東海第二発電所　新規制基準適合への対応状況(安全保護回路(第24条))

第２４条第６号は，不正アクセス行為等による被害を防止できるように安全保護回路を設ける設計とすることを要求しているため、以下の事項について対応状況を示す。

（安全保護回路）
第二十四条　発電用原子炉施設には、次に掲げるところにより、安全保護回路（安全施設に属するものに限る。以下この条において同じ。）を設けなければならない。
一　運転時の異常な過渡変化が発生する場合において、その異常な状態を検知し、及び原子炉停止系統その他系統と併せて機能することにより、燃料要素の許容損傷限界を超えないようにできるものとすること。
二　設計基準事故が発生する場合において、その異常な状態を検知し、原子炉停止系統及び工学的安全施設を自動的に作動させるものとすること。
三　安全保護回路を構成する機械若しくは器具又はチャンネルは、単一故障が起きた場合又は使用状態からの単一の取り外しを行った場合において、安全保護機能を失わないよう、多重性を確保するものとすること。
四　安全保護回路を構成するチャンネルは、それぞれ互いに分離し、それぞれのチャンネル間において安全保護機能を失わないように独立性を確保するものとすること。
五　駆動源の喪失、系統の遮断その他の不利な状況が発生した場合においても、発電用原子炉施設をより安全な状態に移行するか、又は当該状態を維持することにより、発電用原子炉施設の安全上支障がない状態を維持できるものとすること。
六　不正アクセス行為その他の電子計算機に使用目的に沿うべき動作をさせず、又は使用目的に反する動作をさせる行為による被害を防止することができるものとすること。
七　計測制御系統施設の一部を安全保護回路と共用する場合には、その安全保護機能を失わないよう、計測制御系統施設から機能的に分離されたものとすること。

1 第１号について、安全保護回路の運転時の異常な過渡変化時の機能の具体例としては、原子炉の過出力状態や出力の急激な上昇を防止するために、異常な状態を検知し、原子炉停止系統を含む適切な系統を作動させ、緊急停止の動作を開始させること等をいう。
2 第３号に規定する「チャンネル」とは、安全保護動作に必要な単一の信号を発生させるために必要な構成要素（抵抗器、コンデンサ、トランジスタ、スイッチ及び導線等）及びモジュール（内部連絡された構成要素の集合体）の配列であって、検出器から論理回路入口までをいう。
3 第４号に規定する「それぞれ互いに分離し」とは、独立性を有するようなチャンネル間の物理的分離及び電気的分離等をいう。
4 第５号に規定する「駆動源の喪失、系統の遮断その他の不利な状況」とは、電力若しくは計装用空気の喪失又は何らかの原因により安全保護回路の論理回路が遮断される等の状況をいう。なお、不利な状況には、環境条件も含むが、どのような状況を考慮するかは、個々の設計に応じて判断する。
5 第５号に規定する「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」とは、安全保護回路が単一故障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ことにより、最終的に発電用原子炉施設が安全側の状態を維持するか、又は安全保護回路が単一故障してそのままの状態にとどまっても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をいう。
6 第６号に規定する「不正アクセス行為その他の電子計算機に使用目的に沿うべき動作をさせず、又は使用目的に反する動作をさせる行為による被害を防止すること」とは、ハードウェアの物理的分離、機能的分離に加え、システムの導入段階、更新段階又は試験段階でコンピュータウイルスが混入することを防止する等、承認されていない動作や変更を防ぐ設計のことをいう。
7 第７号に規定する「安全保護機能を失わない」とは、接続された計測制御系統施設の機器又はチャンネルに単一故障、誤操作若しくは使用状態からの単一の取り外しが生じた場合においても、これにより悪影響を受けない部分の安全保護回路が第１号から第６号を満たすことをいう。

設置許可基準規則第十六条 適合への対応状況

設置許可基準規則/解釈	基準適合への対応状況	審査資料記載内容
第二十四条　発電用原子炉施設には、次に掲げるところにより、安全保護回路（安全施設に属するものに限る。以下この条において同じ。）を設けなければならない。 一　運転時の異常な過渡変化が発生する場合において、その異常な状態を検知し、及び原子炉停止系統その他系統と併せて機能することにより、燃料要素の許容損傷限界を超えないようにできるものとすること。 （解釈） 1　第１号について、安全保護回路の運転時の異常な過渡変化時の機能の具体例としては、原子炉の過出力状態や出力の急激な上昇を防止するために、異常な状態を検知し、原子炉停止系統を含む適切な系統を作動させ、緊急停止の動作を開始させること等をいう。	第１項第１号について (1)　安全保護系は，運転時の異常な過渡変化時に，中性子束及び原子炉圧力等の変化を検出し，原子炉緊急停止系を含む適切な系統の作動を自動的に開始させ，燃料の許容設計限界を超えることがないように設計する。 (2)　安全保護系は，偶発的な制御棒引抜きのような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，燃料の許容設計限界を超えないよう，中性子束高スクラム及び原子炉出力ペリオド短スクラムにより原子炉を停止できるように設計する。	規制要求変更なし
二　設計基準事故が発生する場合において、その異常な状態を検知し、原子炉停止系統及び工学的安全施設を自動的に作動させるものとすること。	第１項第２号について 安全保護系は，設計基準事故時に異常状態を検知し，原子炉緊急停止系を自動的に作動させる。また自動的に主蒸気隔離弁の閉鎖，非常用炉心冷却系の起動，原子炉建屋ガス処理系の起動を行わせる等の保護機能を有する設計とする。 (1)　発電用原子炉は，下記の条件の場合にスクラムする。 ａ．原子炉圧力高 ｂ．原子炉水位低 ｃ．ドライウェル圧力高 ｄ．原子炉出力ペリオド短（起動領域計装） ｅ．中性子束高（起動及び出力領域計装） ｆ．中性子束指示低（出力領域計装） ｇ．中性子計装動作不能（起動及び出力領域計装） ｈ．スクラム・ディスチャージ・ボリューム水位高 ｉ．主蒸気隔離弁閉 ｊ．主蒸気管放射能高 ｋ．主蒸気止め弁閉	規制要求変更なし

設置許可基準規則/解釈	基準適合への対応状況	審査資料記載内容
	l．蒸気加減弁急速閉（ＥＨＣ油圧低） m．地震加速度大 n．原子炉モード・スイッチ「停止」の位置 o．手　　動 (2)　その他主要な安全保護系（工学的安全施設作動回路）には，次のようなものを設ける。 a．原子炉水位異常低下，主蒸気管放射能高，主蒸気管圧力低，主蒸気管流量大，主蒸気管トンネル温度高，復水器真空度低のいずれかの信号による主蒸気隔離弁の閉鎖 b．ドライウェル圧力高，原子炉水位低，原子炉建屋放射能高のいずれかの信号による常用換気系の閉鎖と原子炉建屋ガス処理系の起動 c．原子炉水位異常低下又はドライウェル圧力高の信号による高圧炉心スプレイ系，低圧炉心スプレイ系及び低圧注水系の起動 d．原子炉水位異常低下及びドライウェル圧力高の同時信号による自動減圧系の作動 e．原子炉水位異常低下又はドライウェル圧力高の信号による非常用ディーゼル発電機の起動 f．原子炉水位低，原子炉水位異常低下，ドライウェル圧力高のいずれかの信号による主蒸気隔離弁以外の隔離弁の閉鎖	
三　安全保護回路を構成する機械若しくは器具又はチャンネルは、単一故障が起きた場合又は使用状態からの単一の取り外しを行った場合において、安全保護機能を失わないよう、多重性を確保するものとすること。 （解釈） 2　第３号に規定する「チャンネル」とは、安全保護動作に必要な単一の信号を発生させるために必要な構成要素（抵抗器、コンデンサ、トランジスタ、スイッチ及び導線等）及びモジュール（内部連絡された構成要素の集合体）の配列であって、検出器から論理回路入口までをいう。	第１項第３号について 安全保護系は，十分に信頼性のある少なくとも2チャンネルの保護回路で構成し，機器又はチャンネルの単一故障が起きた場合，又は使用状態からの単一の取り外しを行った場合においても，安全保護機能を失わないように，多重性を備えた設計とする。 具体例は下記のとおりである。 (1)　原子炉緊急停止系作動回路は，検出器，トリップ接点，論理回路，主トリップ継電器等で構成し，基本的に二重の「1 out of 2」方式とする。 安全保護機能を維持するため，原子炉緊急停止系作動回路は，運転中すべて励磁状態であり，電源の喪失，継電器の断線及び検出器を取外した場合，回路が無励磁状態で，	規制要求変更なし

設置許可基準規則/解釈	基準適合への対応状況	審査資料記載内容
	チャンネル・トリップになるようにする。 したがって，これらの単一故障が起きた場合，又は使用状態からの単一の取外しを行った場合においても，その安全保護機能を維持できる。 核計装系は，安全保護回路として必要な最小チャンネル数よりも一つ以上多いチャンネルを持ち，運転中でもバイパスして保守，調整及び校正できる。 したがって，これが故障の場合，故障チャンネルはバイパスし，残りのチャンネルにより安全保護回路の機能が維持できる。 (2) 第１項第２号の(2)項に示す工学的安全施設を作動させるチャンネル（検出器を含む。）は，多重性をもった構成とする。したがって，これらの単一故障が起きた場合，又は使用状態からの単一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。	
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。 （解釈） ３ 第４号に規定する「それぞれ互いに分離し」とは、独立性を有するようなチャンネル間の物理的分離及び電気的分離等をいう。	第１項第４号について 安全保護系は，通常運転時，補修時，試験時，運転時の異常な過渡変化時及び設計基準事故時において，その安全機能を失わないように，その系統を構成するチャンネル相互が分離され，また計測制御系からも原則として分離し，独立性を持つ設計とする。 具体例は下記のとおりである。 (1) 格納容器を貫通する計装配管は，物理的に独立した貫通部を有する2系列を設ける。 (2) 検出器からのケーブル，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。 (3) 原子炉緊急停止系動作回路の電源は，分離・独立した母線から供給する。	規制要求変更なし
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	第１項第５号について 安全保護系の駆動源として電源あるいは計器用空気を使用する。この系統に使用する弁等は，フェイル・セイフの設計とするか，又は故障と同時に現状維持（フェイル・ア	規制要求変更なし

設置許可基準規則/解釈	基準適合への対応状況	審査資料記載内容
ものとすること。 （解釈） 4　第５号に規定する「駆動源の喪失、系統の遮断その他の不利な状況」とは、電力若しくは計装用空気の喪失又は何らかの原因により安全保護回路の論理回路が遮断される等の状況をいう。なお、不利な状況には、環境条件も含むが、どのような状況を考慮するかは、個々の設計に応じて判断する。 5　第５号に規定する「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」とは、安全保護回路が単一故障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ことにより、最終的に発電用原子炉施設が安全側の状態を維持するか、又は安全保護回路が単一故障してそのままの状態にとどまっても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をいう。	ズ・イズ）になるようにし，この現状維持の場合でも多重化された他の回路によって保護動作を行うことができる設計とする。 　フェイル・セイフとなるものの主要なものをあげると以下のとおりである。 (1)　電源喪失 ａ．スクラム ｂ．主蒸気隔離弁閉 ｃ．格納容器ベント弁閉 (2)　制御用空気喪失 ａ．スクラム ｂ．格納容器ベント弁閉 　また，主蒸気隔離弁以外の工学的安全施設を作動させる安全保護系の場合，駆動源である電源の喪失時には，系統を現状維持とする設計とする。 　系統の遮断やその他，火災，浸水等不利な状況が発生した場合でも，この工学的安全施設作動回路及び工学的安全施設自体が多重性，独立性を持つことで原子炉施設を十分に安全な状態に導くよう設計する。	

設置許可基準規則/解釈	基準適合への対応状況	審査資料記載内容
六　不正アクセス行為その他の電子計算機に使用目的に沿うべき動作をさせず、又は使用目的に反する動作をさせる行為による被害を防止することができるものとすること。 （解釈） 6　第６号に規定する「不正アクセス行為その他の電子計算機に使用目的に沿うべき動作をさせず、又は使用目的に反する動作をさせる行為による被害を防止すること」とは、ハードウェアの物理的分離、機能的分離に加え、システムの導入段階、更新段階又は試験段階でコンピュータウイルスが混入することを防止する等、承認されていない動作や変更を防ぐ設計のことをいう。	第１項第６号について 安全保護系のアナログ回路は，これが収納された盤の施錠等により，ハードウェアを直接接続させない措置を実施することで物理的に分離するとともに，外部ネットワークへのデータ伝送の必要がある場合は，防護装置を介して安全保護回路の信号を一方向（送信機能のみ）通信に制限することで機能的に分離し，外部からの不正アクセスを防止する設計とする。 また，発電所での出入管理による物理的アクセスの制限により不正な変更等による承認されていない動作や変更を防止する設計とする。 【説明資料（2.1：P24条-31,32）（2.2：P24条-32,33）（2.3：P24条-34）（2.4：P24条-35）（2.5：P24条-36）（2.6：P24-36,37）】	安全保護回路の検出器はアナログ機器，論理回路はハードワイヤーロジック（補助継電器や配線等）で構成されており，ソフトウェアを用いないアナログ回路である。 安全保護回路（原子炉緊急停止系，工学的安全施設作動回路）のうちデジタル処理部のある機器については，下記対策を実施している。 (1)　物理的及び電気的アクセスの制限対策 発電所への入域に対しては，出入管理により物理的アクセスを制限し，電気的アクセスについては，安全保護回路を有する制御盤を施錠管理とし，デジタル処理部を持つ機器からデータを採取するデータ収集端末にはデジタル処理を行う演算回路からのデータ受信機能のみを設けるとともに，データ収集端末を施錠管理された場所に保管することで管理されない変更を防止している。 【審査資料（24条-34　別紙1-１　別紙3-1～5　別紙4-1　別紙5-1)】 (2)　ハードウェアの物理的な分離又は機能的な分離対策 安全保護回路の信号は，安全保護回路→プロセス計算機・データ伝送装置→防護装置→緊急時対策支援システム伝送装置→防護装置を介して外部に伝送している。この信号の流れにおいて，安全保護回路からは発信されるのみであり，外部からの信号を受信しないこと，及びハードウェアを直接接続しないことで物理的及び機能的分離を行っている。 【審査資料（24条-35)】 (3)　外部ネットワークからの遠隔操作及びウイルス等の侵入防止対策 安全保護回路の信号で外部ネットワークへのデータ伝送の必要がある場合は，防護装置を介して安全保護回路の信号を一方向（送信機能のみ）通信に制限※し外部からのデータ書き込み機能を設けないことでウイルスの侵入及び外部からの不正アクセスを防止している。 ※データダイオード装置（ハードウェアレベルでダイオードのように片方向のみ通信を許可する装置）により一方向通信に制限する。 【審査資料（24条-35　別紙3-1)】 (4)　システムの導入段階，更新段階または試験段階で承認されていない動作や変更を防ぐ対策 安全保護回路のうちデジタル処理部を持つ機器は，固有のプログラム言語を使用（一般的なコンピュータウイルスが動作しない環境）するとともに，保守以外の不要な演算回路へのアクセス制限対策として入域制限や設定値変更作業での鍵管理及びパスワード管理を行い，関係者以外の不正な変更等を防止している。 【審査資料（24条-34　別紙1-１　別紙3-1,2　別紙4-1　別紙5-1)】

設置許可基準規則/解釈	基準適合への対応状況	審査資料記載内容
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。 （解釈） 7　第７号に規定する「安全保護機能を失わない」とは、接続された計測制御系統施設の機器又はチャンネルに単一故障、誤操作若しくは使用状態からの単一の取り外しが生じた場合においても、これにより悪影響を受けない部分の安全保護回路が第１号から第６号を満たすことをいう。	第１項第７号について 安全保護系と計測制御系とは電源，検出器，ケーブル・ルート及び格納容器を貫通する計装配管を，原則として分離する設計とする。 安全保護系と計測制御系で計装配管を共用する場合は，安全保護系の計装配管として設計する。 また，核計装等の検出部が表示，記録計用検出部と共用しているが，計測制御系の短絡，地絡又は断線によって安全保護系に影響を与えない設計とする。	規制要求変更なし