度及び酸素濃度は、連続的に測定し、指示又は記録する。また、冷却材喪失事故後の格納容器内の圧力、温度、水素濃度、酸素濃度、放射線レベル等も測定し、記録する。その他、ドライウェルの湿度並びにサプレッション・チェンバのプール水位及び水温も連続的に測定し、指示又は記録する。</u> <u>ドライウェル圧力高、水素濃度高及び酸素濃度高で警報を出す。ドライウェル圧力の上昇が更に大きい場合には、原子炉緊急停止系及び工学的安全施設を作動させるための信号を出す（第6.6－3図及び第6.6－5図参照）。</u> <u>サプレッション・チェンバでは、プール水位低、プール水位高、プール水温高、水素濃度高及び酸素濃度高で警報を出す。</u> <u>(6) 漏えい検出系計装</u> <u>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、格納容器床ドレン流量、格納容器機器ドレン流量及び格納容器雰囲気中の核分裂生成物の放射性物質濃度の測定により約3.8L／minの漏えいを1時間以内に検出できるようにする。測定値は、指示するとともに、原子炉冷却材の漏えい量が多い場合には警報を出す。</u> <u>(7) その他の原子炉プラント・プロセス計装</u> <u>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。</u> <u>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。</u> <u>6.3.5 試験検査</u> <u>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。</u>		

柏崎刈羽原子力発電所 6／7号炉 (2017.12.20版)	東海第二発電所 (2018.9.18版)	島根原子力発電所 2号炉	備考
	<u>6.3.6 評価</u> <u>(1) 原子炉プラント・プロセス計装は、通常運転時及び運転時の異常な過渡変化時において、炉心、原子炉冷却材圧力バウンダリ及び格納容器バウンダリ並びにそれらに関連する系統の健全性を確保するために必要なパラメータを予想変動範囲内で監視することができる設計としている。</u> <u>(2) 原子炉プラント・プロセス計装は、設計基準事故時において、事故の状態を知り対策を講じるのに必要なパラメータを監視することができる設計としている。</u> <u>(3) 安全保護系に関連する原子炉プラント・プロセス計装は、「6.6 安全保護系」に記載する設計方針(4)～(9)を満足する設計としている。</u> <u>(4) 原子炉プラント・プロセス計装は、原子炉冷却材圧力バウンダリからの冷却材の漏えいがあった場合、その漏えいを検出することができる設計としている。</u> <u>6.6 安全保護系</u> <u>6.6.1 概要</u> <u>安全保護系は、発電用原子炉の安全性を損なうおそれのある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、発電用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、電氣的に分離し、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。</u> <u>6.6.2 設計方針</u> <u>(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、燃料要素の許容損傷限界を超えないようにする。</u> <u>(2) 安全保護系は、偶発的な制御棒引抜きのような原子炉停止系のいかなる単一の誤動作に対しても、燃料要素の許容損傷限界を超えないようにする。</u> <u>(3) 安全保護系は、設計基準事故時にあつては、直ちにこれを検知し、原子炉緊急停止系及び工学的安全施設の作動を自動的に</u>		

柏崎刈羽原子力発電所 6／7号炉 (2017.12.20版)	東海第二発電所 (2018.9.18版)	島根原子力発電所 2号炉	備考
	<u>開始させる。</u> <u>(4) 安全保護系は、多重性及び電氣的・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。</u> <u>(5) 安全保護系は、系統の遮断、駆動源の喪失においても、安全上許容される状態（フェイル・セイフ又はフェイル・アズ・イズ）になるようにする。</u> <u>(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。</u> <u>(7) 安全保護系は、通常運転中においても、定期的に機能試験を行うことができるようにする。</u> <u>(8) 安全保護系は、監視装置、警報等によりその作動状況が確認できる設計とする。</u> <u>(9) 安全保護系は、不正アクセス行為その他の電子計算機に使用目的に沿うべき動作をさせず、又は使用目的に反する動作をさせる行為による被害を防止することができる設計とする。</u> <u>【説明資料 (2.1：P24条-37,38) (2.2：P24条-39) (2.3：P24条-40) (2.4：P24条-41) (2.5：P24条-42) (2.6：P24条-42,43)】</u> <u>6.6.3 主要設備の仕様</u> <u>原子炉緊急停止系作動回路の主要設備の仕様を第6.6-1表、第6.6-1図及び第6.6-3図に、その他の主要な安全保護系の仕様を第6.6-2表、第6.6-4図及び第6.6-5図に示す。</u> <u>6.6.4 主要設備</u> <u>(1) 原子炉緊急停止系の機能</u> <u>原子炉緊急停止系は、第6.6-1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、発電用原子炉がスクラムされるようになっている。</u> <u>発電用原子炉は、下記の条件の場合にスクラムされる。</u> <u>a. 原子炉圧力高</u> <u>b. 原子炉水位低</u> <u>c. ドライウェル圧力高</u>		

柏崎刈羽原子力発電所 6／7号炉 (2017.12.20版)	東海第二発電所 (2018.9.18版)	島根原子力発電所 2号炉	備考
	<u>d. 原子炉出力ペリオド短 (起動領域計装)</u> <u>e. 中性子束高 (起動及び平均出力領域計装)</u> <u>f. 中性子束低 (平均出力領域計装)</u> <u>g. 中性子束計装動作不能 (起動及び平均出力領域計装)</u> <u>h. スクラム水排出容器水位高</u> <u>i. 主蒸気隔離弁閉</u> <u>j. 主蒸気管放射能高</u> <u>k. 主蒸気止め弁閉</u> <u>l. 蒸気加減弁急速閉</u> <u>m. 地震加速度大</u> <u>n. 原子炉モード・スイッチ「停止」</u> <u>o. 手 動</u> <u>検出器の形式、配置場所及びスクラム設定値は、第 6.6-1 表に示すとおりである。</u> <u>この他、原子炉緊急停止系作動回路の電源喪失の場合にも発電用原子炉はスクラムする。</u> <u>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。</u> <u>(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 4.1MPa [gage] 以下のときには自動的にバイパスされ、スクラム水排出容器水位高によるスクラム信号も手動でバイパス可能である。</u> <u>(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 4.1MPa [gage] 以下のときは自動的にバイパスされる。さらに、スクラム水排出容器水位高によるスクラム信号も手動でバイパス可能であるが、この場合には制御棒を引き抜くことはできない。</u> <u>(c) 「起動」このモードは発電用原子炉を起動し、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、発電用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 4.1MPa [gage] 以下のときには自動的にバイパスされる。</u> <u>(d) 「運転」このモードでは、バイパスはすべて解除され、運</u>		

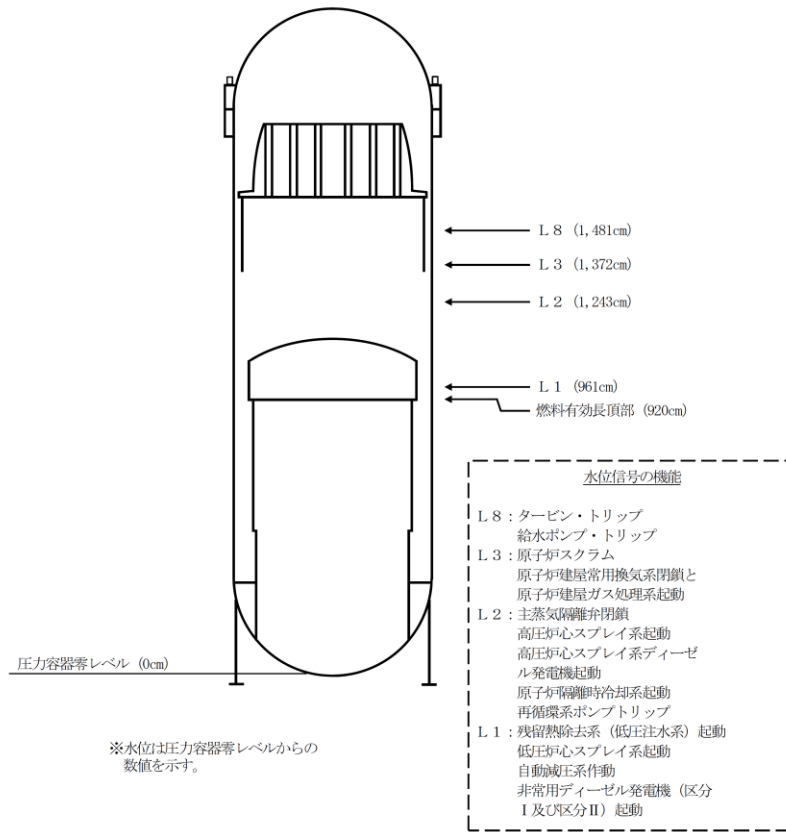
柏崎刈羽原子力発電所 6／7号炉 (2017.12.20版)	東海第二発電所 (2018.9.18版)	島根原子力発電所 2号炉	備考
	<u>転手順の上で特に許される場合にのみ保守上の目的で、個々の計器をバイパスさせることができる。</u> <u>(2) その他の主要な安全保護系の種類</u> <u>その他の主要な安全保護系（工学的安全施設作動回路）には、次のようなものを設ける。</u> <u>a. 原子炉水位異常低下、主蒸気管放射能高、主蒸気管圧力低、主蒸気管流量大、主蒸気管トンネル温度高、復水器真空度低のいずれかの信号による主蒸気隔離弁の閉鎖</u> <u>b. ドライウエル圧力高、原子炉水位低、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</u> <u>c. 原子炉水位異常低下又はドライウエル圧力高の信号による高圧炉心スプレイ系、低圧炉心スプレイ系及び残留熱除去系（低圧注水系）の起動</u> <u>d. 原子炉水位異常低下及びドライウエル圧力高の同時信号による自動減圧系の作動</u> <u>e. 原子炉水位異常低下又はドライウエル圧力高の信号による高圧炉心スプレイ系ディーゼル発電機及び非常用ディーゼル発電機の起動</u> <u>f. 原子炉水位低、原子炉水位異常低下、ドライウエ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</u> <u>また、その他保護動作としては次のようなものがある。</u> <u>a. 原子炉水位異常低下信号による原子炉隔離時冷却系の起動</u> <u>(3) 原子炉緊急停止系の動作</u> <u>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。</u> <u>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・セーフ”になっている。</u> <u>一方、接点の焼損又は溶着等“フェイル・セーフ”に反する方向の故障に対しては、各接点を流れる電流が定格の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</u>		

柏崎刈羽原子力発電所 6／7号炉 (2017.12.20版)	東海第二発電所 (2018.9.18版)	島根原子力発電所 2号炉	備考
	<u>いる。</u> <u>第6.6－1図に示すように、論理回路の継電器接点はすべて直列に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。</u> <u>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。</u> <u>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、発電用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。</u> <u>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。</u> <u>(4) リセット及び警報</u> <u>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、運転監視装置が、各検出器トリップの時間的順序を記録する。</u> <u>(5) 後備緊急停止系統</u> <u>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</u>		

柏崎刈羽原子力発電所 6／7号炉 (2017.12.20版)	東海第二発電所 (2018.9.18版)	島根原子力発電所 2号炉	備考
	<u>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発電用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。</u> <u>(6) 原子炉緊急停止系の電源回路</u> <u>原子炉緊急停止系の電源回路は、第6.6-2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ーが大きいので、瞬間的な電圧降下では原子炉スクラムは生じない。</u> <u>原子炉保護系用M-G装置(はずみ車付)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。</u> <u>6.6.5 試験検査</u> <u>(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。</u> <u>a. 手動スクラム・パイロット弁作動試験：手動スクラム・スイッチによるパイロット弁ソレノイドの無励磁の確認</u> <u>b. 自動スクラム・パイロット弁作動試験：各トリップ・チャンネルごとの鍵付テスト・スイッチによるトリップ・チャンネル及びパイロット弁ソレノイドの無励磁の確認</u> <u>c. 検出器作動試験：各検出器の校正用タップ及びトリップ・チャンネルの試験端子から校正用模擬信号を入れることによるトリップ・チャンネルの作動の確認</u> <u>d. 制御棒スクラム試験：手動スイッチによる同一水圧制御ユニットに属する1組又は1本の制御棒のスクラム時間の確認</u> <u>以上のうちb.及びc.の試験により、各チャンネルの独立性の確認も行うことができる。</u> <u>(2) 工学的安全施設作動回路は、原子炉運転中でもテスト信号</u>		

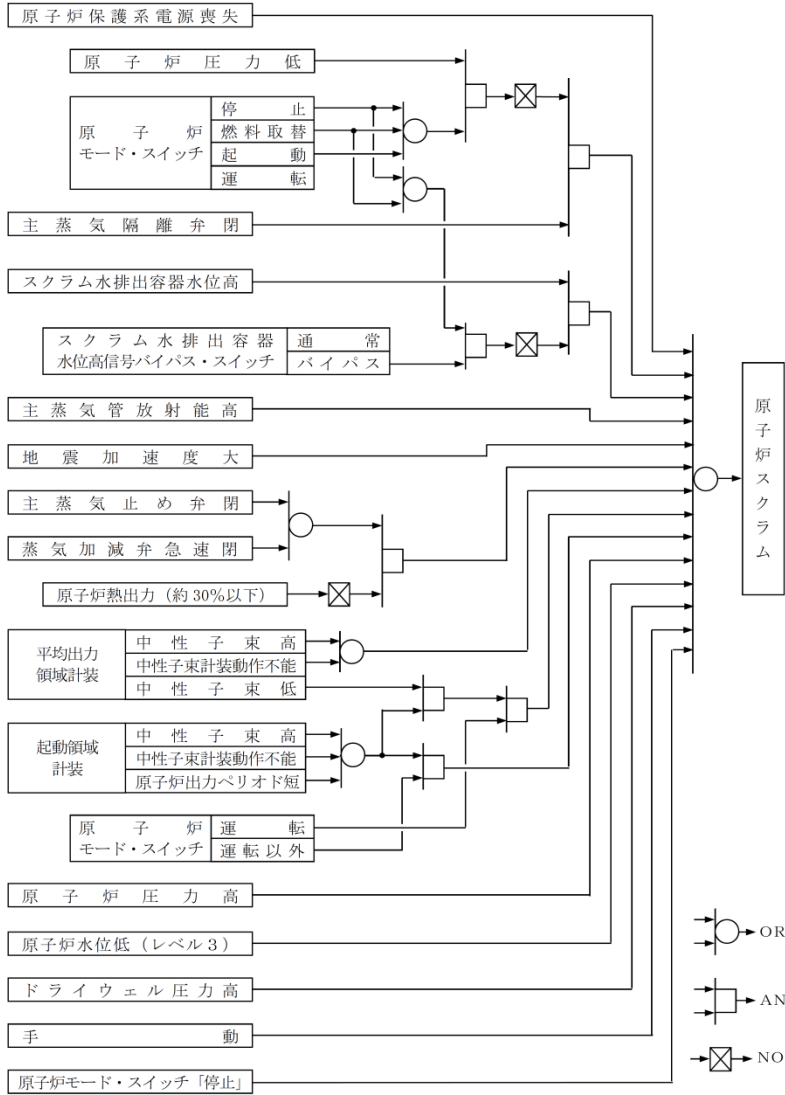
柏崎刈羽原子力発電所 6／7号炉 (2017.12.20版)	東海第二発電所 (2018.9.18版)	島根原子力発電所 2号炉	備考
	<u>によって各々のチャンネル（検出器含む）の試験を行うことができ、定期的にその機能が喪失していないことを確認できる。</u> <u>なお、論理回路を含む全系統の試験については、原子炉停止時に行うことができる。</u> <u>6.6.6 手順等</u> <u>安全保護系に関して、以下の内容を含む手順等を定め、適切な管理を行う。</u> <u>(1) 安全保護回路を有する制御盤については、施錠管理方法を定め、運用する。</u> <u>(2) 発電所の出入管理方法については、「1.1.1.5 人の不法な侵入等の防止(3)手順等」に示す。</u> <u>(3) 発電所の出入管理に係る教育については、「1.1.1.5 人の不法な侵入等の防止(3)手順等」に示す。</u>		

柏崎刈羽原子力発電所 6 / 7 号炉 (2017. 12. 20 版)	東海第二発電所 (2018. 9. 18 版)	島根原子力発電所 2 号炉	備考																
	第 6.3-1 表 原子炉プラント・プロセス計装一覧表 <table><tr><th>項 目</th><th>名 称</th></tr><tr><td>原子炉圧力容器計装</td><td>原子炉水位, 圧力 圧力容器胴部温度 圧力容器フランジ部シール漏えい</td></tr><tr><td>再循環回路計装</td><td>再循環流量 冷却材温度 再循環系ポンプ出入口差圧 炉心流量 シール漏えい流量 再循環系ポンプ冷却水流量, 温度</td></tr><tr><td>原子炉給水系及び蒸気系計装</td><td>原子炉給水流量 蒸気流量 給水温度 タービン第一段圧力</td></tr><tr><td>制御棒駆動機構計装</td><td>制御棒駆動ポンプ出口圧力 フィルタ圧力 原子炉と駆動水圧系との差圧 駆動ヘッド流量 制御棒駆動機構温度 アキュムレータ窒素圧力 アキュムレータ漏えい水量 スクラム水排出容器水位</td></tr><tr><td>原子炉格納容器内雰囲気計装</td><td>格納容器内圧力 格納容器内温度 格納容器内湿度 格納容器内水素濃度及び酸素濃度 格納容器内放射線 サブプレッション・プール水位 サブプレッション・プール水温</td></tr><tr><td>漏えい検出系計装</td><td>格納容器床ドレン流量 格納容器機器ドレン流量 格納容器雰囲気中の核分裂生成物の放射性物質濃度</td></tr><tr><td>その他の原子炉プラント・プロセス計装</td><td>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 高圧炉心スプレイ系ポンプ出口圧力 低圧炉心スプレイ系ポンプ出口圧力 残留熱除去系ポンプ出口圧力</td></tr></table>	項 目	名 称	原子炉圧力容器計装	原子炉水位, 圧力 圧力容器胴部温度 圧力容器フランジ部シール漏えい	再循環回路計装	再循環流量 冷却材温度 再循環系ポンプ出入口差圧 炉心流量 シール漏えい流量 再循環系ポンプ冷却水流量, 温度	原子炉給水系及び蒸気系計装	原子炉給水流量 蒸気流量 給水温度 タービン第一段圧力	制御棒駆動機構計装	制御棒駆動ポンプ出口圧力 フィルタ圧力 原子炉と駆動水圧系との差圧 駆動ヘッド流量 制御棒駆動機構温度 アキュムレータ窒素圧力 アキュムレータ漏えい水量 スクラム水排出容器水位	原子炉格納容器内雰囲気計装	格納容器内圧力 格納容器内温度 格納容器内湿度 格納容器内水素濃度及び酸素濃度 格納容器内放射線 サブプレッション・プール水位 サブプレッション・プール水温	漏えい検出系計装	格納容器床ドレン流量 格納容器機器ドレン流量 格納容器雰囲気中の核分裂生成物の放射性物質濃度	その他の原子炉プラント・プロセス計装	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 高圧炉心スプレイ系ポンプ出口圧力 低圧炉心スプレイ系ポンプ出口圧力 残留熱除去系ポンプ出口圧力		
項 目	名 称																		
原子炉圧力容器計装	原子炉水位, 圧力 圧力容器胴部温度 圧力容器フランジ部シール漏えい																		
再循環回路計装	再循環流量 冷却材温度 再循環系ポンプ出入口差圧 炉心流量 シール漏えい流量 再循環系ポンプ冷却水流量, 温度																		
原子炉給水系及び蒸気系計装	原子炉給水流量 蒸気流量 給水温度 タービン第一段圧力																		
制御棒駆動機構計装	制御棒駆動ポンプ出口圧力 フィルタ圧力 原子炉と駆動水圧系との差圧 駆動ヘッド流量 制御棒駆動機構温度 アキュムレータ窒素圧力 アキュムレータ漏えい水量 スクラム水排出容器水位																		
原子炉格納容器内雰囲気計装	格納容器内圧力 格納容器内温度 格納容器内湿度 格納容器内水素濃度及び酸素濃度 格納容器内放射線 サブプレッション・プール水位 サブプレッション・プール水温																		
漏えい検出系計装	格納容器床ドレン流量 格納容器機器ドレン流量 格納容器雰囲気中の核分裂生成物の放射性物質濃度																		
その他の原子炉プラント・プロセス計装	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 高圧炉心スプレイ系ポンプ出口圧力 低圧炉心スプレイ系ポンプ出口圧力 残留熱除去系ポンプ出口圧力																		

柏崎刈羽原子力発電所 6 / 7 号炉 (2017. 12. 20 版)	東海第二発電所 (2018. 9. 18 版)	島根原子力発電所 2 号炉	備考										
	 圧力容器零レベル (0cm) ※水位は圧力容器零レベルからの数値を示す。 <table><tr><th colspan="2">水位信号の機能</th></tr><tr><td>L 8</td><td>タービン・トリップ 給水ポンプ・トリップ</td></tr><tr><td>L 3</td><td>原子炉スクラム 原子炉建屋常用換気系閉鎖と 原子炉建屋ガス処理系起動</td></tr><tr><td>L 2</td><td>主蒸気隔離弁閉鎖 高圧炉心スプレイ系起動 高圧炉心スプレイ系ディーゼル発電機起動 原子炉隔離時冷却系起動 再循環系ポンプトリップ</td></tr><tr><td>L 1</td><td>残留熱除去系（低圧注水系）起動 低圧炉心スプレイ系起動 自動減圧系作動 非常用ディーゼル発電機（区分Ⅰ及び区分Ⅱ）起動</td></tr></table>	水位信号の機能		L 8	タービン・トリップ 給水ポンプ・トリップ	L 3	原子炉スクラム 原子炉建屋常用換気系閉鎖と 原子炉建屋ガス処理系起動	L 2	主蒸気隔離弁閉鎖 高圧炉心スプレイ系起動 高圧炉心スプレイ系ディーゼル発電機起動 原子炉隔離時冷却系起動 再循環系ポンプトリップ	L 1	残留熱除去系（低圧注水系）起動 低圧炉心スプレイ系起動 自動減圧系作動 非常用ディーゼル発電機（区分Ⅰ及び区分Ⅱ）起動		
水位信号の機能													
L 8	タービン・トリップ 給水ポンプ・トリップ												
L 3	原子炉スクラム 原子炉建屋常用換気系閉鎖と 原子炉建屋ガス処理系起動												
L 2	主蒸気隔離弁閉鎖 高圧炉心スプレイ系起動 高圧炉心スプレイ系ディーゼル発電機起動 原子炉隔離時冷却系起動 再循環系ポンプトリップ												
L 1	残留熱除去系（低圧注水系）起動 低圧炉心スプレイ系起動 自動減圧系作動 非常用ディーゼル発電機（区分Ⅰ及び区分Ⅱ）起動												
	第 6.3－1 図 原子炉水位計装説明図												

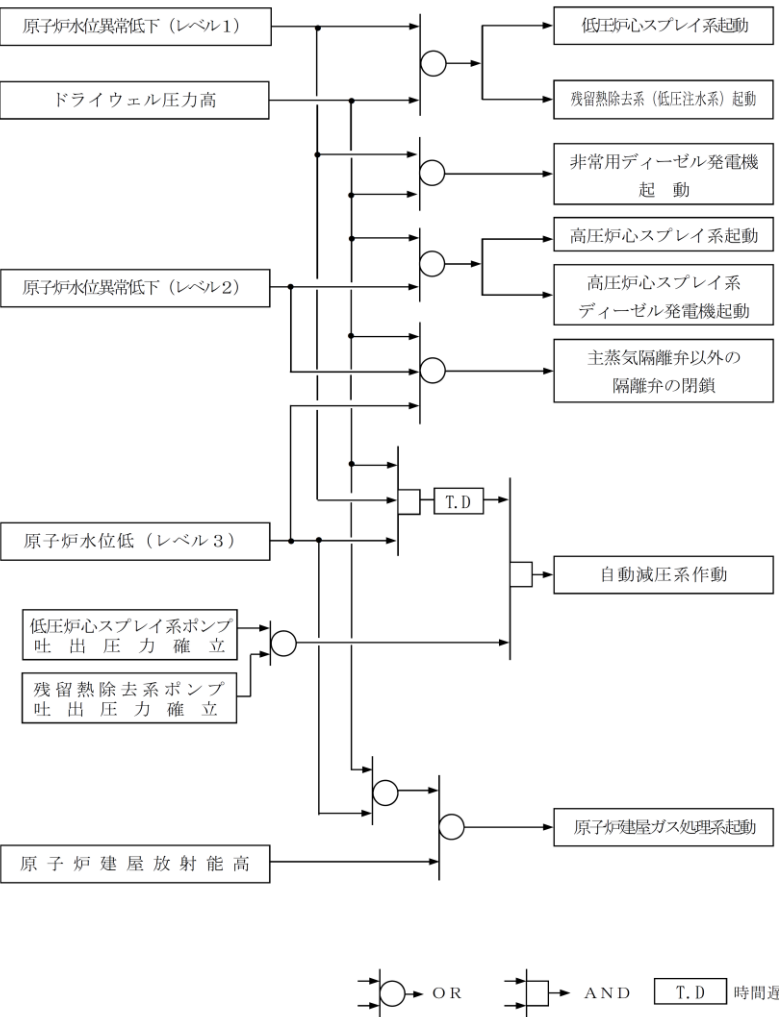
柏崎刈羽原子力発電所 6／7号炉 (2017.12.20版)	東海第二発電所 (2018.9.18版)	島根原子力発電所 2号炉	備考																																																																								
	<u>第6.6－1表 原子炉スクラム信号一覧表</u> <table> <tr> <th rowspan="2">スクラム 信号の種類</th><th colspan="2">検出器</th><th rowspan="2">スクラム設定値</th></tr> <tr> <th>型式</th><th>配置場所</th></tr> <tr> <td>原子炉圧力高</td><td>圧力スイッチ</td><td>原子炉圧力容器</td><td>7.25MPa〔gage〕</td></tr> <tr> <td>原子炉水位低</td><td>差圧スイッチ</td><td>原子炉圧力容器</td><td>1,372cm (ベッセルゼロより上)</td></tr> <tr> <td>ドライウェル圧力高</td><td>圧力スイッチ</td><td>ドライウェル</td><td>13.7kPa〔gage〕</td></tr> <tr> <td>原子炉出力バリエーション短</td><td>起動領域計装</td><td>炉心内</td><td>10秒</td></tr> <tr> <td rowspan="2">中性子束高</td><td>起動領域計装</td><td>炉心内</td><td>最終レンジ目盛の120/125</td></tr> <tr> <td>出力領域計装</td><td>炉心内</td><td>・原子炉モード・スイッチ「運転」位置 で定格出力の120% ・原子炉モード・スイッチ「運転」位置 以外で定格出力の15% ・自動可変設定</td></tr> <tr> <td>中性子束低</td><td>出力領域計装</td><td>炉心内</td><td>定格出力の2%</td></tr> <tr> <td rowspan="2">中性子束計装動作不能</td><td>起動領域計装</td><td>中央制御室</td><td>中性子束計装動作不能の場合</td></tr> <tr> <td>出力領域計装</td><td>中央制御室</td><td>中性子束計装動作不能の場合</td></tr> <tr> <td>スクラム水排出容器水位高</td><td>レベル・ スイッチ</td><td>スクラム水排出容器</td><td>0.189m³に相当するレベル</td></tr> <tr> <td>主蒸気隔離弁閉</td><td>弁位置スイッチ</td><td>主蒸気隔離弁</td><td>開度90%</td></tr> <tr> <td>主蒸気管放射能高</td><td>ガンマ線モニタ</td><td>ドライウェル外側の 主蒸気管</td><td>通常運転時の放射能の10倍以下</td></tr> <tr> <td>主蒸気止め弁閉</td><td>弁位置スイッチ</td><td>主蒸気止弁</td><td>開度90%</td></tr> <tr> <td>蒸気加減弁急速閉</td><td>圧力スイッチ</td><td>蒸気加減弁</td><td>4.12MPa〔gage〕</td></tr> <tr> <td>地震加速度大</td><td>加速度検出器</td><td>原子炉建屋内</td><td>水平方向300gal (EL.14.0m) 水平方向250gal (EL. -4.0m) 鉛直方向120gal (EL. -4.0m)</td></tr> <tr> <td>原子炉モード・スイッチ 「停止」</td><td>原子炉モード・ スイッチ</td><td>中央制御室</td><td></td></tr> <tr> <td>手 動</td><td>押しボタン</td><td>中央制御室</td><td></td></tr> </table>	スクラム 信号の種類	検出器		スクラム設定値	型式	配置場所	原子炉圧力高	圧力スイッチ	原子炉圧力容器	7.25MPa〔gage〕	原子炉水位低	差圧スイッチ	原子炉圧力容器	1,372cm (ベッセルゼロより上)	ドライウェル圧力高	圧力スイッチ	ドライウェル	13.7kPa〔gage〕	原子炉出力バリエーション短	起動領域計装	炉心内	10秒	中性子束高	起動領域計装	炉心内	最終レンジ目盛の120/125	出力領域計装	炉心内	・原子炉モード・スイッチ「運転」位置 で定格出力の120% ・原子炉モード・スイッチ「運転」位置 以外で定格出力の15% ・自動可変設定	中性子束低	出力領域計装	炉心内	定格出力の2%	中性子束計装動作不能	起動領域計装	中央制御室	中性子束計装動作不能の場合	出力領域計装	中央制御室	中性子束計装動作不能の場合	スクラム水排出容器水位高	レベル・ スイッチ	スクラム水排出容器	0.189m ³ に相当するレベル	主蒸気隔離弁閉	弁位置スイッチ	主蒸気隔離弁	開度90%	主蒸気管放射能高	ガンマ線モニタ	ドライウェル外側の 主蒸気管	通常運転時の放射能の10倍以下	主蒸気止め弁閉	弁位置スイッチ	主蒸気止弁	開度90%	蒸気加減弁急速閉	圧力スイッチ	蒸気加減弁	4.12MPa〔gage〕	地震加速度大	加速度検出器	原子炉建屋内	水平方向300gal (EL.14.0m) 水平方向250gal (EL. -4.0m) 鉛直方向120gal (EL. -4.0m)	原子炉モード・スイッチ 「停止」	原子炉モード・ スイッチ	中央制御室		手 動	押しボタン	中央制御室			
スクラム 信号の種類	検出器		スクラム設定値																																																																								
	型式	配置場所																																																																									
原子炉圧力高	圧力スイッチ	原子炉圧力容器	7.25MPa〔gage〕																																																																								
原子炉水位低	差圧スイッチ	原子炉圧力容器	1,372cm (ベッセルゼロより上)																																																																								
ドライウェル圧力高	圧力スイッチ	ドライウェル	13.7kPa〔gage〕																																																																								
原子炉出力バリエーション短	起動領域計装	炉心内	10秒																																																																								
中性子束高	起動領域計装	炉心内	最終レンジ目盛の120/125																																																																								
	出力領域計装	炉心内	・原子炉モード・スイッチ「運転」位置 で定格出力の120% ・原子炉モード・スイッチ「運転」位置 以外で定格出力の15% ・自動可変設定																																																																								
中性子束低	出力領域計装	炉心内	定格出力の2%																																																																								
中性子束計装動作不能	起動領域計装	中央制御室	中性子束計装動作不能の場合																																																																								
	出力領域計装	中央制御室	中性子束計装動作不能の場合																																																																								
スクラム水排出容器水位高	レベル・ スイッチ	スクラム水排出容器	0.189m ³ に相当するレベル																																																																								
主蒸気隔離弁閉	弁位置スイッチ	主蒸気隔離弁	開度90%																																																																								
主蒸気管放射能高	ガンマ線モニタ	ドライウェル外側の 主蒸気管	通常運転時の放射能の10倍以下																																																																								
主蒸気止め弁閉	弁位置スイッチ	主蒸気止弁	開度90%																																																																								
蒸気加減弁急速閉	圧力スイッチ	蒸気加減弁	4.12MPa〔gage〕																																																																								
地震加速度大	加速度検出器	原子炉建屋内	水平方向300gal (EL.14.0m) 水平方向250gal (EL. -4.0m) 鉛直方向120gal (EL. -4.0m)																																																																								
原子炉モード・スイッチ 「停止」	原子炉モード・ スイッチ	中央制御室																																																																									
手 動	押しボタン	中央制御室																																																																									

柏崎刈羽原子力発電所 6 / 7 号炉 (2017. 12. 20 版)	東海第二発電所 (2018. 9. 18 版)	島根原子力発電所 2 号炉	備考																																											
	第 6. 6－2 表 その他の主要な安全保護系作動信号一覧表 <table><tr><th>信 号 の 種 類</th><th>保 護 機 能 の 種 類</th><th>設 定 値</th></tr><tr><td>原 子 炉 水 位 低</td><td>原子炉建屋ガス処理系起動</td><td>1, 372cm (ベッセルゼロより上) (レベル 3)</td></tr><tr><td rowspan="4">原子炉水位異常低下</td><td>主蒸気隔離弁閉鎖</td><td rowspan="3">1, 243cm (ベッセルゼロより上) (レベル 2)</td></tr><tr><td>高圧炉心スプレイ系起動</td></tr><tr><td>高圧炉心スプレイ系ディーゼル発電機起動</td></tr><tr><td>低圧炉心スプレイ系起動</td><td rowspan="4">961cm (ベッセルゼロより上) (レベル 1)</td></tr><tr><td>残留熱除去系（低圧注水系）起動</td></tr><tr><td>自動減圧系作動</td></tr><tr><td>非常用ディーゼル発電機起動</td></tr><tr><td rowspan="6">ドライウエル圧力高</td><td>低圧炉心スプレイ系起動</td><td rowspan="6">13. 7kPa [gage]</td></tr><tr><td>残留熱除去系（低圧注水系）起動</td></tr><tr><td>高圧炉心スプレイ系起動</td></tr><tr><td>自動減圧系作動</td></tr><tr><td>原子炉建屋ガス処理系起動</td></tr><tr><td>高圧炉心スプレイ系ディーゼル発電機起動</td></tr><tr><td>非常用ディーゼル発電機起動</td></tr><tr><td>主 蒸 気 管 圧 力 低</td><td>主蒸気隔離弁閉鎖</td><td>5. 89MPa [gage]</td></tr><tr><td>主 蒸 気 管 流 量 大</td><td>主蒸気隔離弁閉鎖</td><td>定格流量の 140％相当</td></tr><tr><td>復 水 器 真 空 度 低</td><td>主蒸気隔離弁閉鎖</td><td>真空度 24. 0kPa</td></tr><tr><td>主 蒸 気 管 放 射 能 高</td><td>主蒸気隔離弁閉鎖</td><td>通常運転時の放射能の 10 倍以下</td></tr><tr><td>主蒸気管トンネル温度高</td><td>主蒸気隔離弁閉鎖</td><td>93℃</td></tr><tr><td>原 子 炉 建 屋 放 射 能 高</td><td>原子炉建屋ガス処理系起動</td><td>通常運転時の放射能の 10 倍以下</td></tr></table>	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, 372cm (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	1, 243cm (ベッセルゼロより上) (レベル 2)	高圧炉心スプレイ系起動	高圧炉心スプレイ系ディーゼル発電機起動	低圧炉心スプレイ系起動	961cm (ベッセルゼロより上) (レベル 1)	残留熱除去系（低圧注水系）起動	自動減圧系作動	非常用ディーゼル発電機起動	ドライウエル圧力高	低圧炉心スプレイ系起動	13. 7kPa [gage]	残留熱除去系（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	高圧炉心スプレイ系ディーゼル発電機起動	非常用ディーゼル発電機起動	主 蒸 気 管 圧 力 低	主蒸気隔離弁閉鎖	5. 89MPa [gage]	主 蒸 気 管 流 量 大	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		
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, 372cm (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	1, 243cm (ベッセルゼロより上) (レベル 2)																																												
	高圧炉心スプレイ系起動																																													
	高圧炉心スプレイ系ディーゼル発電機起動																																													
	低圧炉心スプレイ系起動	961cm (ベッセルゼロより上) (レベル 1)																																												
残留熱除去系（低圧注水系）起動																																														
自動減圧系作動																																														
非常用ディーゼル発電機起動																																														
ドライウエル圧力高	低圧炉心スプレイ系起動	13. 7kPa [gage]																																												
	残留熱除去系（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																																													
	高圧炉心スプレイ系ディーゼル発電機起動																																													
非常用ディーゼル発電機起動																																														
主 蒸 気 管 圧 力 低	主蒸気隔離弁閉鎖	5. 89MPa [gage]																																												
主 蒸 気 管 流 量 大	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																																												

柏崎刈羽原子力発電所 6／7号炉 (2017.12.20版)	東海第二発電所 (2018.9.18版)	島根原子力発電所 2号炉	備考
	 第 6.6－3 図 原子炉緊急停止系機能説明図		

柏崎刈羽原子力発電所 6／7号炉 (2017.12.20版)	東海第二発電所 (2018.9.18版)	島根原子力発電所 2号炉	備考
	○ → OR □ → AND □(X) → NOT		

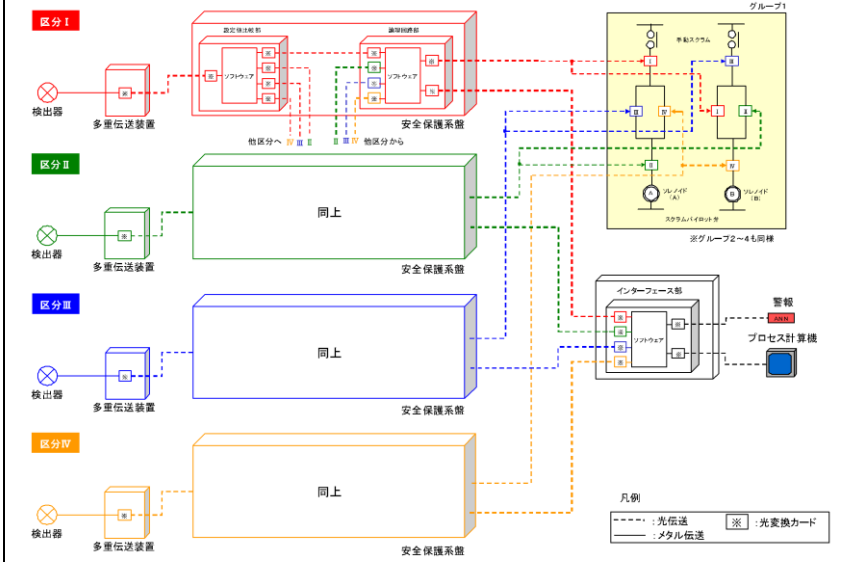
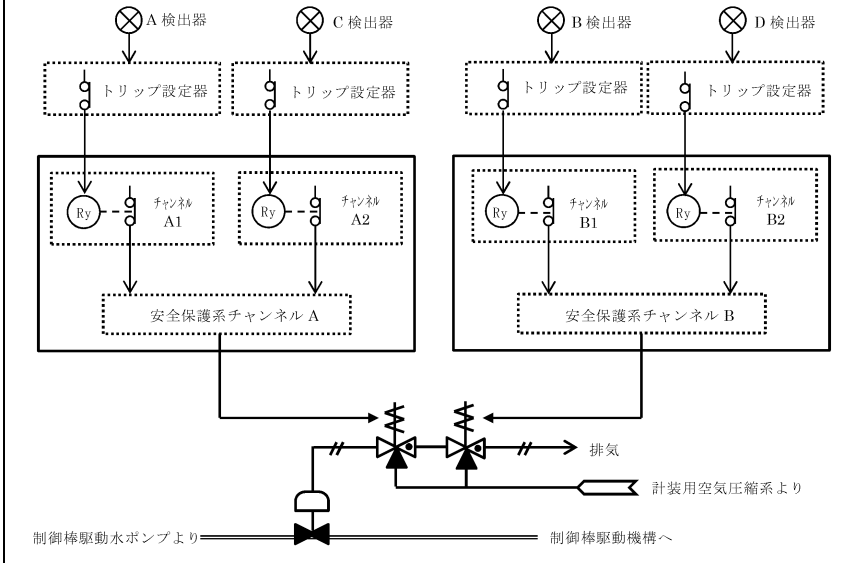
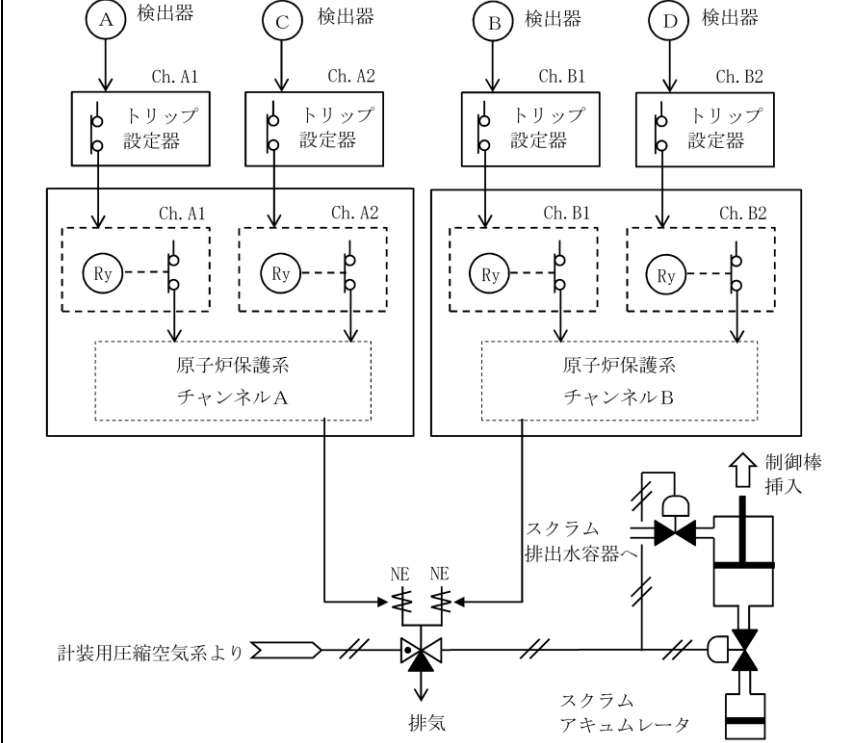
第 6.6－4 図 その他の主要な安全保護系機能説明図（その 1）

柏崎刈羽原子力発電所 6／7号炉 (2017.12.20版)	東海第二発電所 (2018.9.18版)	島根原子力発電所 2号炉	備考
	 第 6.6－5 図 その他の主要な安全保護系機能説明図（その 2）		

柏崎刈羽原子力発電所 6／7号炉 (2017. 12. 20 版)	東海第二発電所 (2018. 9. 18 版)	島根原子力発電所 2号炉	備考
2. 追加要求事項に対する適合方針 2.1 <u>安全保護系</u>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。』に対して、<u>ディジタル化している安全保護系（原子炉緊急停止系作動回路、工学的安全施設作動回路）</u>は下記の対策を実施している。 (1) 物理的及び電氣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、電氣的アクセスについては、<u>安全保護系制御装置の保守ツールを施錠管理された場所に保管するとともに、安全保護系制御装置の保守ツールの接続部を施錠することや保守ツールのパスワード管理※により不要なソフトウェアへのアクセスを制限することで、管理されない変更を防止している。</u> (2) ハードウェアの物理的な分離又は機能的な分離対策 <u>安全保護系</u>の信号は、<u>安全保護系盤→プロセス計算機→防護装置→緊急時対策支援システム伝送装置（ERSS）→防護装置</u>を介して外部に伝送している。この信号の流れにおいて、安全保護系からは発信されるのみであり、外部からの信号を受信しないこと、及びハードウェアを直接接続しないことで物理的及び機能的分離を行っている。 (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 <u>安全保護系</u>の信号で外部ネットワークへのデータ伝送の	2. 安全保護回路 2.1 <u>安全保護回路</u>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。』が要求されている。 <u>東海第二発電所の安全保護回路は、検出信号処理において一部ディジタル演算処理を行う機器がある他は、アナログ回路で構成している。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）の不正アクセス行為による被害防止については、ディジタル演算処理を行う機器も含め、下記の対策を実施している。</u> (1) 物理的及び電氣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、電氣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、<u>ディジタル演算処理を行う機器からデータを採取するデータ収集端末にはディジタル演算処理を行う機器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。</u> (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、<u>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</u>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 <u>安全保護回路とそれ以外の設備との間で用いる信号はアナログ信号（接点信号を含む）であり、外部ネットワークを介した不正アクセス等による被害を受けることはない。</u> 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	2. 追加要求事項に対する適合方針 2.1 <u>安全保護回路</u>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。』に対して、<u>安全保護回路（原子炉保護系、工学的安全施設作動回路）のうちディジタル化している部分については、下記の対策を実施している。</u> (1) 物理的及び電氣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、電氣的アクセスについては、<u>安全保護回路を有する制御盤を施錠管理とし、ディジタル処理部と接続する保守ツールは施錠管理された場所に保管し、パスワード管理することで管理されない変更を防止している。</u> (2) ハードウェアの物理的な分離又は機能的な分離対策 <u>安全保護回路</u>の信号は、<u>安全保護回路→S P D Sデータ収集サーバ→防護装置→S P D S伝送サーバ→防護装置</u>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 <u>安全保護回路</u>の信号で外部ネットワークへデータ伝送の	・設備の相違 【柏崎 6/7】 島根 2 号炉の安全保護回路は一部ディジタル演算処理を行う機器がある他は、アナログ回路で構成している（以下、④の相違） ・運用の相違 【柏崎 6/7】 設備構成の相違による運用の相違（島根 2 号炉は保守ツールの接続部の施錠管理については、接続部は盤内にあるため盤を施錠管理している。他については同様）（以下、⑤の相違） 【東海第二】 島根 2 号炉で使用する保守ツールは送信機能もある（以下、⑥の相違）

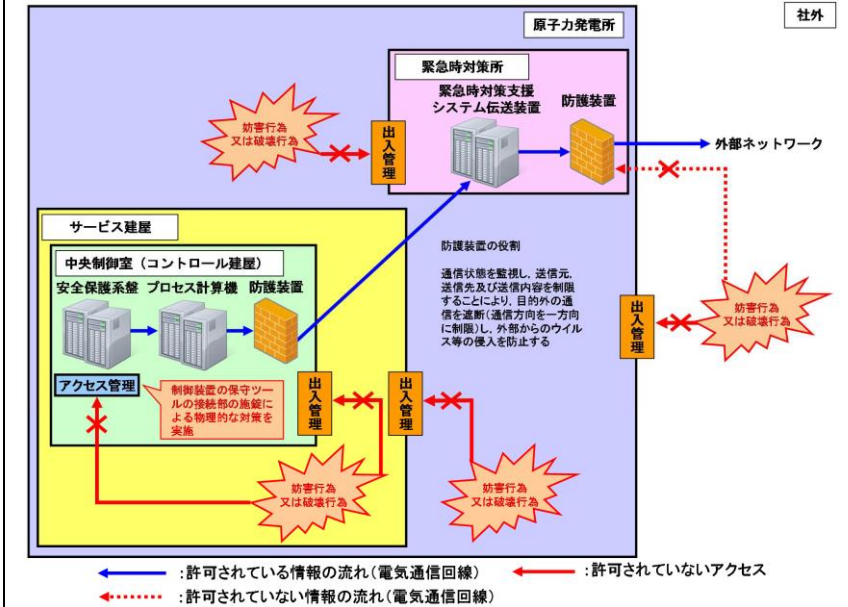
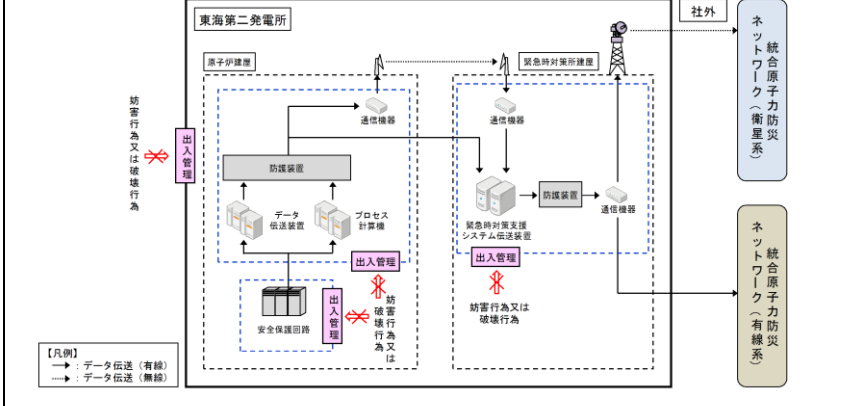
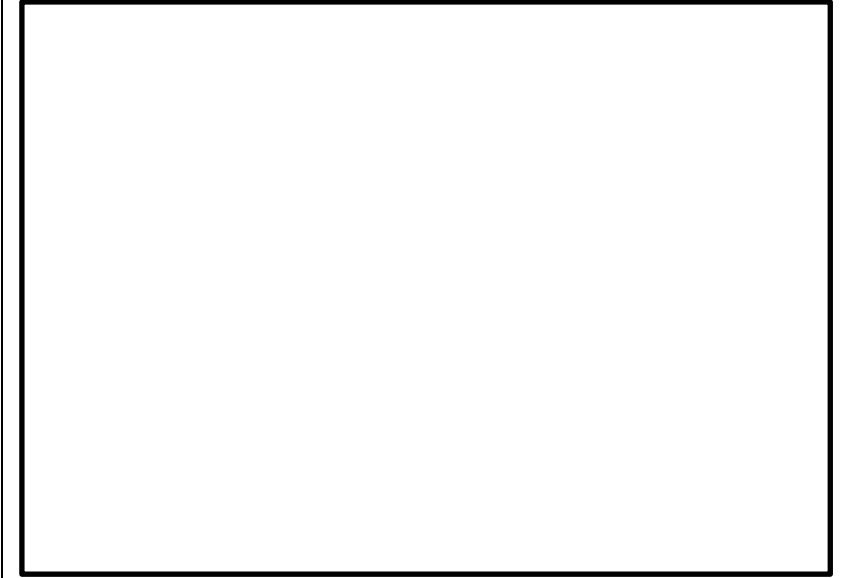
柏崎刈羽原子力発電所 6／7号炉 (2017. 12. 20 版)	東海第二発電所 (2018. 9. 18 版)	島根原子力発電所 2号炉	備考
必要がある場合は、防護装置（通信状態を監視し、送信元、送信先及び送信内容を制限することにより、目的外の通信を遮断）を介して<u>安全保護系盤</u>の信号を一方向（送信機能のみ）通信に制限し外部からのデータ書き込み機能を設けないことでウイルスの侵入及び外部からの不正アクセスを防止している。 (4) システムの導入段階、更新段階又は試験段階で承認されていない動作や変更を防ぐ対策 <u>「安全保護系へのデジタル計算機の適用に関する規程（JEAC4620）」及び「デジタル安全保護系の検証及び妥当性確認に関する指針（JEAG4609）」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（V&V）がなされたソフトウェアを使用している。また、安全保護系は、固有のプログラム言語を使用（一般的なコンピュータウイルスが動作しない環境）するとともに、保守以外の不要なソフトウェアへのアクセス制限対策として入域制限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。</u> (5) 耐ノイズ・サージ対策 <u>安全保護系は、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にラインフィルタや絶縁回路を設置、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。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。</u>（電源ノイズ試験・誘導ノイズ試験／参考規格 ANSI C 37.90, 静電ノイズ試験／参考規格 IEC-Pub801-2, 電波障害試験／参考規格 JEIDA-29「工業用計算機設置環境基準」、インパルス試験／参考規格 JEC-210, 212）	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。 <u>※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。</u> (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 安全保護回路のうち、<u>一部デジタル演算処理を行う機器は、固有のプログラム言語を使用（一般的なコンピュータウイルスが動作しない環境）するとともに、保守以外の不要な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。</u> (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。	必要がある場合は、防護装置（<u>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</u>）を介して<u>安全保護回路</u>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。 (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 <u>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。</u> (5) 耐ノイズ・サージ対策 <u>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している。</u> <u>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。</u>	・設備の相違 【柏崎 6/7】 島根 2 号炉で使用するアナログ型安全保護回路は、J E A C 4620, J E A G 4609 の適用対象外（以下、⑦の相違） ・設備の相違 【柏崎 6/7】 柏崎 6/7 は光ケーブルの耐性の説明であり、島根 2 号炉は金属シールド付ケーブルを使用しノイズ等の対策を図っている（以下、⑧の相違）

柏崎刈羽原子力発電所 6／7号炉 (2017. 12. 20 版)	東海第二発電所 (2018. 9. 18 版)	島根原子力発電所 2号炉	備考											
(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 <u>ウイルスの侵入防止対策も含め、当社の安全保護系への妨害行為又は破壊行為を防止するため、第2.1表のようなセキュリティ対策を安全保護系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。なお、当社は供給者に対し、品質保証に関する監査を継続的に実施することにより、適切に管理されているかを確認することとしている。</u> <u>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している。</u> <u>※ 社内マニュアル3次文書「Z-29・KK業シス-01 情報システムへのウイルス対策ガイド」に規定</u> 第 2.1 表 供給者への要求事項及び供給者で実施している対策 <table><tr><th>項目</th><th>当社の要求</th><th>供給者の対応</th></tr><tr><td>開発・改造に関する設計上の要求</td><td colspan="2" rowspan="6"></td></tr><tr><td>媒体の管理</td></tr><tr><td>保守に関する要求</td></tr><tr><td>教育</td></tr><tr><td>設定及び設定変更管理</td></tr><tr><td>作業実施</td></tr></table> : 防護上の観点から公開できません	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		<u>(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</u> <u>供給者は、制御システムへ保守ツールや小型記憶媒体の機器接続が必要な場合、当社所有の保守ツール及び小型記憶媒体（MOディスク、CDを含む）については、作業前に当社によりウイルスチェックが実施され、ウイルス感染がないことを確認して供給者が使用する。また、供給者所有のパソコン、小型記憶媒体を使用する場合は、供給者は、ウイルスチェックを行いウイルス感染がないことを確認し、その結果を当社に提出する。</u>	・運用の相違 【柏崎 6/7，東海第二】 島根 2 号炉は、アナログ型安全保護回路による設備構成であり、一部のデジタル部については、保守ツール及び小型記憶媒体からのウイルス侵入が考えられることから供給者に対して要求し対策を図っている（以下，⑨の相違）
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														

柏崎刈羽原子力発電所 6／7号炉 (2017. 12. 20 版)	東海第二発電所 (2018. 9. 18 版)	島根原子力発電所 2号炉	備考
2.2 安全保護系盤の概要 <u>安全保護系盤は、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、原子炉緊急停止信号及び工学的安全施設作動に係わる信号を発信する設備である。</u> <u>デジタル設備の適用に当たっては、「安全保護系へのデジタル計算機の適用に関する規程」（JEAC4620）及び「デジタル安全保護系の検証及び妥当性確認に関する指針」（JEAG4609）に準じた検証及び妥当性確認を行っている。</u>  第 2.2 図 安全保護系盤構成図（例：原子炉緊急停止信号）	2.2 安全保護回路の概要 安全保護回路は、検出信号処理において一部デジタル演算処理を行う機器がある他は、アナログ回路で構成している。また安全保護回路とそれ以外の設備との間で用いる信号はアナログ信号（接点信号を含む）であり、外部ネットワークを介した不正アクセス等による被害を受けることはない。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、多重性及び電氣的・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	2.2 安全保護回路の概要 <u>安全保護回路は、検出信号処理において一部デジタル演算処理を行う機器がある他は、アナログ回路で構成している。また安全保護回路とそれ以外の設備との間で用いる信号はアナログ信号であり、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。</u> <u>例として、原子炉保護系の構成例を第 2.2－1 図に示す。</u> 安全保護回路は、安全保護系のプロセス計装からの信号を受信し、<u>原子炉停止(スクラム)系</u>を自動的に作動させる信号を発する原子炉保護系と、安全保護系のプロセス計装からの信号を受信し、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、多重性及び電氣的・物理的な独立性を持たせている。  第 2.2－1 図 原子炉保護系の構成例	・設備の相違 【柏崎 6/7】 ④の相違 ・設備の相違 【柏崎 6/7】 ⑦の相違 ・設備の相違 【柏崎 6/7】 デジタル型・アナログ型安全保護回路による論理回路の相違（島根 2 号炉はソフトウェアを使用していないハードワイヤの論理回路であるため）（以下、⑩の相違） 【東海第二】 プラントの相違による設備構成の相違

柏崎刈羽原子力発電所 6／7号炉 (2017.12.20版)	東海第二発電所 (2018.9.18版)	島根原子力発電所 2号炉	備考
<u>安全保護系は、相互干渉が起こらないように、物理的、電氣的独立性を持たせている。盤内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。</u>			・設備の相違 【柏崎 6/7】 ⑩の相違

柏崎刈羽原子力発電所 6／7号炉 (2017. 12. 20 版)	東海第二発電所 (2018. 9. 18 版)	島根原子力発電所 2号炉	備考
2.3 <u>安全保護系制御装置のソフトウェア管理方法について</u> 安全保護系制御装置のソフトウェア変更にあたっては、保管庫内の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、使用時は安全保護系制御装置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している。安全保護系制御装置へソフトウェアをインストールする場合は、以下の手順で実施する。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。 なお、多重伝送装置については、保守ツール等を接続する事ができない構成となっており、管理されない変更を防止している。	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。 データ収集端末 保管ラック 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	2.3 <u>安全保護回路の物理的分離対策</u> <u>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ついては施錠を行うこととし、保守ツールは施錠管理された保管ラック内に保管しており、許可された者以外はハードウェアへ直接接続できない対策を実施している。</u> 第 2.3－1 図 安全保護系盤及び保守ツール	・設備の相違 【柏崎 6/7，東海第二】 島根 2 号炉は、アナログ型安全保護回路による設備構成であり、一部のデジタル部については、保守ツールから不正アクセスが考えられることから、保守ツールと安全保護系盤等の施錠管理を行っている（以下、⑪の相違）
第 2.3 図 安全保護系制御装置及び保守ツール ：防護上の観点から公開できません			

柏崎刈羽原子力発電所 6／7号炉 (2017.12.20版)	東海第二発電所 (2018.9.18版)	島根原子力発電所 2号炉	備考
2.4 外部からの不正アクセス行為防止について 安全保護系盤は、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、防護装置を介して接続している。また、安全保護系盤の制御装置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。 発電所への入域については、出入管理により制限しており、外部からの人的妨害行為又は破壊行為を防止している。また、安全保護系制御装置の保守ツールの接続部に対して施錠を行い、関係者以外のアクセスを防止している。  第 2.4 図 ネットワーク概略図	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。 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	2.4 外部からの不正アクセス行為防止について 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している。 外部ネットワークとの接続構成概要を第 2.4-1 図に示す。  第 2.4-1 図 外部ネットワークとの接続構成概要	備考 ・設備の相違 【柏崎 6/7】 ④の相違 ・設備の相違 【柏崎 6/7，東海第二】 外部侵入防止の考え方（防護装置の設置及び出入管理による防御）は同じ

柏崎刈羽原子力発電所 6／7号炉 (2017.12.20版)	東海第二発電所 (2018.9.18版)	島根原子力発電所 2号炉	備考														
2.5 安全保護系の検証及び妥当性確認について 安全保護系のソフトウェアは、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。 第 2.5-1 表 ライフサイクルプロセスにおける各段階での対策 <table><tr><th>段階</th><th>内容</th><th>対策</th></tr><tr><td>設計プロセス</td><td>安全保護系設備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。</td><td rowspan="5"></td></tr><tr><td>製作プロセス</td><td>安全保護系設備ソフトウェア設計要求仕様より安全保護系設備ソフトウェアを製作する。</td></tr><tr><td>試験プロセス</td><td>製作された安全保護系設備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製作されていることを試験により確認する。</td></tr><tr><td>装荷プロセス</td><td>実機へ安全保護系設備ソフトウェアを実装する。</td></tr><tr><td>変更プロセス</td><td>安全保護系設備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。</td></tr></table> ：防護上の観点から公開できません デジタル安全保護系ソフトウェアは、設計、製作、試験、変更管理の各段階で、「安全保護系へのデジタル計算機の適用に関する規程」（JEAC4620）及び「デジタル安全保護系の検証及び妥当性確認に関する指針」（JEAG4609）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、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。 なお、設計要求仕様の変更及びソフトウェアの変更が生じた際は、変更理由、変更箇所等を文書化し、変更の影響範囲を明確にした上で、変更を実施する。必要に応じ、変更箇所及び変更の影響を受ける部分について検証及び妥当性確認作業を再度実施する。 以下に、検証及び妥当性確認の流れと内容を示す。	段階	内容	対策	設計プロセス	安全保護系設備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。		製作プロセス	安全保護系設備ソフトウェア設計要求仕様より安全保護系設備ソフトウェアを製作する。	試験プロセス	製作された安全保護系設備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	実機へ安全保護系設備ソフトウェアを実装する。	変更プロセス	安全保護系設備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。			・設備の相違 【柏崎 6/7】 ④の相違
段階	内容	対策															
設計プロセス	安全保護系設備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。																
製作プロセス	安全保護系設備ソフトウェア設計要求仕様より安全保護系設備ソフトウェアを製作する。																
試験プロセス	製作された安全保護系設備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	実機へ安全保護系設備ソフトウェアを実装する。																
変更プロセス	安全保護系設備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。																

柏崎刈羽原子力発電所 6／7号炉 (2017.12.20版)	東海第二発電所 (2018.9.18版)	島根原子力発電所 2号炉	備考														
設計プロセス 製作プロセス 試験プロセス 装荷プロセス 変更プロセス 運転・保守プロセス 変更プロセス 廃止プロセス デジタル安全保護系システム要求事項 システム設計要求仕様 ハードウェアソフトウェア設計要求仕様 ハードウェア設計・製作 ソフトウェア設計・製作 ハードウェア・ソフトウェア統合 試験 装荷 変更 運転・保守 変更 廃止 基本計画 検証1 検証2 検証3, 4 検証5 妥当性確認 検証と妥当性確認 (必要に依じ) 基本計画の確認 【基本計画書】 検証と妥当性確認 (V&V) 要領書の審査 報告書の確認 【要領書、報告書】 設計図書の審査 【設定値相関表、インターロックブロック線図、ソフトウェア図他】 検証と妥当性確認 (V&V) 要領書の審査 報告書の確認 【要領書、報告書】 V&V実施範囲 V&V: 検証と妥当性確認 (Verification and Validation)																	
第2.5 図 デジタル安全保護系のソフトウェアに対する検証及び妥当性確認の流れ 第 2.5-2 表 検証項目及び検証内容 <table><tr><th>検証項目</th><th>検証内容</th></tr><tr><td>検証 1</td><td>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。</td></tr><tr><td>検証 2</td><td>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。</td></tr><tr><td>検証 3</td><td>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。</td></tr><tr><td>検証 4</td><td>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。</td></tr><tr><td>検証 5</td><td>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。</td></tr><tr><td>妥当性確認</td><td>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。</td></tr></table>				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。
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。																

柏崎刈羽原子力発電所 6／7号炉 (2017.12.20版)	東海第二発電所 (2018.9.18版)	島根原子力発電所 2号炉	備考																			
2.6 想定脅威に対する対策について 安全保護系のソフトウェアは、工場製作段階から以下の想定脅威に対する対策を適切に行うことで高い信頼性を実現している。 第 2.6 表 想定脅威に対する対策（工場製作及び出荷） <table><tr><th>想定脅威</th><th>対策</th></tr><tr><td colspan="2"></td></tr></table>	想定脅威	対策			2.5 想定脅威に対する対策について デジタル処理を行う機器については、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） <table><tr><th>想定脅威</th><th>対策</th></tr><tr><td>外部脅威</td><td>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</td></tr><tr><td rowspan="4">内部脅威</td><td>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</td></tr><tr><td>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</td></tr><tr><td>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</td></tr><tr><td>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</td></tr><tr><td>人的要因</td><td>作業ミス，知識不足による情報漏えい等 情報セキュリティ教育の実施</td></tr></table>	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	2.5 想定脅威に対する対策について 安全保護回路の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 2.5－1 表に示す想定脅威に対する対策を行っている。 第 2.5－1 表 想定脅威に対する対策（工場製作及び出荷） <table><tr><th>想定脅威</th><th>対策</th></tr><tr><td colspan="2"></td></tr></table>	想定脅威	対策			
想定脅威	対策																					
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																					
想定脅威	対策																					

柏崎刈羽原子力発電所 6／7号炉 (2017.12.20版)	東海第二発電所 (2018.9.18版)	島根原子力発電所 2号炉	備考
2.7 物理的分離及び電気的分離について <u>安全保護系盤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（計測制御系で短絡等の故障が生じても安全保護系に影響を与えない）を行っている。</u>	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。	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 <u>安全保護回路と計測制御系とは、電源、検出器、ケーブルルート及び格納容器を貫通する計測配管を原則として分離する設計とする。</u> <u>安全保護回路と計測制御系で計測配管を共用する場合は、安全保護回路の計測配管として設計する。</u> (2) 電気的分離について <u>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リレー等の隔離装置を用いて、電気的に分離（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）を行っている。</u> 原子炉中性子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。 <u>隔離装置（アイソレータ及び補助リレー）を第2.6－1図に示す。</u>	・設備の相違 【柏崎6/7】 柏崎6/7は光変換カードによる分離の説明であり、島根2号炉はアイソレータ及び補助リレーを使用し分離を図っている ・設備の相違 【柏崎6/7】 柏崎6/7は光変換カードによる分離の説明であり、島根2号炉はアイソレータ及び補助リレーを使用し分離を図っている
第 2.7 図 通信における分離概念図	第 2.6 図 隔離装置（アイソレータ及び補助継電器）	第 2.6－1 図 隔離装置（アイソレータ及び補助リレー）	

柏崎刈羽原子力発電所 6／7号炉 (2017.12.20版)	東海第二発電所 (2018.9.18版)	島根原子力発電所 2号炉	備考
2.8 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は、2.5 節にて説明した検証及び妥当性確認の品質保証活動に基づき適切な管理のもとに実施するが、変更作業において万が一、ウイルス、バグ等が安全保護系盤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である。また、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録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系盤に書き込み、変更作業前の状態に復元することが可能である。 【ソフトウェア変更前確認の流れ】(Ver. X からVer. X+1 へ変更する例) ①全保護系盤に装荷されているソフトウェア (Ver. X) と、変更前マスター記録媒体 (Ver. X) を照合確認し、全てが一致していることを確認する。 ② 更ソフトウェア記録媒体 (Ver. X+1) と変更前ソフトウェア (Ver. X) を保守ツールにて照合確認し、意図した箇所以外の変更がないことを確認する。 <pre>graph LR A[変更前マスター記録媒体 Ver.X] -- ①照合確認 --> D[変更前ソフトウェア Ver.X] B[変更ソフトウェア記録媒体 Ver.X+1] -- ②照合確認 --> D D -- ①照合確認 --> E[CPUソフトウェア Ver.X] D --> F[保守ツール] F --> D</pre> 変更前マスター記録媒体 (Ver.X) 変更ソフトウェア記録媒体 (Ver.X+1) 変更前ソフトウェア (Ver.X) 保守ツール CPUソフトウェア (Ver.X) 安全保護系盤 第2.8-1 図 ソフトウェア変更作業の流れ (ソフトウェア変更前)			・設備の相違 【柏崎 6/7】 ⑩の相違

柏崎刈羽原子力発電所 6／7号炉 (2017. 12. 20 版)	東海第二発電所 (2018. 9. 18 版)	島根原子力発電所 2号炉	備考
【変更ソフトウェアの安全保護系盤への書き込み及び確認の流れ】 ③変更ソフトウェア (Ver. X+1) を記録媒体から保守ツールへ読み込み、その後、照合確認にてソフトウェア (Ver. X+1) が保守ツールへ正しく読み込みされたことを確認する。 ④変更ソフトウェア (Ver. X+1) を保守ツールより安全保護系盤に書き込み、その後、照合確認にて変更ソフトウェア (Ver. X+1) が正しく安全保護系盤へ書き込まれたことを確認する。 ⑤実機に変更ソフトウェア (Ver. X+1) を書き込んだ後に、ウイルス、バグ等にて演算処理に不具合が発生した場合は、変更前マスター記録媒体 (Ver. X) から変更前ソフトウェアを戻し入れ、変更作業前の状態に復元する。 ＜通常のソフトウェア変更＞ ※保守ツールにて制御装置で動作可能な形式に変換したものを書き込む。 第2. 8-2 図 ソフトウェア変更作業の流れ (ソフトウェア変更)			・設備の相違 【柏崎 6/7】 ⑩の相違

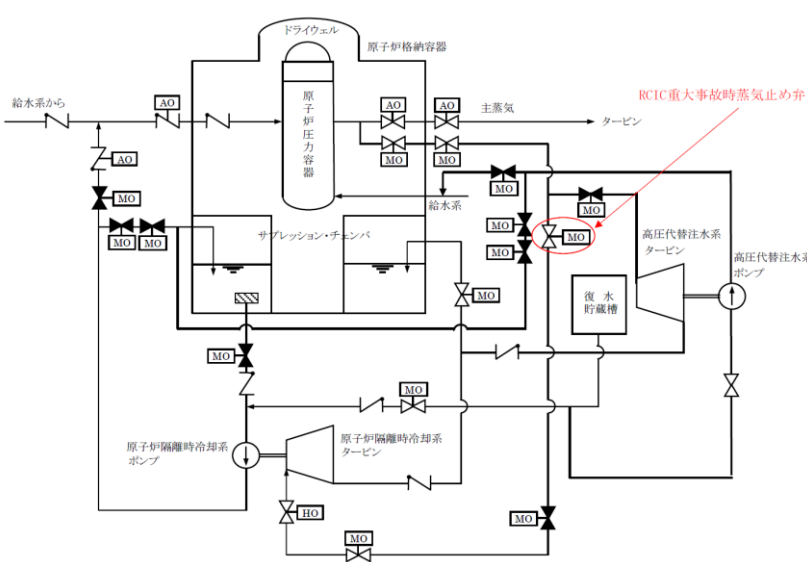
柏崎刈羽原子力発電所 6／7号炉 (2017.12.20版)	東海第二発電所 (2018.9.18版)	島根原子力発電所 2号炉	備考
別紙1 アナログ型安全保護回路について、承認されていない動作や変更を防ぐ設計方針 アナログ型の安全保護回路はハードワイヤーロジック（リレーや配線によるアナログ回路）で構成されており、これらの回路に対し、承認されていない動作や変更を防ぐ措置として、以下を実施している。 安全保護回路の変更が生じる場合は、上流図書から下流図書（第1図参照）へ変更内容が反映されていることを設備図書で承認する。 ・改造後はインターロック試験や定期事業者検査等にて、安全保護回路が正しく動作することを複数の人間でチェックしている。 ・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。	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設計方針 安全保護回路は、<u>検出信号処理において一部デジタル演算処理を行う機器がある他は、アナログ回路で構成している。</u> <u>安全保護回路に対し、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。</u> - 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。 <u>デジタル演算処理を行う機器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。</u> ・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。 <u>・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る、外部からの人的妨害行為又は破壊行為を防止している。</u>	別紙1 <u>アナログ型安全保護回路</u>について、承認されていない動作や変更を防ぐ設計方針 <u>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（リレーや配線によるアナログ回路）で構成されており、これらの回路に対し、承認されていない動作や変更を防ぐ措置として、以下を実施している。</u> 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。 ・<u>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。</u>	・記載箇所の相違 【東海第二】 島根2号炉は別紙8安全保護回路のうち一部デジタル演算処理を行う機器のソフトウェアの検証及び妥当性確認について記載 ・記載箇所の相違 【東海第二】 島根2号炉は別紙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 に記載

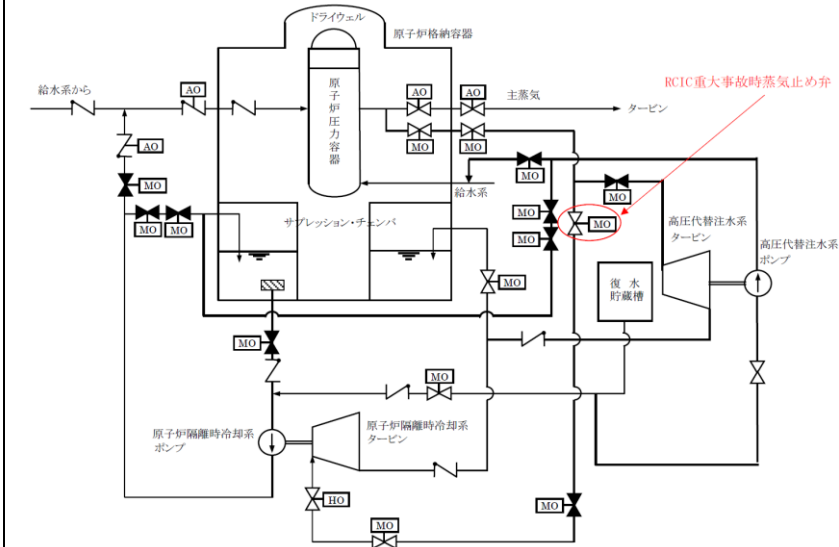
柏崎刈羽原子力発電所 6／7号炉 (2017. 12. 20 版)	東海第二発電所 (2018. 9. 18 版)	島根原子力発電所 2号炉	備考
アナログ型安全保護系 安全保護系 システム要求事項 (設置許可申請書) ↓ システム設計要求仕様 (系統設計仕様書, 設定値根拠書) ↓ ハードウェア設計要求仕様 (インターロックブロック線図) ↓ ハードウェア設計・製作 (展開接続図) ↓ 試 験 (参考)デジタル型安全保護系 デジタル安全保護系 システム要求事項 (設置許可申請書) ↓ システム設計要求仕様 (系統設計仕様書, 設定値根拠書) ↓ ハードウェア・ソフトウェア 設計要求仕様 (機器設計仕様書, インターロックブロック線図) ↓ ハードウェア 設計・製作 (展開接続図) ↓ ソフトウェア 設計・製作 (ソフトウェア図) ↓ ハードウェア・ソフトウェア統合 ↓ 試 験 第1 図 安全保護系の設計・製作・試験の流れ (例)	安全保護回路 システム要求事項 (設置許可申請書) ↓ システム設計要求仕様 (系統設計仕様書, 設定値根拠書) ↓ ハードウェア設計要求仕様 (インターロックブロック線図) ↓ ハードウェア設計・製作 (展開接続図) ↓ 試 験 第 1 図 安全保護回路の設計・製作・試験の流れ (例)	安全保護系 システム要求事項 (設置許可申請書) ↓ システム設計要求仕様 (系統設計仕様書, 設定値根拠書) ↓ ハードウェア設計要求仕様 (インターロックブロック線図) ↓ ハードウェア設計・製作 (展開接続図) ↓ 試験 第 1 図 安全保護回路の設計・製作・試験の流れ (例)	

第1 図 安全保護系の設計・製作・試験の流れ (例)

柏崎刈羽原子力発電所 6／7号炉 (2017.12.20版)	東海第二発電所 (2018.9.18版)	島根原子力発電所 2号炉	備考
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 <u>設置変更許可申請に関わる安全保護回路の変更は行っていない。なお、重大事故等対処設備の設置（自主対策含む）に伴い、デジタル安全保護系設備のソフトウェア改造を実施している事例が下記2件あるが、「安全保護系へのデジタル計算機の適用に関する規程（JEAC4620）」及び「デジタル安全保護系の検証及び妥当性確認に関する指針（JEAG4609）」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（V&V）を実施することで、ソフトウェア改造に伴う影響を防止する設計としている。また、ATWS 緩和設備（代替制御棒挿入機能：ARI）と代替自動減圧ロジック（代替自動減圧機能）については、安全保護回路に変更を施しておらず、安全保護回路と電氣的・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している（参考1）。詳細は各条文の基準適合性説明資料にて説明する。</u>	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 <u>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。</u> <u>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A T W S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、安全保護回路と電氣的・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）。</u> 第1図 安全保護回路の変更に係る改造抽出フロー	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 <u>安全対策工事等のうち、安全保護回路の変更に係る工事を抽出し、確認を行った。抽出フローを第1図に示す。</u> <u>既設の制御盤の改造及び新たな制御盤の設置に関する改造から、安全保護回路及び工学的安全施設作動回路の論理に係る改造を確認対象として抽出した結果、3件が抽出された。いずれの改造も既設の安全保護回路へ影響が無いよう対策が図られていることを確認するとともに、重大事故等対策による改造であっても、既設の安全保護回路へ影響が無いことを確認した。</u> <u>安全保護回路の変更に係る設備の抽出結果並びに抽出された設備についての個別の確認結果を第1表に示す。</u> なお、A T W S緩和設備（代替制御棒挿入機能）及び代替自動減圧ロジック（代替自動減圧機能）については、安全保護回路に変更を施しておらず、安全保護回路と電氣的・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している（参考1）。詳細は各条文の基準適合性説明資料にて説明する。 第1図 安全保護回路の論理に係る改造抽出フロー	・設備の相違 【柏崎 6/7，東海第二】 設備構成の相違による安全保護回路の変更に係る工事の抽出結果の相違だが、いずれも安全保護回路への影響がないことを確認している ・設備の相違 【柏崎 6/7】 工事対象設備の相違（抽出フローを明示）

柏崎刈羽原子力発電所　6／7号炉　（2017. 12. 20 版）	東海第二発電所　（2018. 9. 18 版）	島根原子力発電所　2号炉	備考	
	第1表　安全保護回路の変更に係る設備の抽出結果		・設備の相違 【柏崎 6/7，東海第二】 設備構成の相違による安全保護回路の変更に係る工事の抽出結果の相違	
	改造概要	条文		安全保護回路への影響評価
	A T W S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 46 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，電氣的に分離する。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，電氣的に分離する。
		第1表　安全保護回路の論理に係る改造の抽出結果		
		改造概要	条文	安全保護回路への影響評価
		A T W S時に自動減圧系の作動を阻止する手動回路を追加する。	第 44 条 第 46 条	自動減圧系の手動阻止回路は自動減圧系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，電氣的に分離する。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，電氣的に分離する。
		A T W S時に原子炉の緊急停止操作を実施する手動回路を追加する。	第 44 条	緊急停止操作の手動回路は緊急停止系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，電氣的に分離する。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，電氣的に分離する。
		自動減圧系の作動条件に低圧E C C Sポンプが運転状態であることを追加する。	第 12 条	自動減圧系作動に追加する条件信号回路は，安全保護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，計測制御系統施設から物理的，電氣的に分離する。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，電氣的に分離する。

柏崎刈羽原子力発電所 6／7号炉 (2017. 12. 20 版)	東海第二発電所 (2018. 9. 18 版)	島根原子力発電所 2号炉	備考								
「6 号及び7 号炉 高圧代替注水設備（HPAC）設置に伴う弁操作機能の追加」 ・重大事故等時に原子炉隔離時冷却系（RCIC）が機能喪失した場合において、高圧注水設備の代替手段として、高圧代替注水設備（HPAC）を設置することとしている。 ・高圧代替注水設備（HPAC）は原子炉隔離時冷却系（RCIC）と同様に発電用原子炉からの主蒸気を駆動源としたタービン駆動のポンプであり、原子炉隔離時冷却系（RCIC）蒸気管より分岐した蒸気系のライン構成となっている。 ・原子炉隔離時冷却系（RCIC）起動失敗、又は機能喪失時に、原子炉隔離時冷却系（RCIC）蒸気入口弁操作不能（開状態で停止）で高圧代替注水設備（HPAC）起動後も高圧代替注水設備（HPAC）蒸気量低で定格流量が得られない状況を回避するため、原子炉隔離時冷却系（RCIC）重大事故時蒸気止め弁を設置しており、この弁操作を原子炉隔離時冷却系（RCIC）系から実施可能とするためのソフトウェア改造を実施することとしている。	(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、発電用原子炉が臨界状態であるため、高圧炉心スプレイ系及び残留熱除去系（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。	(1) 自動減圧系の手動阻止回路について 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、急激な低圧注水系流量増加は、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代替自動減圧機能が作動しないように、手動阻止回路を設置する。 b. 手動阻止回路 自動減圧系手動阻止回路を第2図に示す。自動減圧系（D B）と代替自動減圧機能（S A）の論理回路は各々分離しており、追加設置する自動減圧系手動阻止回路は、代替自動減圧機能手動阻止回路とは分離した設計とすることで互いに悪影響を与えない設計とする。 また、自動減圧系手動阻止回路は、単一故障等により本来の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設置するものとする。 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手動阻止回路が、自動減圧系に対して悪影響を与えないことを第2表に示す。	・設備の相違 【柏崎 6/7】 設備構成の相違による安全保護回路の変更に係る工事の抽出結果の相違								
 第1 図 高圧代替注水系 (HPAC) の系統概要	<table><tr><th>設置許可基準規則 第 24 条（安全保護回路）</th><th>自動減圧系への影響</th></tr><tr><td>発電用原子炉施設には、次に掲げるところにより、安全保護回路（安全施設に属するものに限る。以下この条において同じ。）を設けなければならない。 一 運転時の異常な過渡変化が発生する場合において、その異常な状態を検知し、及び原子炉停止系統その他系統と併せて機能することにより、燃料要素の許容損傷限界を超えないようにできるものとする。</td><td>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。</td></tr></table>	設置許可基準規則 第 24 条（安全保護回路）	自動減圧系への影響	発電用原子炉施設には、次に掲げるところにより、安全保護回路（安全施設に属するものに限る。以下この条において同じ。）を設けなければならない。 一 運転時の異常な過渡変化が発生する場合において、その異常な状態を検知し、及び原子炉停止系統その他系統と併せて機能することにより、燃料要素の許容損傷限界を超えないようにできるものとする。	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。	<table><tr><th>設置許可基準規則 第 24 条（安全保護回路）</th><th>自動減圧系への影響</th></tr><tr><td>発電用原子炉施設には、次に掲げるところにより、安全保護回路（安全施設に属するものに限る。以下この条において同じ。）を設けなければならない。 一 運転時の異常な過渡変化が発生する場合において、その異常な状態を検知し、及び原子炉停止系統その他系統と併せて機能することにより、燃料要素の許容損傷限界を超えないようにできるものとする。</td><td>阻止回路は、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。</td></tr></table>	設置許可基準規則 第 24 条（安全保護回路）	自動減圧系への影響	発電用原子炉施設には、次に掲げるところにより、安全保護回路（安全施設に属するものに限る。以下この条において同じ。）を設けなければならない。 一 運転時の異常な過渡変化が発生する場合において、その異常な状態を検知し、及び原子炉停止系統その他系統と併せて機能することにより、燃料要素の許容損傷限界を超えないようにできるものとする。	阻止回路は、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。	
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。	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。										
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。	阻止回路は、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。										



第1 図 高圧代替注水系 (HPAC) の系統概要

柏崎刈羽原子力発電所　6／7号炉　（2017.12.20版）	東海第二発電所（2018.9.18版）		島根原子力発電所　2号炉		備考
	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。	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。	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	
	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。	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。	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。	自動減圧系の多重性、独立性に悪影響を与えないよう、区分ごとに阻止回路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。	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。	自動減圧系の多重性、独立性に悪影響を与えないよう、区分ごとに阻止回路を設置しているため問題ない。	
	五　駆動源の喪失、系統の遮断その他の不利な状況が発生した場合においても、発電用原子炉施設をより安全な状態に移行するか、又は当該状態を維持することにより、発電用原子炉施設の安全上支障がない状態を維持できるものとする。	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発電用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。	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。	自動減圧系の多重性、独立性に悪影響を与えないよう、区分ごとに阻止回路を設置しているため問題ない。	
	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。	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。	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。	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。追加する阻止回路はこの安全保護動作を阻害するものではない。	
	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。	計測制御系とは共用していないため、影響はない。	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。	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。	

柏崎刈羽原子力発電所 6／7号炉 (2017.12.20版)	東海第二発電所 (2018.9.18版)	島根原子力発電所 2号炉		備考			
		<table><tr><td>設置許可基準規則 第24条 (安全保護回路)</td><td>自動減圧系への影響</td></tr><tr><td>七 計測制御系統施設の一部を安全保護回路と共用する場合には、その安全保護機能を失わないよう、計測制御系統施設から機能的に分離されたものとする。</td><td>計測制御系とは共用していないため、影響はない。</td></tr></table>	設置許可基準規則 第24条 (安全保護回路)	自動減圧系への影響	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。	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24条 (安全保護回路)	自動減圧系への影響				
		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。	計測制御系とは共用していないため、影響はない。				
		<table><tr><td>設置許可基準規則 第12条 (安全施設)</td><td>自動減圧系への影響</td></tr><tr><td>4 安全施設は、その健全性及び能力を確認するため、その安全機能の重要度に応じ、発電用原子炉の運転中又は停止中に試験又は検査ができるものでなければならない。</td><td>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。</td></tr></table>	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。	
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。						
<table><tr><td>設置許可基準規則 第12条 (安全施設)</td><td>自動減圧系への影響</td></tr><tr><td>4 安全施設は、その健全性及び能力を確認するため、その安全機能の重要度に応じ、発電用原子炉の運転中又は停止中に試験又は検査ができるものでなければならない。</td><td>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。</td></tr></table>	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。			
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。						
<table><tr><td>設置許可基準規則 第12条 (安全施設)</td><td>自動減圧系への影響</td></tr><tr><td>4 安全施設は、その健全性及び能力を確認するため、その安全機能の重要度に応じ、発電用原子炉の運転中又は停止中に試験又は検査ができるものでなければならない。</td><td>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。</td></tr></table>	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。			
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。						

柏崎刈羽原子力発電所 6／7号炉 (2017.12.20版)	東海第二発電所 (2018.9.18版)	島根原子力発電所 2号炉	備考
「6号炉 直流125V 6A 蓄電池室 換気空調設備の制御回路の追加」 ・ 直流125V 蓄電池 6A の増容量に伴い、蓄電池室（換気空調設備含む）を新設しており、 換気空調設備の制御回路追加のソフトウェア改造を実施することとしている。	自動減圧機能論理回路 過渡時自動減圧機能論理回路 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	第2図 自動減圧系手動阻止回路図 (2) A T W S緩和設備（代替制御棒挿入機能）の手動起動回路について a. 目的 発電用原子炉の運転を緊急に停止することができない事象のおそれがある場合において、手動による原子炉の緊急停止操作を実施するため、手動回路を設置する。 b. 手動回路 A T W S緩和設備（代替制御棒挿入機能）の手動回路を第3図に示す。A T W S緩和設備（代替制御棒挿入機能）は、検出器から代替制御棒挿入機能用電磁弁まで設計基準事故対処設備である多重化された原子炉保護系とは独立した構成となっており、多重化された原子炉保護系に悪影響	・ 設備の相違 【柏崎6/7】 設備構成の相違による安全保護回路の変更に係る工事の抽出結果の相違 【東海第二】 設備構成の相違による論理回路の相違 ・ 設備の相違 【柏崎6/7，東海第二】 設備構成の相違による安全保護回路の変更に係る工事の抽出結果の相違

柏崎刈羽原子力発電所 6／7号炉 (2017.12.20版)	東海第二発電所 (2018.9.18版)	島根原子力発電所 2号炉	備考								
		<u>を及ぼさない設計としている。</u> c. <u>原子炉保護系への影響について</u> <u>追加設置するATWS緩和設備（代替制御棒挿入機能）の手動回路が、原子炉保護系に対して悪影響を与えないことを第3表に示す。</u> <u>第3表 原子炉保護系への影響</u> <table><tr><th>設置許可基準規則 第24条（安全保護回路）</th><th>原子炉保護系への影響</th></tr><tr><td>発電用原子炉施設には、次に掲げるところにより、安全保護回路（安全施設に属するものに限る。以下この条において同じ。）を設けなければならない。</td><td rowspan="3">運転時の異常な過渡変化時には使用しないため問題ない。</td></tr><tr><td>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。</td></tr><tr><td>二 設計基準事故が発生する場合において、その異常な状態を検知し、原子炉停止系統及び工学的安全施設を自動的に作動させるものとする。</td></tr><tr><td>三 安全保護回路を構成する機械若しくは器具又はチャンネルは、単一故障が起きた場合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。</td><td>原子炉保護系の多重性、独立性に悪影響を与えないよう、原子炉保護系とは独立した構成となっているため問題ない。</td></tr></table>	設置許可基準規則 第24条（安全保護回路）	原子炉保護系への影響	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。	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。	一 運転時の異常な過渡変化が発生する場合において、その異常な状態を検知し、及び原子炉停止系統その他系統と併せて機能することにより、燃料要素の許容損傷限界を超えないようにできるものとする。	二 設計基準事故が発生する場合において、その異常な状態を検知し、原子炉停止系統及び工学的安全施設を自動的に作動させるものとする。	三 安全保護回路を構成する機械若しくは器具又はチャンネルは、単一故障が起きた場合又は使用状態からの単一の取り外しを行った場合において、安全保護機能を失わないよう、多重性を確保するものとする。	原子炉保護系の多重性、独立性に悪影響を与えないよう、原子炉保護系とは独立した構成となっているため問題ない。	
設置許可基準規則 第24条（安全保護回路）	原子炉保護系への影響										
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。	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。										
一 運転時の異常な過渡変化が発生する場合において、その異常な状態を検知し、及び原子炉停止系統その他系統と併せて機能することにより、燃料要素の許容損傷限界を超えないようにできるものとする。											
二 設計基準事故が発生する場合において、その異常な状態を検知し、原子炉停止系統及び工学的安全施設を自動的に作動させるものとする。											
三 安全保護回路を構成する機械若しくは器具又はチャンネルは、単一故障が起きた場合又は使用状態からの単一の取り外しを行った場合において、安全保護機能を失わないよう、多重性を確保するものとする。	原子炉保護系の多重性、独立性に悪影響を与えないよう、原子炉保護系とは独立した構成となっているため問題ない。										

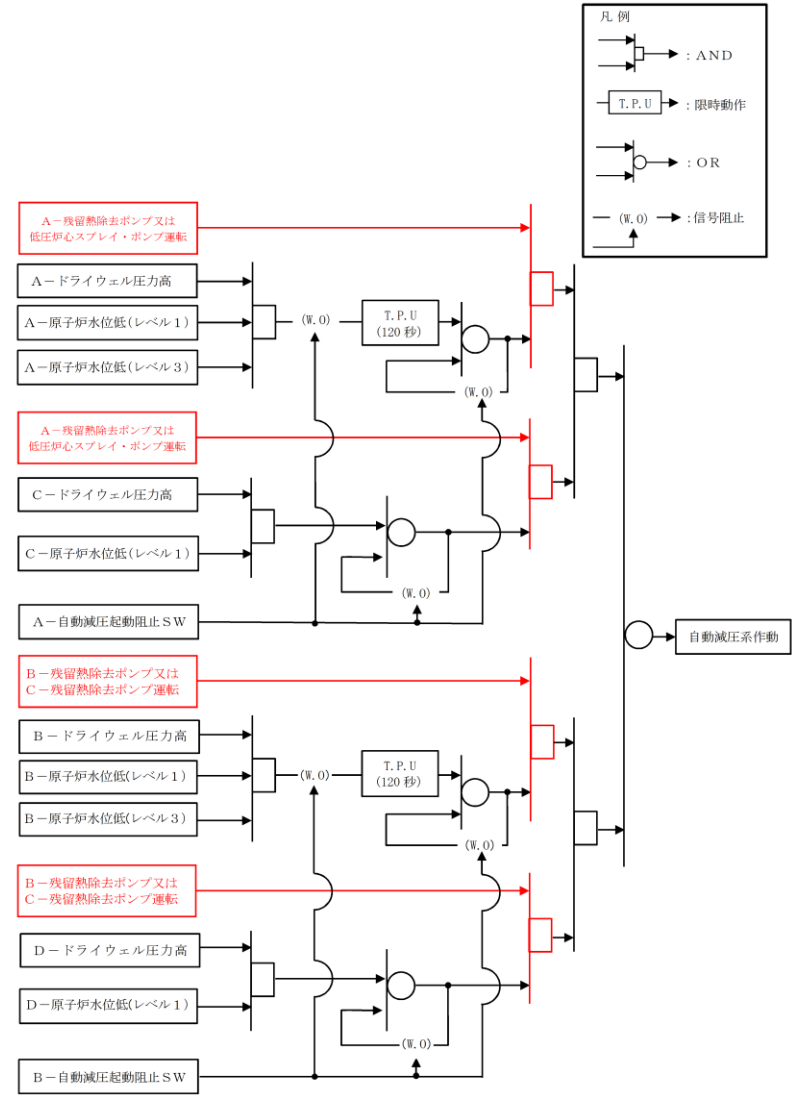
柏崎刈羽原子力発電所 6／7号炉 (2017.12.20版)	東海第二発電所 (2018.9.18版)	島根原子力発電所 2号炉		備考
		設置許可基準規則 第24条 (安全保護回路)		
		四 安全保護回路を構成するチャンネルは、それぞれ互いに分離し、それぞれのチャンネル間において安全保護機能を失わないように独立性を確保するものとする	原子炉保護系への影響	
		五 駆動源の喪失、系統の遮断その他の不利な状況が発生した場合においても、発電用原子炉施設をより安全な状態に移行するか、又は当該状態を維持することにより、発電用原子炉施設の安全上支障がない状態を維持できるものとする	原子炉保護系の多重性、独立性に悪影響を与えないよう、原子炉保護系とは独立した構成となっているため問題ない。	
		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	駆動源の喪失、系統の遮断等においても安全上許容される状態（フェイル・セーフ）になるようにしている。手動回路はこの状態を阻害するものではない。	
		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	手動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。	

柏崎刈羽原子力発電所 6 / 7 号炉 (2017. 12. 20 版)	東海第二発電所 (2018. 9. 18 版)	島根原子力発電所 2 号炉	備考				
		<table border="1"> <thead> <tr> <th>設置許可基準規則 第 12 条 (安全施設)</th><th>原子炉保護系への影響</th></tr> </thead> <tbody> <tr> <td>4 安全施設は、その健全性及び能力を確認するため、その安全機能の重要度に応じ、発電用原子炉の運転中又は停止中に試験又は検査ができるものでなければならない。</td><td>手動回路を設置することで原子炉保護系の試験に影響を与えることはない。</td></tr> </tbody> </table> 凡例 - AND 論理 - OR 論理 - ARI : 代替制御棒挿入機能 - NE : 常時励磁 - ND : 常時無励磁 第 3 図 A T W S 緩和設備（代替制御棒挿入機能）の手動回路図	設置許可基準規則 第 12 条 (安全施設)	原子炉保護系への影響	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。	手動回路を設置することで原子炉保護系の試験に影響を与えることはない。	
設置許可基準規則 第 12 条 (安全施設)	原子炉保護系への影響						
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。	手動回路を設置することで原子炉保護系の試験に影響を与えることはない。						

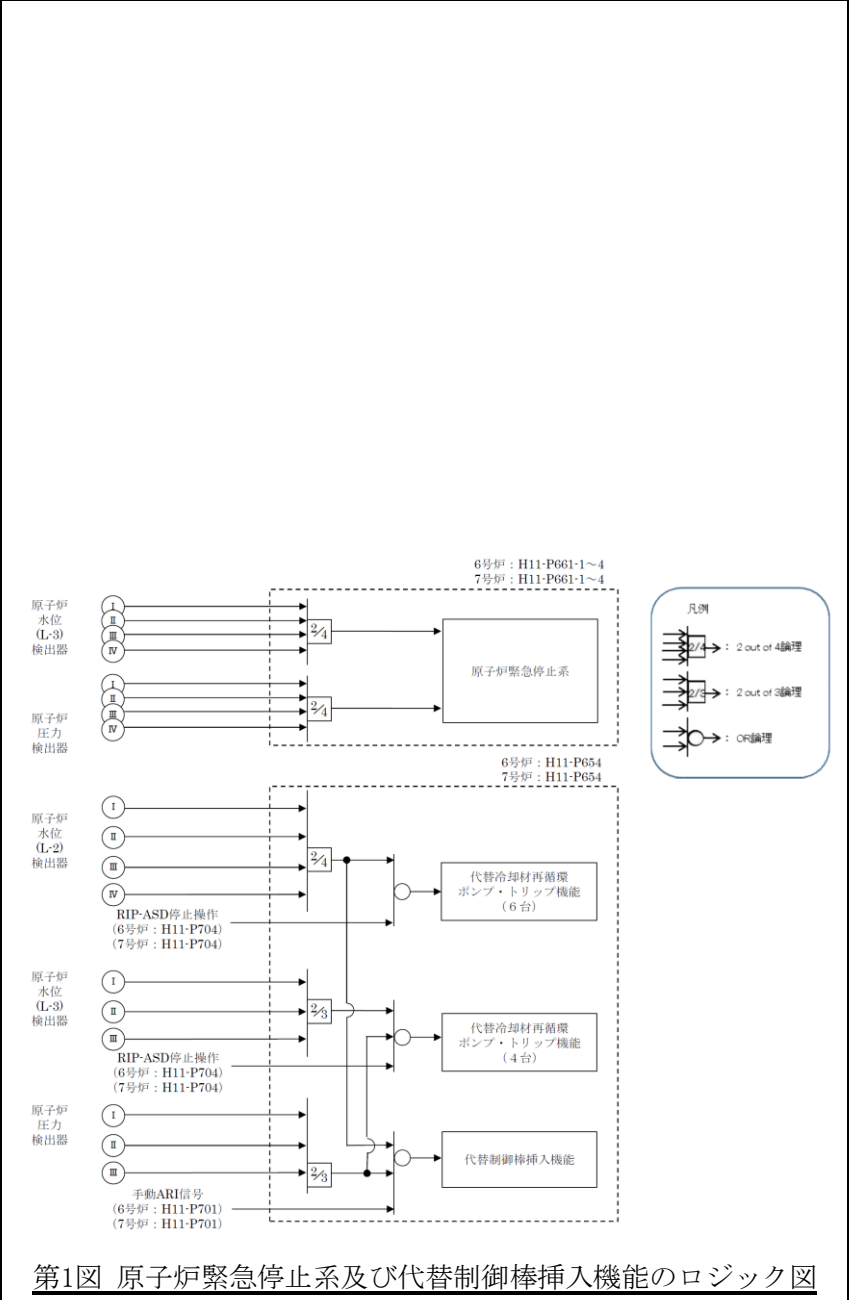
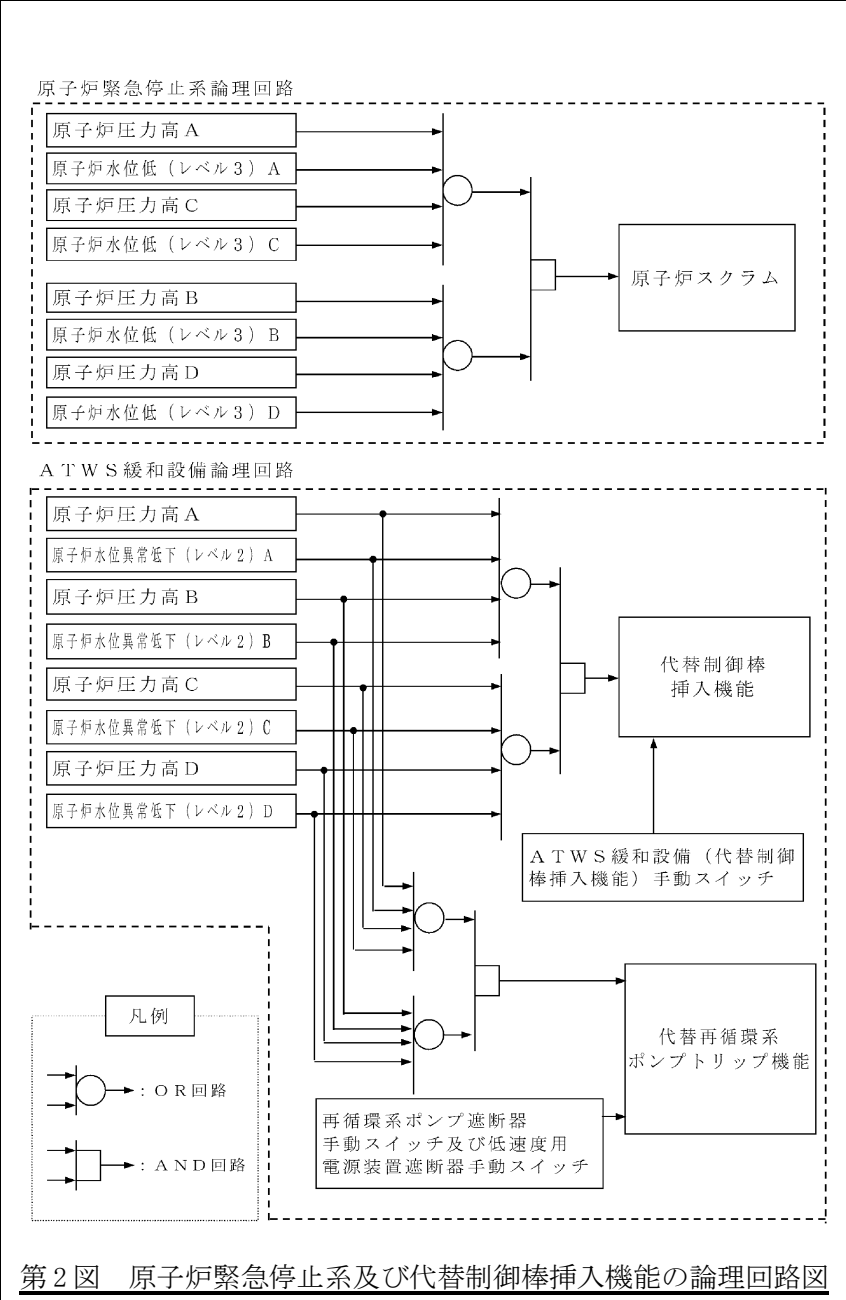
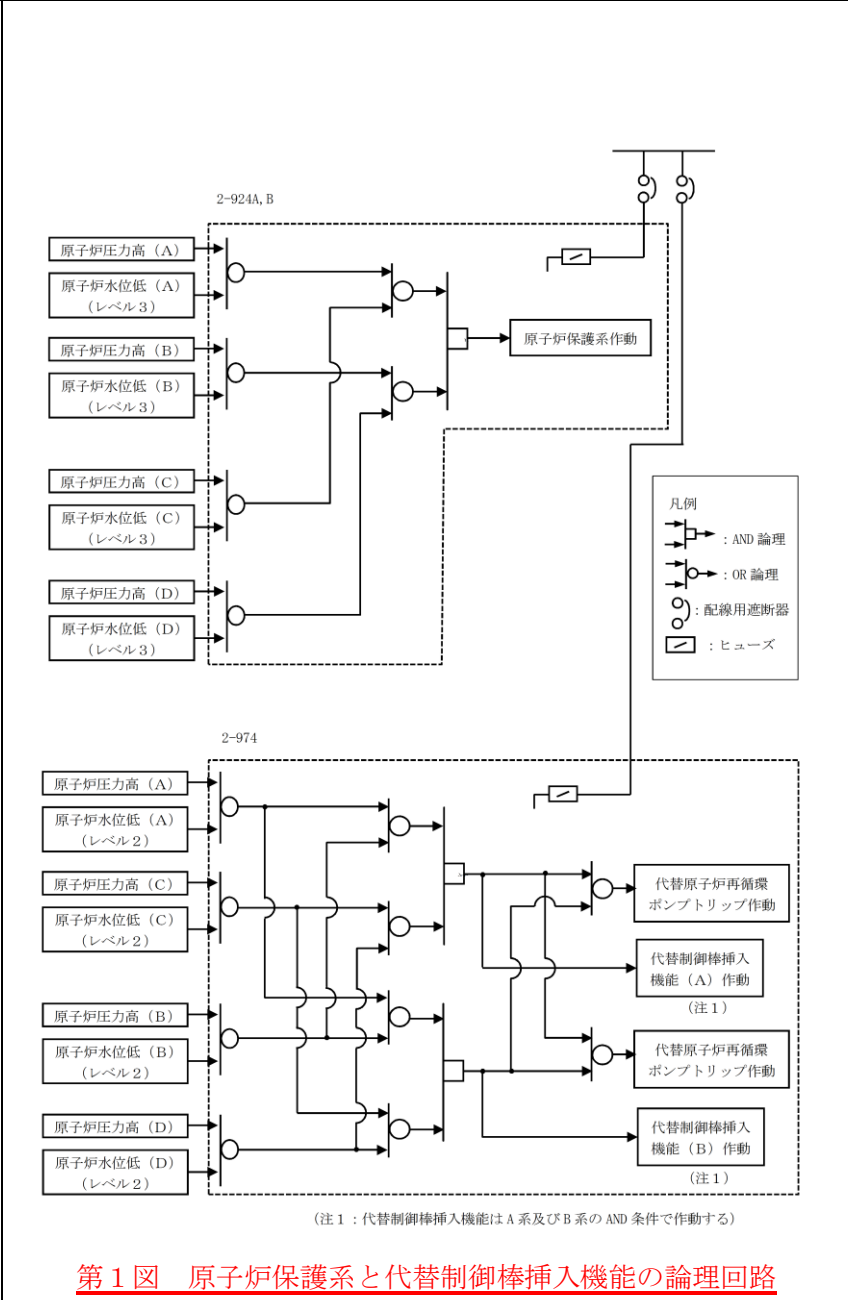
柏崎刈羽原子力発電所 6 / 7 号炉 (2017. 12. 20 版)	東海第二発電所 (2018. 9. 18 版)	島根原子力発電所 2 号炉	備考
		(3) <u>自動減圧系作動の条件信号回路追加について</u> a. <u>目的</u> <u>原子炉注水が行われない状態で自動減圧系が作動した場合、原子炉冷却材が急減するおそれがあることから、低圧注水系の待機状態で、自動減圧系を作動させるため、新たに低圧E C C S ポンプ（残留熱除去ポンプ又は低圧炉心スプレイ・ポンプ）の運転状態を条件信号として、自動減圧系の作動回路に追加する。</u> b. <u>条件信号回路</u> <u>自動減圧系に追加する条件信号回路を第 4 図に示す。この条件信号回路は、単一故障等により本来の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設置するものとする。</u> c. <u>自動減圧系への影響について</u> <u>自動減圧系作動回路に追加する条件信号回路が、自動減圧系に対して悪影響を与えないことを第 4 表に示す。</u>	・設備の相違 【柏崎 6/7，東海第二】 設備構成の相違による安全保護回路の変更に係る工事の抽出結果の相違

柏崎刈羽原子力発電所 6／7号炉 (2017.12.20版)	東海第二発電所 (2018.9.18版)	島根原子力発電所 2号炉	備考										
		第4表 自動減圧系への影響 <table><tr><th>設置許可基準規則 第24条 (安全保護回路)</th><th>自動減圧系への影響</th></tr><tr><td>発電用原子炉施設には、次に掲げるところにより、安全保護回路 (安全施設に属するものに限る。以下この条において同じ。)を設けなければならない。 一 運転時の異常な過渡変化が発生する場合において、その異常な状態を検知し、及び原子炉停止系統その他系統と併せて機能することにより、燃料要素の許容損傷限界を超えないようにできるものとする。</td><td>自動減圧系は設計基準事象 (中小破断LOCA)の際に使用するものであり、運転時の異常な過渡変化時には使用しないため問題ない。</td></tr><tr><td>二 設計基準事故が発生する場合において、その異常な状態を検知し、原子炉停止系統及び工学的安全施設を自動的に作動させるものとする。</td><td>条件信号回路を追加しても、低圧注水系が待機状態にある場合は、異常な状態を検知し自動的に作動させることができる。 自動減圧系は、低圧炉心注水を促進することを目的とした設備であり問題ない。</td></tr><tr><td>三 安全保護回路を構成する機械若しくは器具又はチャンネルは、単一故障が起きた場合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。</td><td>自動減圧系の多重性、独立性に悪影響を与えないよう、区分ごとに条件信号回路を設けているため問題ない。</td></tr><tr><td>四 安全保護回路を構成するチャンネルは、それぞれ互いに分離し、それぞれのチャンネル間において安全保護機能を失わないように独立性を確保するものとする。</td><td>自動減圧系の多重性、独立性に悪影響を与えないよう、区分ごとに条件信号回路を設けているため問題ない。</td></tr></table>	設置許可基準規則 第24条 (安全保護回路)	自動減圧系への影響	発電用原子炉施設には、次に掲げるところにより、安全保護回路 (安全施設に属するものに限る。以下この条において同じ。)を設けなければならない。 一 運転時の異常な過渡変化が発生する場合において、その異常な状態を検知し、及び原子炉停止系統その他系統と併せて機能することにより、燃料要素の許容損傷限界を超えないようにできるものとする。	自動減圧系は設計基準事象 (中小破断LOCA)の際に使用するものであり、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。	条件信号回路を追加しても、低圧注水系が待機状態にある場合は、異常な状態を検知し自動的に作動させることができる。 自動減圧系は、低圧炉心注水を促進することを目的とした設備であり問題ない。	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。	自動減圧系の多重性、独立性に悪影響を与えないよう、区分ごとに条件信号回路を設け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。	自動減圧系の多重性、独立性に悪影響を与えないよう、区分ごとに条件信号回路を設けているため問題ない。	
設置許可基準規則 第24条 (安全保護回路)	自動減圧系への影響												
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。	自動減圧系は設計基準事象 (中小破断LOCA)の際に使用するものであり、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。	条件信号回路を追加しても、低圧注水系が待機状態にある場合は、異常な状態を検知し自動的に作動させることができる。 自動減圧系は、低圧炉心注水を促進することを目的とした設備であり問題ない。												
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。	自動減圧系の多重性、独立性に悪影響を与えないよう、区分ごとに条件信号回路を設け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。	自動減圧系の多重性、独立性に悪影響を与えないよう、区分ごとに条件信号回路を設けているため問題ない。												

柏崎刈羽原子力発電所 6 / 7 号炉 (2017. 12. 20 版)	東海第二発電所 (2018. 9. 18 版)	島根原子力発電所 2 号炉	備考								
		<table><tr><th>設置許可基準規則 第 24 条 (安全保護回路)</th><th>自動減圧系への影響</th></tr><tr><td>五 駆動源の喪失、系統の遮断その他の不利な状況が発生した場合においても、発電用原子炉施設をより安全な状態に移行するか、又は当該状態を維持することにより、発電用原子炉施設の安全上支障がない状態を維持できるものとする。</td><td>自動減圧系は、駆動源である電源の喪失で系統の現状維持（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。追加する条件信号回路はこの安全保護動作を阻害するものではない。</td></tr><tr><td>六 不正アクセス行為その他の電子計算機に使用目的に沿うべき動作をさせず、又は使用目的に反する動作をさせる行為による被害を防止することができるものとする。</td><td>条件信号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。</td></tr><tr><td>七 計測制御系統施設の一部を安全保護回路と共用する場合には、その安全保護機能を失わないよう、計測制御系統施設から機能的に分離されたものとする。</td><td>計測制御系とは共用していないため、影響はない。</td></tr></table>	設置許可基準規則 第 24 条 (安全保護回路)	自動減圧系への影響	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。	自動減圧系は、駆動源である電源の喪失で系統の現状維持（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。追加する条件信号回路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。	条件信号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。	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 24 条 (安全保護回路)	自動減圧系への影響								
		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。	自動減圧系は、駆動源である電源の喪失で系統の現状維持（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。追加する条件信号回路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。	条件信号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。	計測制御系とは共用していないため、影響はない。								
		<table><tr><th>設置許可基準規則 第 12 条 (安全施設)</th><th>自動減圧系への影響</th></tr><tr><td>4 安全施設は、その健全性及び能力を確認するため、その安全機能の重要度に応じ、発電用原子炉の運転中又は停止中に試験又は検査ができるものでなければならない。</td><td>条件信号回路を設けることで自動減圧系の試験に影響を与えることはない。</td></tr></table>	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。	条件信号回路を設けることで自動減圧系の試験に影響を与えることはない。					
		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。	条件信号回路を設けることで自動減圧系の試験に影響を与えることはない。								

柏崎刈羽原子力発電所 6 / 7 号炉 (2017. 12. 20 版)	東海第二発電所 (2018. 9. 18 版)	島根原子力発電所 2 号炉	備考
		 The diagram illustrates the logic for the automatic pressure reduction system, incorporating additional condition signals. It is organized into four main sections, each corresponding to a different reactor (A, C, B, D). Each section includes a set of input conditions (e.g., 'A-ドライウエル圧力高', 'A-原子炉水位低(レベル1)', 'A-原子炉水位低(レベル3)') and a corresponding output signal ('A-自動減圧起動阻止 SW'). The logic involves AND gates, OR gates, and time delays (T.P.U. 120秒). A legend in the top right corner defines the symbols: AND gate, OR gate, time delay (T.P.U.), and signal inhibition ((W,0)). 凡例 - AND - T.P.U. (120 秒) - OR (W,0) : 信号阻止 第4図 自動減圧系に追加する条件信号回路図	

柏崎刈羽原子力発電所 6／7号炉 (2017.12.20版)	東海第二発電所 (2018.9.18版)	島根原子力発電所 2号炉	備考
参考1 新規制対応設備の安全保護系への影響について 1. 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、制御棒駆動機構を作動させる原子炉緊急停止系の故障によるATWS発生時に、スクラム用計装空気配管に取り付けられた排気弁を開放することによって制御棒を急速に挿入し、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 原子炉緊急停止系と代替制御棒挿入機能のロジック回路は第1図のとおり、検出器からロジックまで、原子炉緊急停止系と代替制御棒挿入機能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する。 なお、第2図のとおり原子炉緊急停止系の作動電磁弁についても、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する。	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 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、発電用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。	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. 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、制御棒駆動機構を作動させる原子炉保護系の故障によるATWS発生時に、スクラム用計装空気配管に取り付けられた排気弁を開放することによって制御棒を急速に挿入し、原子炉出力を低下させることを目的とする。 (2) 原子炉保護系への影響について 原子炉保護系と代替制御棒挿入機能の論理回路は第1図のとおり、検出器から論理回路まで、原子炉保護系と代替制御棒挿入機能は独立した構成となっており、原子炉保護系に悪影響を与えない設計とする。 なお、第2図のとおり原子炉保護系の作動電磁弁についても、代替制御棒挿入機能と原子炉保護系では独立した構成とする。	

柏崎刈羽原子力発電所 6／7号炉 (2017.12.20版)	東海第二発電所 (2018.9.18版)	島根原子力発電所 2号炉	備考
 第1図 原子炉緊急停止系及び代替制御棒挿入機能のロジック図	 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1図 原子炉保護系と代替制御棒挿入機能の論理回路	・設備の相違 【柏崎 6/7，東海第二】 設備構成の相違による論理回路の相違

柏崎刈羽原子力発電所 6 / 7 号炉 (2017. 12. 20 版)	東海第二発電所 (2018. 9. 18 版)	島根原子力発電所 2 号炉	備考
凡例 NE : 常時励磁 ND : 常時無励磁 第2図 作動電磁弁について	凡例 電磁弁 空気配管 電気信号 第3図 作動電磁弁について	凡例 AND 論理 OR 論理 ARI : 代替制御棒挿入機能 NE : 常時励磁 ND : 常時無励磁 第2図 作動電磁弁について	・設備の相違 【柏崎 6/7, 東海第二】 設備構成の相違による系統構成の相違

柏崎刈羽原子力発電所 6／7号炉 (2017. 12. 20 版)	東海第二発電所 (2018. 9. 18 版)	島根原子力発電所 2号炉	備考
2. 代替自動減圧ロジック（代替自動減圧機能） (1) 目的 代替自動減圧機能は、原子炉冷却材圧力バウンダリが高圧の場合であって、自動減圧系が有する発電用原子炉の減圧機能が喪失するおそれがある場合又は発生した場合に、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 自動減圧系と代替自動減圧機能の論理回路は第3 図のとおりであり、自動減圧系に対して独立した論理回路を構成しており、自動減圧系に悪影響を与えない設計としている。 第4 図のとおり検出器（原子炉水位低（レベル1）、<u>残留熱除去系ポンプ吐出圧力高</u>）からの入力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氣的に分離しており、自動減圧系への悪影響を与えない設計とする。 <u>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氣的に分離しており、自動減圧系への悪影響を与えない設計とする。</u> なお、原子炉スクラム失敗時に自動減圧が自動起動すると、<u>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繋がるため、自動減圧系及び代替自動減圧機能の自動起動阻止回路を用いて、自動起動を阻止する設計とする。自動減圧系回路と代替自動減圧機能回路の自動起動阻止回路は、手動阻止スイッチ（ハードスイッチ）を共用しているが、ハードスイッチは単純な構造であり、スイッチ接点以降は分離していることから、自動減圧系に悪影響を与えない設計とする。</u>	1. <u>過渡時自動減圧機能</u>について (1) 目的 <u>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発電用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。</u> (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。 <u>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</u>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氣的に分離しており、自動減圧系への悪影響を与えない設計としている。 <u>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氣的に分離しており、自動減圧系への悪影響を与えない設計としている。</u>	2. <u>代替自動減圧ロジック（代替自動減圧機能）</u> (1) 目的 <u>代替自動減圧機能は、原子炉冷却材圧力バウンダリが高圧の場合であって、自動減圧系が有する発電用原子炉の減圧機能が喪失するおそれがある場合又は発生した場合に、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。</u> (2) 自動減圧系への影響について 自動減圧系と代替自動減圧機能の論理回路を第 3 図に示す。自動減圧系に対して独立した論理回路を構成しており、自動減圧系に悪影響を与えない設計としている。 <u>第 4 図のとおり原子炉水位低（レベル 1）、低圧炉心スプレイ・ポンプ運転及び残留熱除去ポンプ運転信号</u>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氣的に分離しており、自動減圧系への悪影響を与えない設計とする。 <u>なお、原子炉スクラム失敗時に自動減圧系が自動起動すると、高圧炉心スプレイ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繋がるため、自動減圧系及び代替自動減圧機能の自動起動阻止回路を用いて、自動起動を阻止する設計とする。自動減圧系及び代替自動減圧機能の自動起動阻止回路は、手動阻止スイッチ（ハードスイッチ）を分離することで、自動減圧系に悪影響を及ぼさない設計とする。</u>	・炉型の相違 【柏崎 6/7】 島根 2 号炉は BWR－5 であり低圧炉心スプレイ系を設置している ・設備の相違 【柏崎 6/7、東海第二】 島根 2 号炉は、ポンプ運転状態（遮断器閉）信号を作動条件に使用している ・設備の相違 【柏崎 6/7、東海第二】 島根 2 号炉は、自動減圧系と代替自動減圧系の作動用電磁弁を共用していない ・設備の相違 【柏崎 6/7】 島根 2 号炉は、手動阻止スイッチを共用していない

柏崎刈羽原子力発電所 6 / 7 号炉 (2017. 12. 20 版)	東海第二発電所 (2018. 9. 18 版)	島根原子力発電所 2 号炉	備考
第3 図 自動減圧機能及び代替自動減圧機能のロジック回路		第 3 図 自動減圧系及び代替自動減圧機能の論理回路	・設備の相違 【柏崎 6/7, 東海第二】 設備構成の相違による論理回路の相違（東海第二は別紙 2 第 2 図に記載）

柏崎刈羽原子力発電所 6 / 7 号炉 (2017. 12. 20 版)	東海第二発電所 (2018. 9. 18 版)	島根原子力発電所 2 号炉	備考
自動減圧系と代替自動減圧機能のロジック回路の電源は、それぞれ分離されており自動減圧系に悪影響を与えない設計とする(遮断器によって分離を実施)。 検出器 配線用遮断器 配線用遮断器 過がし安全弁用電磁弁 自動減圧系 代替自動減圧機能 原子炉水位検出器信号 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又は残熱除去系ポンプ(A)吐出圧力低下 隔離装置の概要図 警報設定器 設定値 出力信号 自動減圧系と電気的な隔離装置(リレー)を用いて信号を分離し、自動減圧系への悪影響を与えない設計とする。 第4 図 信号の分離について	自動減圧系と過渡時自動減圧機能の論理回路の電源は、それぞれ分離されており自動減圧系に悪影響を与えない設計とする(遮断器によって分離を実施)。 検出器 論理回路 ヒューズ 自動減圧機能 過渡時自動減圧機能 過がし安全弁用電磁弁 配線用遮断器 配線用遮断器 自動減圧系 代替自動減圧機能 原子炉水位検出器信号 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又は残熱除去系ポンプ(A)吐出圧力低下 隔離装置の概要図 警報設定器 設定値 出力信号 自動減圧系と電気的な隔離装置(リレー)を用いて信号を分離し、自動減圧系への悪影響を与えない設計とする。 第1 図 信号の分離について	自動減圧系と代替自動減圧機能の論理回路の電源は、それぞれ分離されており自動減圧系に悪影響を与えない設計とする(遮断器によって分離を実施)。 検出器 論理回路 ヒューズ 自動減圧系 代替自動減圧機能 原子炉水位検出器信号 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又は残熱除去系ポンプ(A)吐出圧力低下 隔離装置の概要図 警報設定器 設定値 出力信号 自動減圧系と電気的な隔離装置(リレー)を用いて信号を分離し、自動減圧系への悪影響を与えない設計とする。 第4 図 信号の分離について	・炉型の相違 【柏崎 6/7】 島根 2 号炉は BWR - 5 であり低圧炉心スプレイ系を設置している ・設備の相違 【柏崎 6/7, 東海第二】 島根 2 号炉は、自動減圧系と代替自動減圧系の作動用電磁弁を共用していない

柏崎刈羽原子力発電所 6／7号炉 (2017.12.20版)	東海第二発電所 (2018.9.18版)	島根原子力発電所 2号炉	備考
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から作動回路について、検出器はアナログ機器、作動回路はハードワイヤーロジック（リレーや配線によるアナログ回路）で構成されており、一部の安全保護回路への出力信号処理でデジタル型制御装置を使用している（<u>起動領域モニタ</u>、<u>平均出力領域モニタ</u>、<u>安全系放射線モニタ</u>）。例として、原子炉緊急停止系の構成例を第1図に示す。 不正アクセス行為等による対策については、「2.1 <u>安全保護系の不正アクセス行為防止のための措置について</u>」に記載の設計方針としている（下記に、「2.1」の記載内容の一部再掲）。 (1) 物理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、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 <u>安全保護系の信号は、安全保護系盤→プロセス計算機→防護装置→緊急時対策支援システム伝送装置（ERSS）→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</u>	別紙3 安全保護回路の不正アクセス行為等の防止対策 安全保護回路は、<u>検出信号処理において一部デジタル演算処理を行う機器がある他は、アナログ回路で構成している。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。</u> <u>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又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。</u> (1) 物理的及び電氣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、電氣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、<u>デジタル演算処理を行う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演算処理を行う機器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。</u> (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、<u>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</u>	別紙3 <u>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</u> <u>アナログ型安全保護回路の検出器から論理回路について、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（リレーや配線によるアナログ回路）で構成しており、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（原子炉保護系、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。原子炉保護系の構成例を第1図、抽出結果を第1表、第2表に示す。</u> <u>構成機器のうちデジタル処理部のある機器としてプロセス放射線モニタ及び平均出力計装の演算回路がある。ただし、これらのデジタル処理部のある機器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。</u> <u>不正アクセス行為等による対策については、「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」に記載の設計方針としている（下記に、「2.1」の記載内容の一部再掲）。</u> (1) 物理的アクセス及び電氣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、<u>電氣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、デジタル処理部と接続する保守ツールは施錠管理された場所に保管し、パスワード管理することで管理されない変更を防止している。</u> (2) ハードウェアの物理的な分離又は機能的な分離対策 <u>安全保護回路の信号は、安全保護回路→S.P.D.Sデータ収集サーバ→防護装置→S.P.D.S伝送サーバ→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</u>	・設備の相違 【柏崎 6/7】 ④の相違 ・運用の相違 【柏崎 6/7】 島根 2号炉は電氣的アクセスの制限対策についても記載 【東海第二】 ⑥の相違

柏崎刈羽原子力発電所 6／7号炉 (2017. 12. 20 版)	東海第二発電所 (2018. 9. 18 版)	島根原子力発電所 2号炉	備考
護系からは発信されるのみであり、外部からの信号を受信しないこと、及びハードウェアを直接接続しないことで物理的及び機能的分離を行っている。 (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 <u>安全保護系</u>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（通信状態を監視し、送信元、送信先及び送信内容を制限することにより、目的外の通信を遮断）を介して安全保護系盤の信号を一方向（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。 (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 <u>アナログ型安全保護回路は別紙1 のとおり。</u> <u>なお、ディジタル型制御装置（起動領域モニタ、平均出力領域モニタ、安全系放射線モニタ）については、「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）」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（V&V）がなされたソフトウェアを使用している。</u>また、安全保護系は、固有のプログラム言語を使用（一般的なコンピュータウイルスが動作しない環境）するとともに、保守以外の不要なソフトウェアへのアクセス制限対策として入域制限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 <u>安全保護系は、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にラインフィルタや絶縁回路を設置、外部からの信号入出力部にラインフィルタ</u>	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<u>安全保護回路</u>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。 <u>※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。</u> (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 安全保護回路の<u>デジタル演算処理を行う機器</u>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・<u>誘導サージ</u>・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	<u>全保護回路</u>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 <u>安全保護回路</u>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（<u>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</u>）を介して<u>安全保護系盤</u>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。 (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ない動作や変更を防ぐ対策 <u>アナログ型安全保護回路は別紙1 のとおり。</u> <u>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。</u> (5) 耐ノイズ・サージ対策 <u>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して</u>	・設備の相違 【柏崎 6/7】 ⑦の相違

柏崎刈羽原子力発電所 6／7号炉 (2017.12.20版)	東海第二発電所 (2018.9.18版)	島根原子力発電所 2号炉	備考
<u>や絶縁回路を設置</u>している。 (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 <u>ウイルスの侵入防止対策も含め、当社の安全保護系への妨害行為又は破壊行為を防止するため、第2.1表のようなセキュリティ対策を安全保護系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。なお、当社は供給者に対し、品質保証に関する監査を継続的に実施することにより、適切に管理されているかを確認することとしている。</u> <u>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している。</u> <u>※社内マニュアル3 次文書「Z-29・KK 業シス-01 情報システムへのウイルス対策ガイド」に規定</u>	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。	<u>いる。</u> <u>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。</u> <u>(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</u> <u>ウイルスの侵入防止対策も含め、当社の安全保護系への妨害行為又は破壊行為を防止するため、「2.1 (6)」に記載のセキュリティ対策を供給者へ要求することとしている。</u>	・設備の相違 【柏崎 6/7】 島根 2 号炉はアナログ型安全保護回路で金属シールド付ケーブルを使用しノイズ等の対策を図っている ・運用の相違 【柏崎 6/7，東海第二】 ⑨の相違

柏崎刈羽原子力発電所 6／7号炉 (2017. 12. 20 版)	東海第二発電所 (2018. 9. 18 版)	島根原子力発電所 2号炉	備考
アナログ型安全保護回路 (A1 チャンネル) の例 ※他の区分も同様 □ : デジタル機器 (参考) デジタル型安全保護回路 (区分Ⅰ) の例 ※他の区分も同様 □ : デジタル機器 第 1 図 安全保護回路の構成例 (原子炉緊急停止系)	安全保護系 充電器盤 (アナログ) 第 1 図 安全保護系構成概略図	アナログ型安全保護回路 (A1 チャンネル) の例 ※他の区分も同様 □ : デジタル処理部を含む機器 第 1 図 安全保護回路の構成例 (原子炉保護系)	・設備の相違 【柏崎 6/7】 ④の相違 【東海第二】 デジタル化している 設備の相違 (以下, ⑫ の相違)

柏崎刈羽原子力発電所　6／7号炉　（2017.12.20版）	東海第二発電所（2018.9.18版）	島根原子力発電所　2号炉	備考																																																																																																																		
	第1表　原子炉緊急停止系の構成機器 <table><tr><th rowspan="2">原子炉スクラム信号の種類</th><th colspan="2">構成機器</th></tr><tr><th>検出器</th><th>設定器</th></tr><tr><td>原子炉圧力高</td><td>アナログ</td><td>アナログ</td></tr><tr><td>原子炉水位低</td><td>アナログ</td><td>アナログ</td></tr><tr><td>ドライウェル圧力高</td><td>アナログ</td><td>アナログ</td></tr><tr><td>原子炉出力ペリオド短（起動領域計装）</td><td>アナログ</td><td>デジタル</td></tr><tr><td>中性子束高（起動及び平均出力領域計装）</td><td>アナログ</td><td>デジタル</td></tr><tr><td>中性子束低（平均出力領域計装）</td><td>アナログ</td><td>デジタル</td></tr><tr><td>中性子束計装動作不能（起動及び平均出力領域計装）</td><td>アナログ</td><td>デジタル</td></tr><tr><td>スクラム水排出容器水位高</td><td colspan="2">アナログ（接点）</td></tr><tr><td>主蒸気隔離弁閉</td><td colspan="2">アナログ（接点）</td></tr><tr><td>主蒸気管放射能高</td><td>アナログ</td><td>デジタル</td></tr><tr><td>主蒸気止め弁閉</td><td colspan="2">アナログ（接点）</td></tr><tr><td>蒸気加減弁急速閉</td><td colspan="2">アナログ（接点）</td></tr><tr><td>地震加速度大</td><td colspan="2">アナログ（接点）</td></tr><tr><td>原子炉モード・スイッチ「停止」</td><td colspan="2">アナログ（接点）</td></tr><tr><td>手動</td><td colspan="2">アナログ（接点）</td></tr></table>	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（起動及び平均出力領域計装）	アナログ	デジタル	中性子束低（平均出力領域計装）	アナログ	デジタル	中性子束計装動作不能（起動及び平均出力領域計装）	アナログ	デジタル	スクラム水排出容器水位高	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	アナログ（接点）		地震加速度大	アナログ（接点）		原子炉モード・スイッチ「停止」	アナログ（接点）		手動	アナログ（接点）		第1表　原子炉保護系の構成機器 <table><tr><th colspan="2">原子炉スクラム信号の種類</th><th>検出器</th><th>設定器</th></tr><tr><td colspan="2">原子炉圧力高</td><td>アナログ</td><td>アナログ</td></tr><tr><td colspan="2">原子炉水位低（レベル3）</td><td>アナログ</td><td>アナログ</td></tr><tr><td colspan="2">格納容器圧力高</td><td>アナログ</td><td>アナログ</td></tr><tr><td rowspan="2">中性子束高</td><td>平均出力領域計装</td><td>アナログ</td><td>デジタル</td></tr><tr><td>中間領域計装</td><td>アナログ</td><td>アナログ</td></tr><tr><td rowspan="2">中性子計装 不作動</td><td>平均出力領域計装</td><td>アナログ</td><td>デジタル</td></tr><tr><td>中間領域計装</td><td>アナログ</td><td>アナログ</td></tr><tr><td colspan="2" rowspan="2">スクラム排水容器水位高</td><td colspan="2">アナログ（接点）</td></tr><tr><td>アナログ</td><td>アナログ</td></tr><tr><td colspan="2">主蒸気隔離弁閉</td><td colspan="2">アナログ（接点）</td></tr><tr><td colspan="2">主蒸気止め弁閉</td><td colspan="2">アナログ（接点）</td></tr><tr><td colspan="2">蒸気加減弁急速閉</td><td colspan="2">アナログ（接点）</td></tr><tr><td colspan="2">主蒸気管放射線高</td><td>アナログ</td><td>デジタル</td></tr><tr><td colspan="2">地震大</td><td colspan="2">アナログ（接点）</td></tr><tr><td colspan="2">手動</td><td colspan="2">アナログ（接点）</td></tr><tr><td colspan="2">原子炉モード・スイッチ「停止」位置</td><td colspan="2">アナログ（接点）</td></tr></table>	原子炉スクラム信号の種類		検出器	設定器	原子炉圧力高		アナログ	アナログ	原子炉水位低（レベル3）		アナログ	アナログ	格納容器圧力高		アナログ	アナログ	中性子束高	平均出力領域計装	アナログ	デジタル	中間領域計装	アナログ	アナログ	中性子計装 不作動	平均出力領域計装	アナログ	デジタル	中間領域計装	アナログ	アナログ	スクラム排水容器水位高		アナログ（接点）		アナログ	アナログ	主蒸気隔離弁閉		アナログ（接点）		主蒸気止め弁閉		アナログ（接点）		蒸気加減弁急速閉		アナログ（接点）		主蒸気管放射線高		アナログ	デジタル	地震大		アナログ（接点）		手動		アナログ（接点）		原子炉モード・スイッチ「停止」位置		アナログ（接点）		・設備の相違 【柏崎 6/7】 ④の相違 【東海第二】 ⑫の相違
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（起動及び平均出力領域計装）	アナログ	デジタル																																																																																																																			
中性子束低（平均出力領域計装）	アナログ	デジタル																																																																																																																			
中性子束計装動作不能（起動及び平均出力領域計装）	アナログ	デジタル																																																																																																																			
スクラム水排出容器水位高	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	アナログ（接点）																																																																																																																				
地震加速度大	アナログ（接点）																																																																																																																				
原子炉モード・スイッチ「停止」	アナログ（接点）																																																																																																																				
手動	アナログ（接点）																																																																																																																				
原子炉スクラム信号の種類		検出器	設定器																																																																																																																		
原子炉圧力高		アナログ	アナログ																																																																																																																		
原子炉水位低（レベル3）		アナログ	アナログ																																																																																																																		
格納容器圧力高		アナログ	アナログ																																																																																																																		
中性子束高	平均出力領域計装	アナログ	デジタル																																																																																																																		
	中間領域計装	アナログ	アナログ																																																																																																																		
中性子計装 不作動	平均出力領域計装	アナログ	デジタル																																																																																																																		
	中間領域計装	アナログ	アナログ																																																																																																																		
スクラム排水容器水位高		アナログ（接点）																																																																																																																			
		アナログ	アナログ																																																																																																																		
主蒸気隔離弁閉		アナログ（接点）																																																																																																																			
主蒸気止め弁閉		アナログ（接点）																																																																																																																			
蒸気加減弁急速閉		アナログ（接点）																																																																																																																			
主蒸気管放射線高		アナログ	デジタル																																																																																																																		
地震大		アナログ（接点）																																																																																																																			
手動		アナログ（接点）																																																																																																																			
原子炉モード・スイッチ「停止」位置		アナログ（接点）																																																																																																																			

柏崎刈羽原子力発電所 6／7号炉 (2017.12.20版)	東海第二発電所 (2018.9.18版)	島根原子力発電所 2号炉	備考																																																																																																																				
	<u>第2表 工学的安全施設作動回路の構成機器</u> <table> <tr> <th rowspan="2">機能</th><th rowspan="2">信号の種類</th><th colspan="2">構成機器</th></tr> <tr> <th>検出器</th><th>設定器</th></tr> <tr> <td rowspan="6">主蒸気隔離弁閉</td><td>主蒸気管放射能高</td><td>アナログ</td><td>デジタル</td></tr> <tr> <td>主蒸気管圧力低</td><td>アナログ</td><td>アナログ</td></tr> <tr> <td>主蒸気管流量大</td><td>アナログ</td><td>アナログ</td></tr> <tr> <td>原子炉水位異常低下</td><td>アナログ</td><td>アナログ</td></tr> <tr> <td>主蒸気管トンネル温度高</td><td>アナログ</td><td>アナログ</td></tr> <tr> <td>復水器真空度低</td><td>アナログ</td><td>アナログ</td></tr> <tr> <td rowspan="2">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（低圧注水系）の起動</td><td>ドライウエル圧力高</td><td>アナログ</td><td>アナログ</td></tr> <tr> <td>原子炉水位異常低下</td><td>アナログ</td><td>アナログ</td></tr> <tr> <td rowspan="2">自動減圧系の作動</td><td>ドライウエル圧力高</td><td>アナログ</td><td>アナログ</td></tr> <tr> <td>原子炉水位異常低下</td><td>アナログ</td><td>アナログ</td></tr> <tr> <td rowspan="2">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</td><td>ドライウエル圧力高</td><td>アナログ</td><td>アナログ</td></tr> <tr> <td>原子炉水位異常低下</td><td>アナログ</td><td>アナログ</td></tr> <tr> <td rowspan="3">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</td><td>ドライウエル圧力高</td><td>アナログ</td><td>アナログ</td></tr> <tr> <td>原子炉水位低</td><td>アナログ</td><td>アナログ</td></tr> <tr> <td>原子炉建屋放射能高</td><td>アナログ</td><td>デジタル</td></tr> <tr> <td rowspan="3">主蒸気隔離弁以外の主要な隔離弁閉鎖</td><td>ドライウエル圧力高</td><td>アナログ</td><td>アナログ</td></tr> <tr> <td>原子炉水位低</td><td>アナログ</td><td>アナログ</td></tr> <tr> <td>原子炉水位異常低下</td><td>アナログ</td><td>アナログ</td></tr> </table>	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	主蒸気管流量大	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残留熱除去系（低圧注水系）の起動	ドライウエル圧力高	アナログ	アナログ	原子炉水位異常低下	アナログ	アナログ	自動減圧系の作動	ドライウエル圧力高	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	ドライウエル圧力高	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	ドライウエル圧力高	アナログ	アナログ	原子炉水位低	アナログ	アナログ	原子炉建屋放射能高	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	ドライウエル圧力高	アナログ	アナログ	原子炉水位低	アナログ	アナログ	原子炉水位異常低下	アナログ	アナログ	<u>第2表 工学的安全施設作動回路の構成機器</u> <table> <tr> <th>機能</th><th>信号の種類</th><th>検出器</th><th>設定器</th></tr> <tr> <td rowspan="6">主蒸気隔離弁閉鎖</td><td>原子炉水位低（レベル2）</td><td>アナログ</td><td>アナログ</td></tr> <tr> <td>主蒸気管圧力低</td><td>アナログ</td><td>アナログ</td></tr> <tr> <td>主蒸気管流量大</td><td>アナログ</td><td>アナログ</td></tr> <tr> <td>復水器真空度低</td><td>アナログ</td><td>アナログ</td></tr> <tr> <td>主蒸気管放射線高</td><td>アナログ</td><td>デジタル</td></tr> <tr> <td>主蒸気管周囲温度高</td><td>アナログ</td><td>アナログ</td></tr> <tr> <td rowspan="2">主蒸気隔離弁以外の主要な隔離弁閉鎖</td><td>格納容器圧力高</td><td>アナログ</td><td>アナログ</td></tr> <tr> <td>原子炉水位低（レベル3）</td><td>アナログ</td><td>アナログ</td></tr> <tr> <td rowspan="4">非常用ガス処理系起動</td><td>原子炉棟排気放射線高</td><td>アナログ</td><td>デジタル</td></tr> <tr> <td>燃料取替階放射線高</td><td>アナログ</td><td>デジタル</td></tr> <tr> <td>格納容器圧力高</td><td>アナログ</td><td>アナログ</td></tr> <tr> <td>原子炉水位低（レベル3）</td><td>アナログ</td><td>アナログ</td></tr> <tr> <td rowspan="2">高圧炉心スプレイ系及び同ディーゼル起動</td><td>格納容器圧力高</td><td>アナログ</td><td>アナログ</td></tr> <tr> <td>原子炉水位低（レベル1H）</td><td>アナログ</td><td>アナログ</td></tr> </table>	機能	信号の種類	検出器	設定器	主蒸気隔離弁閉鎖	原子炉水位低（レベル2）	アナログ	アナログ	主蒸気管圧力低	アナログ	アナログ	主蒸気管流量大	アナログ	アナログ	復水器真空度低	アナログ	アナログ	主蒸気管放射線高	アナログ	デジタル	主蒸気管周囲温度高	アナログ	アナログ	主蒸気隔離弁以外の主要な隔離弁閉鎖	格納容器圧力高	アナログ	アナログ	原子炉水位低（レベル3）	アナログ	アナログ	非常用ガス処理系起動	原子炉棟排気放射線高	アナログ	デジタル	燃料取替階放射線高	アナログ	デジタル	格納容器圧力高	アナログ	アナログ	原子炉水位低（レベル3）	アナログ	アナログ	高圧炉心スプレイ系及び同ディーゼル起動	格納容器圧力高	アナログ	アナログ	原子炉水位低（レベル1H）	アナログ	アナログ	・設備の相違 【柏崎6/7】 ④の相違 【東海第二】 ⑫の相違
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																																																																																																																				
	主蒸気管流量大	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残留熱除去系（低圧注水系）の起動	ドライウエル圧力高	アナログ	アナログ																																																																																																																				
	原子炉水位異常低下	アナログ	アナログ																																																																																																																				
自動減圧系の作動	ドライウエル圧力高	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	ドライウエル圧力高	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	ドライウエル圧力高	アナログ	アナログ																																																																																																																				
	原子炉水位低	アナログ	アナログ																																																																																																																				
	原子炉建屋放射能高	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	ドライウエル圧力高	アナログ	アナログ																																																																																																																				
	原子炉水位低	アナログ	アナログ																																																																																																																				
	原子炉水位異常低下	アナログ	アナログ																																																																																																																				
機能	信号の種類	検出器	設定器																																																																																																																				
主蒸気隔離弁閉鎖	原子炉水位低（レベル2）	アナログ	アナログ																																																																																																																				
	主蒸気管圧力低	アナログ	アナログ																																																																																																																				
	主蒸気管流量大	アナログ	アナログ																																																																																																																				
	復水器真空度低	アナログ	アナログ																																																																																																																				
	主蒸気管放射線高	アナログ	デジタル																																																																																																																				
	主蒸気管周囲温度高	アナログ	アナログ																																																																																																																				
主蒸気隔離弁以外の主要な隔離弁閉鎖	格納容器圧力高	アナログ	アナログ																																																																																																																				
	原子炉水位低（レベル3）	アナログ	アナログ																																																																																																																				
非常用ガス処理系起動	原子炉棟排気放射線高	アナログ	デジタル																																																																																																																				
	燃料取替階放射線高	アナログ	デジタル																																																																																																																				
	格納容器圧力高	アナログ	アナログ																																																																																																																				
	原子炉水位低（レベル3）	アナログ	アナログ																																																																																																																				
高圧炉心スプレイ系及び同ディーゼル起動	格納容器圧力高	アナログ	アナログ																																																																																																																				
	原子炉水位低（レベル1H）	アナログ	アナログ																																																																																																																				

柏崎刈羽原子力発電所 6／7号炉 (2017.12.20版)	東海第二発電所 (2018.9.18版)	島根原子力発電所 2号炉				備考
		機能	信号の種類	検出器	設定器	
		低圧炉心スプレ 系起動	格納容器圧力高	アナログ	アナログ	
			原子炉水位低（レベル1）	アナログ	アナログ	
		低圧注水 系起動	格納容器圧力高	アナログ	アナログ	
			原子炉水位低（レベル1）	アナログ	アナログ	
		自動減圧 系作動	格納容器圧力高	アナログ	アナログ	
			原子炉水位低（レベル1）	アナログ	アナログ	
		非常用デ イゼル 発電機起 動	格納容器圧力高	アナログ	アナログ	
			原子炉水位低（レベル1）	アナログ	アナログ	

柏崎刈羽原子力発電所 6／7号炉 (2017.12.20版)	東海第二発電所 (2018.9.18版)	島根原子力発電所 2号炉	備考
別紙4 ソフトウェア更新時の立会において、インサイダー等に対するセキュリティ対策 <u>安全保護系制御装置のソフトウェア変更にあたっては、以下の対策を実施している。</u> ・<u>ソフトウェア変更に必要な保守ツール、記憶媒体については、保管庫内の施錠されたラック内に保管している。また、保守ツール使用時は安全保護系制御装置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している。</u> ・<u>保管庫内の施錠されたラック内に保管した保守ツール、記憶媒体は、使用の際に当社監理員立ち会いの下、貸し出しを行っている。</u> ・<u>保守ツールの接続部の鍵は、当直長の許可を得た上で、貸し出しを行っている。</u> ・ソフトウェア変更に係わる者は、情報セキュリティ教育（1回／年）を受講している。	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 <u>安全保護回路について、検出器から論理回路入口までの構成機器のうちデジタル演算処理を行う機器は、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。</u> <u>データ収集端末については、デジタル演算処理を行う機器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。</u> <u>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。</u>	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 <u>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、放射線モニタと平均出力領域計装である。これらについては、以下の対策を実施している。</u> ・<u>保守ツールについては、施錠管理されたラック内に保管する。また、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。</u> ・<u>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<u>うえ</u>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。</u> ・<u>ソフトウェア変更に係わる者は、情報セキュリティ教育を受講している。</u>	・運用の相違 【柏崎6/7】 ⑩の相違 【東海第二】 島根2号炉で使用する保守ツールは送信機能もあり、パスワード管理をしている ・運用の相違 【東海第二】 島根2号炉は、ソフトウェア変更に係わる者に対して、情報セキュリティ教育受講を要求している

柏崎刈羽原子力発電所 6／7号炉 (2017.12.20版)	東海第二発電所 (2018.9.18版)	島根原子力発電所 2号炉	備考
別紙5 <u>デジタル型安全保護回路</u>のシステムへ接続可能なアクセスについて <u>安全保護回路等を含むネットワーク全体構成図は第1図及び第2図のとおりであり、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は、安全保護回路へのネットワーク上の接続可能なアクセスと安全保護系制御装置のソフトウェアへ直接アクセス可能な保守ツール接続箇所となる。</u> <u>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は、以下のとおり対策をしている。</u> (2) <u>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</u> <u>安全保護回路へのネットワーク上の接続可能なアクセスについては、機能的に分離する設計としている。具体的には、安全保護回路と計測制御系は第3図に示すように、通信コントローラとマイクロプロセッサとの間は、通信専用のメモリを介することにより、通信コントローラが直接安全保護系のマイクロプロセッサの動作に関与しない設計とし、機能的に分離している為、計測制御系が安全保護回路のマイクロプロセッサの動作には関与しない。</u>	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 <u>安全保護回路は、検出信号処理において一部デジタル演算処理を行う機器がある他は、アナログ回路で構成している。</u> デジタル演算処理を行う機器への接続可能なアクセスとして、<u>データ収集端末の接続</u>がある。こちらについては以下のとおり対策する。 (1) <u>データ収集端末</u>による不正アクセスの防止対策 <u>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演算処理を行う機器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。</u>	別紙5 <u>安全保護回路のうちデジタル部分</u>のシステムへ接続可能なアクセスについて <u>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ロジック（リレーや配線によるアナログ回路）で構成されており、ソフトウェアを用いないアナログ回路であるが、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。</u> <u>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として、保守ツールがある。こちらについては以下のとおり対策する。</u> (1) <u>保守ツール</u>による不正アクセスの防止対策 <u>保守ツールは、出力領域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が、保守ツールは施錠管理された場所に保管し、パスワード管理することで管理されない変更を防止している。</u>	・設備及び運用の相違 【柏崎6/7】 ⑪の相違 ・設備の相違 【東海第二】 ⑥の相違 ・設備の相違 【東海第二】 ⑥の相違

柏崎刈羽原子力発電所 6／7号炉 (2017. 12. 20 版)	東海第二発電所 (2018. 9. 18 版)	島根原子力発電所 2号炉	備考
(3) 物理的アクセスの制限対策 安全保護系制御装置のソフトウェアへアクセス可能な保守ツールについては、保管庫内の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、使用時は安全保護系制御装置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している。 第1 図 ネットワーク全体構成概念図 (6 号炉 RPS/MSIV の例) 第2 図 ネットワーク全体構成概念図 (7 号炉 RPS/MSIV の例)	(2) 物理的アクセスの制限 <u>データ収集端末</u>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。	(2) 物理的アクセスの制限対策 <u>保守ツール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。</u> 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。 <u>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。</u>	・設備の相違 【東海第二】 ⑥の相違 ・記載方針の相違 【柏崎 6/7】 島根 2 号炉は、発電所への入域における物理的アクセスの制限対策についても記載している ・設備の相違 【柏崎 6/7】 デジタル型・アナログ型安全保護回路による設備構成の相違

柏崎刈羽原子力発電所 6／7号炉 (2017.12.20版)	東海第二発電所 (2018.9.18版)	島根原子力発電所 2号炉	備考
 第3 図 安全保護回路と計測制御系との信号取合概念図			

柏崎刈羽原子力発電所 6／7号炉 (2017.12.20版)	東海第二発電所 (2018.9.18版)	島根原子力発電所 2号炉	備考
別紙6 <u>デジタル型安全保護回路</u>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、<u>デジタル安全保護系ソフトウェアは、設計、製作、試験、変更管理の各段階で、「安全保護系へのデジタル計算機の適用に関する規程」（JEAC4620）及び「デジタル安全保護系の検証及び妥当性確認に関する指針」（JEAG4609）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。</u>	別紙 6 <u>安全保護回路のうちデジタル部分</u>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、<u>デジタル演算処理を行う機器は、工場出荷前試験及び導入時における試験を実施することにより、要求される機能を満足することの確認及び未使用機能等による悪影響がないことの確認が供給者によって確実に実施されていることを確認している。</u>	別紙6 <u>安全保護回路のうちデジタル部分</u>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、<u>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。</u> <u>なお、安全保護回路のうちデジタル部分については、未使用機能がないことを確認している。</u>	・運用の相違 【柏崎 6/7】 ⑦の相違 ・運用の相違 【柏崎 6/7，東海第二】 島根 2 号炉は，未使用機能の有無の確認結果を記載

柏崎刈羽原子力発電所 6／7号炉 (2017.12.20版)	東海第二発電所 (2018.9.18版)	島根原子力発電所 2号炉	備考
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 安全保護系に関わる過去のトラブル情報を抽出し、<u>柏崎刈羽原子力発電所6号及び7号炉の安全保護系の設計面</u>へ反映すべき事項を下記のとおり確認した。 (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。 ① 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 ② キーワード検索（安全保護系、<u>原子炉緊急停止系</u>、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 ③ 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) 過去の不具合事例への対応について 過去の不具合事例を抽出し、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、対応済み、若しくは、反映不要であることを確認した。	別紙8 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、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とおり確認した。 (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、<u>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。</u> <u>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。</u>	別紙7 安全保護系の過去のトラブル（落雷による<u>原子炉</u>スクラム動作事象等）の反映事項 安全保護系に係る過去のトラブル情報を抽出し、<u>島根原子力発電所2号炉の安全保護系の設計面</u>へ反映すべき事項を下記のとおり確認した。 (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。 ①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 ②キーワード検索（安全保護系、<u>原子炉保護系</u>、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 ③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) 過去の不具合事例への対応について <u>過去の不具合事例を抽出し、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、対応済み、もしくは、反映不要であることを確認した。</u>	

柏崎刈羽原子力発電所 6 / 7 号炉 (2017. 12. 20 版)	東海第二発電所 (2018. 9. 18 版)	島根原子力発電所 2 号炉	備考																											
<pre>graph TD; A[ニューシア情報] --> B{安全保護系に影響を及ぼさない事象}; B -- YES --> C[対象外]; B -- NO --> D{人的要因による事象}; D -- YES --> E[操作・手順ミスによる不具合事象 (55 件)]; D -- NO --> F{設備の不具合(設計面への反映なし)による事象}; F -- YES --> G[一過性及び基板故障等の設備不具合 (124 件)]; F -- NO --> H[不具合事象に対して設計面の対策を実施した事象 (1 件)];</pre> 第1 図 設計面への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 <table><tr><th>項目</th><th>事象例</th><th>理由</th></tr><tr><td>人的要因による事象</td><td>安全処置の実施又は復旧時のミス, 作業手順のミス等</td><td>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。</td></tr><tr><td>設備の不具合 (設計面への反映なし) による事象</td><td>計器・部品の単品故障・一過性故障・偶発故障等</td><td>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。</td></tr></table>	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。	<pre>graph TD; A[ニューシア情報] --> B{安全保護系に影響を及ぼさない事象}; B -- YES --> C[対象外]; B -- NO --> D{人的要因による事象}; D -- YES --> E[操作・手順ミスによる不具合事象 (60 件)]; D -- NO --> F{設備の不具合, プラント固有の原因(設計面への反映無し)による事象}; F -- YES --> G[一過性及び基板故障等の設備不具合, 事象発生プラント固有の原因による不具合 (125 件)]; F -- NO --> H[不具合事象に対して設計面の対策を実施した事象 (1 件)];</pre> 第1 図 設計面へ反映が必要となる事象の抽出フロー 第1 表 設計面への反映を不要とする理由 <table><tr><th>項目</th><th>事象例</th><th>理由</th></tr><tr><td>人的要因による事象</td><td>安全処置の実施又は復旧時のミス, 作業手順のミス等</td><td>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。</td></tr><tr><td>設備の不具合, プラント固有の原因 (設計面への反映無し) による事象</td><td>計器・部品の単体故障, 一過性故障, 偶発故障等 プラント固有の原因によるケーブルへのノイズ混入や機器振動の計装配管への伝搬による誤動作</td><td>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。 事象発生プラント固有の原因によるものであり, 東海第二発電所の設計面へ反映すべき事項ではない。</td></tr></table>	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, プラント固有の原因 (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 プラント固有の原因によるケーブルへのノイズ混入や機器振動の計装配管への伝搬による誤動作	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。 事象発生プラント固有の原因によるものであり, 東海第二発電所の設計面へ反映すべき事項ではない。	<pre>graph TD; A[ニューシア情報] --> B{安全保護系に影響を及ぼさない事象}; B -- YES --> C[対象外]; B -- NO --> D{人的要因による事象}; D -- YES --> E[操作・手順ミスによる不具合事象 (60 件)]; D -- NO --> F{設備の不具合(設計面への反映無し)による事象}; F -- YES --> G[一過性及び基板故障等の設備不具合 (125 件)]; F -- NO --> H[不具合事象に対して設計面の対策を実施した事象 (1 件)];</pre> 第1 図 設計面へ反映すべき事項の抽出フロー 第1 表 設計面へ反映不要とする理由 <table><tr><th>項目</th><th>事象例</th><th>理由</th></tr><tr><td>人的要因による事象</td><td>安全処置の実施又は復旧時のミス, 作業手順のミス等</td><td>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。</td></tr><tr><td>設備の不具合 (設計面への反応無し) による事象</td><td>計器・部品の単品故障・一過性故障・偶発故障等</td><td>故障した部品の交換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。</td></tr></table>	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 (設計面への反応無し) による事象	計器・部品の単品故障・一過性故障・偶発故障等	故障した部品の交換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。	・記載表現の相違 【東海第二】 東海第二は, プラント固有の原因による不具合は, 反映不要とすることを明記している
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。																												
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, プラント固有の原因 (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 プラント固有の原因によるケーブルへのノイズ混入や機器振動の計装配管への伝搬による誤動作	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。 事象発生プラント固有の原因によるものであり, 東海第二発電所の設計面へ反映すべき事項ではない。																												
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 (設計面への反応無し) による事象	計器・部品の単品故障・一過性故障・偶発故障等	故障した部品の交換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。																												

柏崎刈羽原子力発電所　6／7号炉　（2017.12.20版）		東海第二発電所　（2018.9.18版）		島根原子力発電所　2号炉		備考	
第2表　抽出された過去の不具合事象		第2表　抽出された過去の不具合事象		第2表　抽出された過去の不具合事象		・設備の相違	
件名		原子炉保護系チャンネルAのトリップについて		島根原子力発電所1号機　「中性子束異常高」信号による原子炉自動停止について		【柏崎 6/7，東海第二】	
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		中国電力株式会社　島根原子力発電所1号機		安全保護系に影響を	
発生日		1982年3月18日		1992年02月20日		及ぼした事象として、	
事象概要		出力1，　1 0 0 MWで定常運転中の3月1 8日1 6時5 6分、原子炉保護系チャンネルAが、原子炉圧力高（A 2）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。		島根原子力発電所1号機は、定格出力（4 6 0 MW _e ）で運転中のところ、平成4年2月2 0日1 1時3 2分「APRM異常高／不作動」の警報が発生し、原子炉が自動停止した。 調査の結果、平均出力領域モニタ（以下、APRM）全6チャンネル中3チャンネル（2， 3， 6）に「中性子束異常高」信号が発生（表示灯が点灯）し、原子炉保護系が動作したものであることが確認された。 また、APRM記録計のチャートでは、APRM全6チャンネル中3チャンネル（2， 3， 6）に、指示値の上昇がわずかに（最大1 0 3 %程度まで）認められた。 一方、原子炉自動停止直前のプラント主要パラメータ（原子炉圧力、原子炉水位、炉心流量等）については、有意な変化は認められなかった。 なお、これによる外部への放射能の影響はなかった。		島根2号炉は、柏崎 6/7と同様に落雷によるノイズの影響を受けた不	
<時系列> 8/22 20:12　「主蒸気管放射能高　区分（Ⅰ）（Ⅲ）」発生 主蒸気隔離弁（内側弁）　「全閉」　実動作 主蒸気ドレン内側弁　「全閉」　実動作 （点検のため上記弁は「全開」であった。なお、主蒸気隔離弁（外側弁）は、「全閉」であった） 「原子炉スクラム」発生（ゼロスクラム） 「スクラムパイロットエア－ヘッダー圧力低」発生 「CRD 充てん水圧力低低」発生 20:22　主蒸気管放射線モニタ　中操確認 区分Ⅰ：レベル高・高高ランプ　点灯　スクラム後指示値　2.0E-13A 区分Ⅱ：警報発生なし　スクラム後指示値　2.0E-13A 区分Ⅲ：レベル高・高高ランプ・下限点灯　スクラム後指示値　2.2E-13A 区分Ⅳ：下限　点灯　スクラム後指示値　ダウンスケール （スクラム前の指示については、記録計が停止中のため採取できず） 20:40　主蒸気隔離弁（内側弁）現場確認：異常なし 20:51～20:54　主蒸気管放射線モニタ（区分Ⅰ～Ⅳ）インターロック除外実施（機能要求はないため再発防止として実施） 21:01　スクラムリセット実施 21:08　HCU 廻り現場確認：異常なし		原因調査の概要 当該圧力スイッチ（B 2 2－N 0 2 3 C）の較正確認試験を実施した結果、セット値7 3． 3 k g／c m ² g（原子炉施設保安規定に定める設定値は7 4． 0 k g／c m ² g）に対し、動作値は7 2． 1 k g／c m ² gであり、動作値がセット値に対し1． 2 k g／c m 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（B 2 2－N 0 2 3 C）は、昨年7月2 8， 2 9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． 3 5 k g／c m 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1 2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。		【原因調査の概要】 （1）「中性子束異常高」信号発生 の要因分析 「中性子束異常高」信号の発生する要因としては、原子炉圧力上昇、炉心流量の増加、炉水温度低下、中性子束を上昇させる操作の実施およびA P R M誤動作の可能性が考えられる。 要因分析に基づき点検調査を行った結果、「中性子束異常高」信号は、実際に中性子束が異常に上昇して発生したものではなく、落雷に伴うノイズ混入によるA P R Mの誤動作で発生したものである可能性強いことがわかった。 （2）落雷に係る調査 6 6 k V鹿島線の避雷器の動作が確認された。また、発電所構内建物、構築物、避雷針について調査したところ、1号機原子炉建物避雷針に新しい落雷の痕跡が認められた。 （3）落雷による中性子計測設備への影響 a．1号機原子炉建物避雷針への落雷により、中性子計測設備に誘導電流が生じた。誘導電流はケーブル長に比例するため、ケーブル長の長いチャンネル2， 3， 6により大きな誘導電流が流れたものと判断された。 b．中性子計測設備のケーブル構成を模擬し、模擬パルス電流を印加して誘導電流を発生させたところ、中性子計測設備のケーブルに「中性子束異常高」スクラム信号レベルを超える信号変化が生じることが確認された。 【事象の原因】 1号機原子炉建物避雷針へ落雷があり、中性子計測設備のケーブルに誘導電流が流れ、これが通常レベルの電流信号に重畳したため、「中性子束異常高」の誤信号が発信したものと推定された。		不具合事象が抽出されたが、いずれも必要な対策を実施している	
原因 雷によるノイズ		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、動作したのと考えられる。		原因 【原因調査の概要】 （1）「中性子束異常高」信号発生 の要因分析 「中性子束異常高」信号の発生する要因としては、原子炉圧力上昇、炉心流量の増加、炉水温度低下、中性子束を上昇させる操作の実施およびA P R M誤動作の可能性が考えられる。 要因分析に基づき点検調査を行った結果、「中性子束異常高」信号は、実際に中性子束が異常に上昇して発生したものではなく、落雷に伴うノイズ混入によるA P R Mの誤動作で発生したものである可能性強いことがわかった。 （2）落雷に係る調査 6 6 k V鹿島線の避雷器の動作が確認された。また、発電所構内建物、構築物、避雷針について調査したところ、1号機原子炉建物避雷針に新しい落雷の痕跡が認められた。 （3）落雷による中性子計測設備への影響 a．1号機原子炉建物避雷針への落雷により、中性子計測設備に誘導電流が生じた。誘導電流はケーブル長に比例するため、ケーブル長の長いチャンネル2， 3， 6により大きな誘導電流が流れたものと判断された。 b．中性子計測設備のケーブル構成を模擬し、模擬パルス電流を印加して誘導電流を発生させたところ、中性子計測設備のケーブルに「中性子束異常高」スクラム信号レベルを超える信号変化が生じることが確認された。 【事象の原因】 1号機原子炉建物避雷針へ落雷があり、中性子計測設備のケーブルに誘導電流が流れ、これが通常レベルの電流信号に重畳したため、「中性子束異常高」の誤信号が発信したものと推定された。		・設備の相違	
対策 （1）アナログ式モニタからデジタル式モニタへ変更。 （2）ケーブルルート見直し 雷サージ電流の進入ルートと考えられる信号ケーブルの電線管ルートを原子炉建屋外壁埋設から原子炉建屋内の露出電線管ルートへの変更を実施した。		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1 1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。		対策 （1）中性子計測設備およびその他の計測設備の点検を実施し、異常のないことを確認した。 （2）念のため、落雷による影響を低減するため、中性子計測設備および中性子計測設備と同様な設備である原子炉建物換気系モニタについては、信号ケーブルを収納している電線管をアルミで内張りしたしゃへい材で包み込むこととした。			

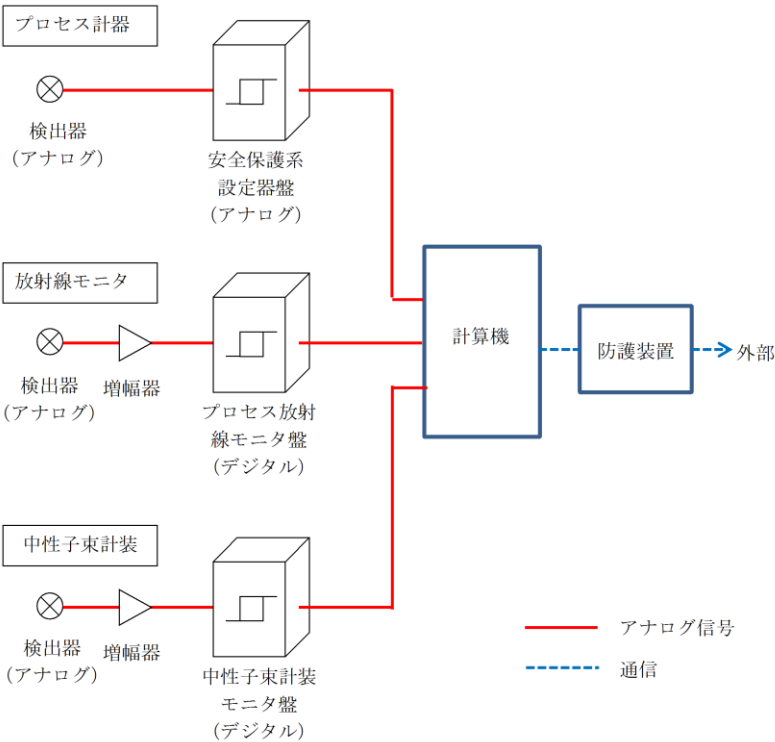
柏崎刈羽原子力発電所 6／7号炉 (2017.12.20版)	東海第二発電所 (2018.9.18版)	島根原子力発電所 2号炉	備考
	別紙7 安全保護回路のうち一部デジタル演算処理を行う機器のソフトウェアの検証及び妥当性確認について 安全保護回路のうち、一部デジタル演算処理を行う機器のソフトウェアは、安全保護上要求される機能が正しく確実に実現されていることを保証するため、設計、製作、試験、変更管理の各段階で「安全保護系へのデジタル計算機の適用に関する規程」(JEAC4620-2008)及び「デジタル安全保護系の検証及び妥当性確認に関する指針」(JEAG4609-2008,以下「JEAG4609」),又はRegulatory Guide 1.152「原子力発電所安全関連システムのプログラマブルデジタル計算機システムソフトウェアの基準」に準じた検証及び妥当性確認を実施する。 東海第二発電所においては<u>起動領域計装</u>,平均出力領域計装,主蒸気管放射能高,<u>原子炉建屋放射能高</u>の演算処理においてソフトウェアを用いている。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。 (1) 平均出力領域計装 <u>平均出力領域計装</u>に用いるソフトウェアはJEAG4609に基づき検証及び妥当性確認を実施している。(第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	別紙8 <u>安全保護回路のうち一部デジタル演算処理を行う機器のソフトウェアの検証及び妥当性確認について</u> <u>安全保護回路のうち、一部デジタル演算処理を行う機器のソフトウェアは、安全保護回路で要求される機能が正しく確実に実現されていることを保証するため、設計、製作、試験、変更管理の各段階で「安全保護系へのデジタル計算機の適用に関する規程」(JEAC4620-2008)及び「デジタル安全保護系の検証及び妥当性確認に関する指針」(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。</u> 島根原子力発電所2号炉においては<u>平均出力領域計装,放射線モニタ(主蒸気管放射線高,原子炉棟排気放射線高,燃料取替階放射線高)</u>の演算処理においてソフトウェアを用いている。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。 (1) <u>平均出力領域計装,放射線モニタ(主蒸気管放射線高,原子炉棟排気放射線高,燃料取替階放射線高)</u> <u>これらに用いるソフトウェアはJEAG4609に準じた検証及び妥当性確認を実施する。(第1図)</u> <u>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。</u> <u>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。</u> <u>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。</u> <u>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</u>	・設備の相違 【柏崎6/7】 島根2号炉は,アナログ型安全保護回路による設備構成であるが,一部デジタル演算処理を行う機器のソフトウェアの検証及び妥当性確認について記載している 【東海第二】 東海第二の設備の一部は,海外製であり,米国の基準に準拠して,検証及び妥当性確認を行っている(以下,⑬の相違) ・設備の相違 【東海第二】 ⑫の相違 ・設備の相違 【東海第二】 ⑫の相違 ・運用の相違 【東海第二】 島根2号炉は,今後導入(工事中含む)するソフトウェアについて,JEAG4609に準じた検証及び妥当性確認を実施することとしている

柏崎刈羽原子力発電所 6／7号炉 (2017.12.20版)	東海第二発電所 (2018.9.18版)	島根原子力発電所 2号炉	備考
	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。 検証1・・・システム設計要求仕様検証 検証2・・・ハードウェア・ソフトウェア設計要求仕様検証 検証3・・・ソフトウェア設計検証 検証4・・・ソフトウェア製作検証 検証5・・・ハードウェア・ソフトウェア統合検証 (注1) □ は、設計・製作作業の範囲を示す。 (注2) □ は、検証・妥当性確認作業の範囲を示す。 第1図 検証及び妥当性確認 (JEAG4609)	ること。 <u>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。</u> <u>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。</u> 検証1・・・システム設計要求仕様検証 検証2・・・ハードウェア・ソフトウェア設計要求仕様検証 検証3・・・ソフトウェア設計検証 検証4・・・ソフトウェア製作検証 検証5・・・ハードウェア・ソフトウェア統合検証 (注1) □ は、設計・製作作業の範囲を示す。 (注2) □ は、検証・妥当性確認作業の範囲を示す。 第1図 検証及び妥当性確認 (JEAG4609)	

柏崎刈羽原子力発電所 6 / 7 号炉 (2017. 12. 20 版)	東海第二発電所 (2018. 9. 18 版)	島根原子力発電所 2 号炉	備考
	<u>(2) 起動領域計装, 主蒸気管放射能高, 原子炉建屋放射能高</u> <u>これらに用いるソフトウェアの検証及び妥当性確認は米国のライセンシング・トピカル・レポートNEDO-31439-A付録E「ハードウェアの品質保証及びソフトウェアの妥当性確認及び検証」に従って実施している。NEDO-31439-A付録Eのソフトウェア検証及び妥当性確認の手法はRegulatory Guide 1.152「原子力発電所安全関連システムのプログラマブルデジタル計算機システムソフトウェアの基準」に準拠しており米国NRCによりエンドースされている。</u> <u>検証は, ソフトウェアの設計, 製作過程を6つの「ベースライン」と呼ばれるフェーズに分け(第1表), 各フェーズを完了し, 次のフェーズに進むために「ベースライン・レビュー」で以下を実施する。</u> <u>・全ての設計のステップが完了し, 検証されていることを確認する。</u> <u>・設計と検証が承認された上位のレベルのベースラインの文書に基づいて行われていることを確認する。</u> <u>・検証の範囲とアプローチが理に適っていること, コメントが文書化されていること, 検証で抽出された問題点が解決されていることを確認する。</u> <u>・レビュー結果を文書化する。次のフェーズで用いる文書の承認状況もこれに含める。</u> <u>本検証手法は, JEAG4609と同様に, ソフトウェア設計の各段階で設計アウトプットが上位設計からの要求事項を満足しているかの観点を主体に, また同様な設計フェーズにおいて検証を行っており(第1表), JEAG4609と同等の検証手法である。</u>		・設備の相違 【東海第二】 ⑬の相違

柏崎刈羽原子力発電所 6／7号炉 (2017. 12. 20 版)	東海第二発電所 (2018. 9. 18 版)	島根原子力発電所 2号炉	備考																
	第1表 NEDO-31439-A付録E「ハードウェアの品質保証及びソフトウェアの妥当性確認及び検証」及びJEAG4609の概要比較 <table><tr><td>NEDO-31439-A 付録 E</td><td>JEAG4609</td></tr><tr><td>【ベースライン1：要求事項と計画の策定】 最上流の要求事項，ソフトウェア管理と V&V の計画を確認する。</td><td>【システム設計要求仕様作成】 システムとしての全体設計を行い，要求仕様を明確に定める。</td></tr><tr><td>【ベースライン1・レビュー】 ベースライン1 が発注者要求事項（基準規格，許認可要求事項等）に基づいていることを確認する。</td><td>【検証1】 JEAC4620 の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。</td></tr><tr><td>【ベースライン2：製品パフォーマンスの決定】 ハードウェア設計，ハードウェア／ソフトウェアの機能の割り当て，通信プロトコル等の基本設計を定める。</td><td>【ハードウェア・ソフトウェア設計要求仕様作成】 ＜ハードウェア・ソフトウェア統合要求仕様＞ ハードウェアとソフトウェアで実現する機能範囲及びそのインターフェイスを図，表などを用いて規定する。 ＜ハードウェア設計要求仕様＞ 全体ハードウェア及び構成されるハードウェア要素（マイクロプロセッサ，電源等）それぞれについての機能・性能を規定する。 ＜ソフトウェア設計要求仕様＞ 入力処理，演算処理，出力処理等のソフトウェア及びこれらを組合せて実現する全体ソフトウェア構成について機能・性能を規定する。</td></tr><tr><td>【ベースライン2・レビュー】 ベースライン2 の設計と検証が上位レベルのベースライン文書に基づいていることを確認する。</td><td>【検証2】 システム設計要求仕様が正しく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。</td></tr><tr><td>【ベースライン3：ハイレベルソフトウェア設計】 アーキテクチャ，ソフトウェアの構造，各モジュールの決定，各モジュールへの機能の割り当て，演算の優先順位等のハイレベル設計を行う。</td><td>【ソフトウェア設計】 ソフトウェア設計要求仕様を実現するためのソフトウェアを設計する。</td></tr><tr><td>【ベースライン3・レビュー】 ベースライン3 の設計と検証が上位レベルのベースライン文書に基づいていることを確認する。</td><td>【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。</td></tr><tr><td>【ベースライン4：詳細設計／コード／モジュール試験】</td><td>【ソフトウェア製作】</td></tr></table>	NEDO-31439-A 付録 E	JEAG4609	【ベースライン1：要求事項と計画の策定】 最上流の要求事項，ソフトウェア管理と V&V の計画を確認する。	【システム設計要求仕様作成】 システムとしての全体設計を行い，要求仕様を明確に定める。	【ベースライン1・レビュー】 ベースライン1 が発注者要求事項（基準規格，許認可要求事項等）に基づいていることを確認する。	【検証1】 JEAC4620 の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。	【ベースライン2：製品パフォーマンスの決定】 ハードウェア設計，ハードウェア／ソフトウェアの機能の割り当て，通信プロトコル等の基本設計を定める。	【ハードウェア・ソフトウェア設計要求仕様作成】 ＜ハードウェア・ソフトウェア統合要求仕様＞ ハードウェアとソフトウェアで実現する機能範囲及びそのインターフェイスを図，表などを用いて規定する。 ＜ハードウェア設計要求仕様＞ 全体ハードウェア及び構成されるハードウェア要素（マイクロプロセッサ，電源等）それぞれについての機能・性能を規定する。 ＜ソフトウェア設計要求仕様＞ 入力処理，演算処理，出力処理等のソフトウェア及びこれらを組合せて実現する全体ソフトウェア構成について機能・性能を規定する。	【ベースライン2・レビュー】 ベースライン2 の設計と検証が上位レベルのベースライン文書に基づいていることを確認する。	【検証2】 システム設計要求仕様が正しく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。	【ベースライン3：ハイレベルソフトウェア設計】 アーキテクチャ，ソフトウェアの構造，各モジュールの決定，各モジュールへの機能の割り当て，演算の優先順位等のハイレベル設計を行う。	【ソフトウェア設計】 ソフトウェア設計要求仕様を実現するためのソフトウェアを設計する。	【ベースライン3・レビュー】 ベースライン3 の設計と検証が上位レベルのベースライン文書に基づいていることを確認する。	【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。	【ベースライン4：詳細設計／コード／モジュール試験】	【ソフトウェア製作】		
NEDO-31439-A 付録 E	JEAG4609																		
【ベースライン1：要求事項と計画の策定】 最上流の要求事項，ソフトウェア管理と V&V の計画を確認する。	【システム設計要求仕様作成】 システムとしての全体設計を行い，要求仕様を明確に定める。																		
【ベースライン1・レビュー】 ベースライン1 が発注者要求事項（基準規格，許認可要求事項等）に基づいていることを確認する。	【検証1】 JEAC4620 の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。																		
【ベースライン2：製品パフォーマンスの決定】 ハードウェア設計，ハードウェア／ソフトウェアの機能の割り当て，通信プロトコル等の基本設計を定める。	【ハードウェア・ソフトウェア設計要求仕様作成】 ＜ハードウェア・ソフトウェア統合要求仕様＞ ハードウェアとソフトウェアで実現する機能範囲及びそのインターフェイスを図，表などを用いて規定する。 ＜ハードウェア設計要求仕様＞ 全体ハードウェア及び構成されるハードウェア要素（マイクロプロセッサ，電源等）それぞれについての機能・性能を規定する。 ＜ソフトウェア設計要求仕様＞ 入力処理，演算処理，出力処理等のソフトウェア及びこれらを組合せて実現する全体ソフトウェア構成について機能・性能を規定する。																		
【ベースライン2・レビュー】 ベースライン2 の設計と検証が上位レベルのベースライン文書に基づいていることを確認する。	【検証2】 システム設計要求仕様が正しく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。																		
【ベースライン3：ハイレベルソフトウェア設計】 アーキテクチャ，ソフトウェアの構造，各モジュールの決定，各モジュールへの機能の割り当て，演算の優先順位等のハイレベル設計を行う。	【ソフトウェア設計】 ソフトウェア設計要求仕様を実現するためのソフトウェアを設計する。																		
【ベースライン3・レビュー】 ベースライン3 の設計と検証が上位レベルのベースライン文書に基づいていることを確認する。	【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。																		
【ベースライン4：詳細設計／コード／モジュール試験】	【ソフトウェア製作】																		

柏崎刈羽原子力発電所 6／7号炉 (2017.12.20版)	東海第二発電所 (2018.9.18版)		島根原子力発電所 2号炉	備考									
	<table><tr><td>ソフトウェア詳細設計，コーディング，モジュールの試験を行う。</td><td>ソフトウェア設計で明らかにされたソフトウェア機能を，デジタル計算機で実現するためのプログラムを作成する。</td></tr><tr><td>【ベースライン4・レビュー】 ベースライン4の設計と検証が上位レベルのベースライン文書に基づいていることを確認する。</td><td>【検証4】 ソフトウェア設計通りに正しくソフトウェアが製作されていることを検証する。</td></tr><tr><td>【ベースライン5：統合試験／最終設計】 ハードウェアとソフトウェアを統合し，試験を行う。</td><td>【ハードウェア・ソフトウェア統合】 ハードウェアにソフトウェアを装荷し，システムとして組みあげる</td></tr><tr><td>【ベースライン5・レビュー】 ベースライン5の設計と検証が上位レベルのベースライン文書に基づいていることを確認する。</td><td>【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通りのシステムとなっていることを検証する。</td></tr><tr><td>【ベースライン6：妥当性確認とファームウェア出荷】 機器の全ての機能についてブラックボックス試験を行い，上位レベルのベースライン文書に基づいていることを確認する。(完了後にファームウェアは製造工程にリリース)</td><td>【妥当性確認】 ソフトウェアとハードウェアを統合して検証されたシステムが，JEAC4620のデジタル安全保護系システム要求事項を満たしていることを確認する。</td></tr></table>	ソフトウェア詳細設計，コーディング，モジュールの試験を行う。	ソフトウェア設計で明らかにされたソフトウェア機能を，デジタル計算機で実現するためのプログラムを作成する。	【ベースライン4・レビュー】 ベースライン4の設計と検証が上位レベルのベースライン文書に基づいていることを確認する。	【検証4】 ソフトウェア設計通りに正しくソフトウェアが製作されていることを検証する。	【ベースライン5：統合試験／最終設計】 ハードウェアとソフトウェアを統合し，試験を行う。	【ハードウェア・ソフトウェア統合】 ハードウェアにソフトウェアを装荷し，システムとして組みあげる	【ベースライン5・レビュー】 ベースライン5の設計と検証が上位レベルのベースライン文書に基づいていることを確認する。	【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通りのシステムとなっていることを検証する。	【ベースライン6：妥当性確認とファームウェア出荷】 機器の全ての機能についてブラックボックス試験を行い，上位レベルのベースライン文書に基づいていることを確認する。(完了後にファームウェアは製造工程にリリース)	【妥当性確認】 ソフトウェアとハードウェアを統合して検証されたシステムが，JEAC4620のデジタル安全保護系システム要求事項を満たしていることを確認する。		
ソフトウェア詳細設計，コーディング，モジュールの試験を行う。	ソフトウェア設計で明らかにされたソフトウェア機能を，デジタル計算機で実現するためのプログラムを作成する。												
【ベースライン4・レビュー】 ベースライン4の設計と検証が上位レベルのベースライン文書に基づいていることを確認する。	【検証4】 ソフトウェア設計通りに正しくソフトウェアが製作されていることを検証する。												
【ベースライン5：統合試験／最終設計】 ハードウェアとソフトウェアを統合し，試験を行う。	【ハードウェア・ソフトウェア統合】 ハードウェアにソフトウェアを装荷し，システムとして組みあげる												
【ベースライン5・レビュー】 ベースライン5の設計と検証が上位レベルのベースライン文書に基づいていることを確認する。	【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通りのシステムとなっていることを検証する。												
【ベースライン6：妥当性確認とファームウェア出荷】 機器の全ての機能についてブラックボックス試験を行い，上位レベルのベースライン文書に基づいていることを確認する。(完了後にファームウェアは製造工程にリリース)	【妥当性確認】 ソフトウェアとハードウェアを統合して検証されたシステムが，JEAC4620のデジタル安全保護系システム要求事項を満たしていることを確認する。												

柏崎刈羽原子力発電所 6／7号炉 (2017.12.20版)	東海第二発電所 (2018.9.18版)	島根原子力発電所 2号炉	備考
	<u>参考1</u> <u>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</u> <u>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。</u> <u>安全保護回路は、検出信号処理において一部デジタル演算処理を行う機器がある他は、アナログ回路で構成している。また安全保護回路とそれ以外の設備との間で用いる信号はアナログ信号（接点信号を含む）であり、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</u><u>る。</u> 		・記載方針の相違 【東海第二】 島根2号炉の安全保護回路については、アナログ型安全保護回路であり、デジタル処理部のある機器は施錠管理されていること及び外部ネットワークとの直接接続はないことから、サイバー攻撃の影響はないと考える

柏崎刈羽原子力発電所 6／7号炉 (2017.12.20版)	東海第二発電所 (2018.9.18版)	島根原子力発電所 2号炉	備考
	<u>参考2</u> <u>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</u> <u>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。</u> <u>東海第二発電所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（24条別紙8-2第1図）により反映不要としている。</u> <u>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」（7.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。</u>		・記載方針の相違 【東海第二】 島根2号炉は、過去のトラブルの反映事項として、柏崎6/7と同様の落雷事象を反映しているため、記載していない

柏崎刈羽原子力発電所 6／7号炉 (2017.12.20版)	東海第二発電所 (2018.9.18版)	島根原子力発電所 2号炉	備考
<u>柏崎刈羽原子力発電所6号及び7号炉</u> 運用，手順説明資料 安全保護回路 別 添	<u>東海第二発電所</u> 運用，手順説明資料 安全保護回路 別 添	<u>島根原子力発電所2号炉</u> 運用，手順説明資料 安全保護回路 別 添	

柏崎刈羽原子力発電所 6／7号炉 (2017. 12. 20 版)	東海第二発電所 (2018. 9. 18 版)	島根原子力発電所 2号炉	備考
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。 安全保護系盤 物理的分離 機能的分離 コンピュータウイルスの混入防止 アクセス制限 不正なアクセスを遮断する措置 出入管理 施錠管理 (保守ツールの施錠管理、保守ツールの接続部の施錠管理) 【第7条 (発電用原子炉施設への人の不法な侵入) にて整理】 検証及び妥当性確認がなされたソフトウェアの使用 固有のプログラム言語を使用 変更管理 (検証及び妥当性確認を含む) 【第7条 (発電用原子炉施設への人の不法な侵入) にて整理】 パスワード管理 (保守ツールのパスワード管理) 工 保 核 工 工 保 核 保 【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。 安全保護盤 物理的分離 機能的分離 コンピュータウイルスの混入防止 アクセス制限 不正なアクセスを遮断する措置 出入管理 施錠管理 (データ収集端末の施錠管理、制御盤の施錠管理) 【第7条 (発電用原子炉施設への人の不法な侵入) にて整理】 固有のプログラム言語を使用 防護装置を介して一方向通信 【第7条 (発電用原子炉施設への人の不法な侵入) にて整理】 施錠管理、パスワード管理 (制御盤及びデータ収集端末保管場所の施錠管理、設定値変更時の鍵管理及びパスワード管理) 工 保 核 工 工 核 工 【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24条 安全保護回路 設置許可基準規則 第24条第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。 安全保護系盤 物理的分離 機能的分離 コンピュータウイルスの混入防止 アクセス制限 不正なアクセスを遮断する装置 出入管理 施錠管理 (制御盤及び保守ツールの施錠管理) 【第7条 (発電用原子炉施設への人の不法な侵入) にて整理】 固有のプログラム及び言語を使用 外部ネットワークと直接接続しない構造 【第7条 (発電用原子炉施設への人の不法な侵入) にて整理】 施錠管理、パスワード管理 (制御盤及び保守ツールの保管場所の施錠管理、保守ツールのパスワード管理) 工 保 核 工 工 核 保 【後段規制との対応】 工：工認（基本方針、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)	・設備および運用の相違 【柏崎 6/7】 島根 2号炉の安全保護回路は一部デジタル演算処理を行う機器がある他は、アナログ回路で構成している 【東海第二】 島根 2号炉は、保守ツールについてパスワード管理を行っている

柏崎刈羽原子力発電所 6／7号炉 (2017.12.20版)	東海第二発電所 (2018.9.18版)	島根原子力発電所 2号炉	備考																																																																														
第1表 運用，手順に係る対策等（設計基準） <table> <tr> <th>設置許可基準 対象条文</th><th>対象項目</th><th>区分</th><th>運用対策等</th></tr> <tr> <td rowspan="12">第24条 安全保護回路</td><td rowspan="4">施錠管理</td><td>運用・手順</td><td>・施錠管理に関する管理方法を定める。</td></tr> <tr> <td>体制</td><td>(運転員，保全員による識別及び施錠管理)</td></tr> <tr> <td>保守・点検</td><td>—</td></tr> <tr> <td>教育・訓練</td><td>—</td></tr> <tr> <td rowspan="4">変更管理</td><td>運用・手順</td><td>・ソフトウェア変更に関する管理方法を定める。 (検証及び妥当性の確認を含む)</td></tr> <tr> <td>体制</td><td>(保全担当による変更管理)</td></tr> <tr> <td>保守・点検</td><td>—</td></tr> <tr> <td>教育・訓練</td><td>—</td></tr> <tr> <td rowspan="4">パスワード 管理</td><td>運用・手順</td><td>・管理（保守ツール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）</td></tr> <tr> <td>体制</td><td>(保全担当によるパスワード管理)</td></tr> <tr> <td>保守・点検</td><td>—</td></tr> <tr> <td>教育・訓練</td><td>—</td></tr> </table>	設置許可基準 対象条文	対象項目	区分	運用対策等	第24条 安全保護回路	施錠管理	運用・手順	・施錠管理に関する管理方法を定める。	体制	(運転員，保全員による識別及び施錠管理)	保守・点検	—	教育・訓練	—	変更管理	運用・手順	・ソフトウェア変更に関する管理方法を定める。 (検証及び妥当性の確認を含む)	体制	(保全担当による変更管理)	保守・点検	—	教育・訓練	—	パスワード 管理	運用・手順	・管理（保守ツール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	(保全担当によるパスワード管理)	保守・点検	—	教育・訓練	—	第 1 表 運用，手順に係る対策等（設計基準） <table> <tr> <th>設置許可基準 対象条文</th><th>対象項目</th><th>区分</th><th>運用対策等</th></tr> <tr> <td rowspan="8">第 24 条 安全保護回路</td><td rowspan="4">施錠管理</td><td>運用・手順</td><td>・施錠管理に関する管理方法を定める。</td></tr> <tr> <td>体制</td><td>(運転員， 保 修 員 による 識別 及び 施 錠 管 理)</td></tr> <tr> <td>保守・点検</td><td>—</td></tr> <tr> <td>教育・訓練</td><td>—</td></tr> <tr> <td rowspan="4">パスワード 管理</td><td>運用・手順</td><td>・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）</td></tr> <tr> <td>体制</td><td>(保 修 員 による パ ス ワ ー ド 管 理)</td></tr> <tr> <td>保守・点検</td><td>—</td></tr> <tr> <td>教育・訓練</td><td>—</td></tr> </table>	設置許可基準 対象条文	対象項目	区分	運用対策等	第 24 条 安全保護回路	施錠管理	運用・手順	・施錠管理に関する管理方法を定める。	体制	(運転員， 保 修 員 による 識別 及び 施 錠 管 理)	保守・点検	—	教育・訓練	—	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	—	運用，手順に係る対策等（設計基準） <table> <tr> <th>設置許可 基準対象 条文</th><th>対象項目</th><th>区分</th><th>運用対策等</th></tr> <tr> <td rowspan="8">第 24 条 安全保護 回路</td><td rowspan="4">施錠管理</td><td>運用・手順</td><td>施錠管理に関する管理方法を定める。</td></tr> <tr> <td>体制</td><td>(運転員， 保 修 員 による 識別 及び 施 錠 管 理)</td></tr> <tr> <td>保守・点検</td><td>—</td></tr> <tr> <td>教育・訓練</td><td>—</td></tr> <tr> <td rowspan="4">パスワード管理</td><td>運用・手順</td><td>管理（盤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）</td></tr> <tr> <td>体制</td><td>(保 修 員 による パ ス ワ ー ド 管 理)</td></tr> <tr> <td>保守・点検</td><td>—</td></tr> <tr> <td>教育・訓練</td><td>—</td></tr> </table>	設置許可 基準対象 条文	対象項目	区分	運用対策等	第 24 条 安全保護 回路	施錠管理	運用・手順	施錠管理に関する管理方法を定める。	体制	(運転員， 保 修 員 による 識別 及び 施 錠 管 理)	保守・点検	—	教育・訓練	—	パスワード管理	運用・手順	管理（盤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	—	・運用の相違 【柏崎 6/7】 島根 2 号炉の安全保護回路は一部デジタル演算処理を行う機器がある他は，アナログ回路で構成している
設置許可基準 対象条文	対象項目	区分	運用対策等																																																																														
第24条 安全保護回路	施錠管理	運用・手順	・施錠管理に関する管理方法を定める。																																																																														
		体制	(運転員，保全員による識別及び施錠管理)																																																																														
		保守・点検	—																																																																														
		教育・訓練	—																																																																														
	変更管理	運用・手順	・ソフトウェア変更に関する管理方法を定める。 (検証及び妥当性の確認を含む)																																																																														
		体制	(保全担当による変更管理)																																																																														
		保守・点検	—																																																																														
		教育・訓練	—																																																																														
	パスワード 管理	運用・手順	・管理（保守ツール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	(保全担当によるパスワード管理)																																																																														
		保守・点検	—																																																																														
		教育・訓練	—																																																																														
設置許可基準 対象条文	対象項目	区分	運用対策等																																																																														
第 24 条 安全保護回路	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	—																																																																														
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（盤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	—																																																																														