資料３－１－１

女川原子力発電所２号炉

安全保護回路について

平成２７年６月２日

東北電力株式会社

第二十四条：安全保護回路

〈目　　次〉

＜概　　要＞

1.において，設計基準事故対処設備の設置許可基準規則，技術基準規則の追加要求事項を明確化するとともに，それら要求に対する女川原子力発電所２号炉における適合性を示す。

2．において，設計基準事故対処設備について，追加要求事項に適合するために必要となる機能を達成するための設備または運用等について説明する。

1.　基本方針

1.1　要求事項の整理

誤操作防止について，設置許可基準規則第二十四条及び技術基準規則第三十五条における要求事項を明確化する（表１）。

表１　設置許可基準規則第十条及び技術基準規則第三十八条　要求事項

設置許可基準規則 第二十四条（安全保護回路）	技術基準規則 第三十五条（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。 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。	発電用原子炉施設には，安全保護装置を次に定めるところにより施設しなければならない。 一　運転時の異常な過渡変化が発生する場合又は地震の発生により発電用原子炉の運転に支障が生じる場合において，原子炉停止系統その他系統と併せて機能することにより，燃料要素の許容損傷限界を超えないようにできるものであること。	変更なし
二　設計基準事故が発生する場合において，その異常な状態を検知し，原子炉停止系統及び工学的安全施設を自動的に作動させるものとすること。	－	変更なし
三　安全保護回路を構成する機械若しくは器具又はチャンネルは，単一故障が起きた場合又は使用状態からの単一の取り外しを行った場合において，安全保護機能を失わないよう，多重性を確保するものとすること。	二　系統を構成する機器若しくは器具又はチャンネルは，単一故障が起きた場合又は使用状態からの単一の取り外しを行った場合において，安全保護機能を失わないよう，多重性を確保すること。	変更なし
四　安全保護回路を構成するチャンネルは，それぞれ互いに分離し，それぞれのチャンネル間において安全保護機能を失わないように独立性を確保するものとすること。	三　系統を構成するチャンネルは，それぞれ互いに分離し，それぞれのチャンネル間において安全保護機能を失わないように独立性を確保すること。	変更なし

設置許可基準規則 第二十四条（安全保護回路）	技術基準規則 第三十五条（安全保護装置）	備　考
五　駆動源の喪失，系統の遮断その他の不利な状況が発生した場合においても，発電用原子炉施設をより安全な状態に移行するか，又は当該状態を維持することにより，発電用原子炉施設の安全上支障がない状態を維持できるものとすること。	四　駆動源の喪失，系統の遮断その他の不利な状況が生じた場合においても，発電用原子炉施設をより安全な状態に移行するか，又は当該状態を維持することにより，発電用原子炉施設の安全上支障がない状態を維持できること。	変更なし
六　不正アクセス行為その他の電子計算機に使用目的に沿うべき動作をさせず，又は使用目的に反する動作をさせる行為による被害を防止することができるものとすること。	五　不正アクセス行為その他の電子計算機に使用目的に沿うべき動作をさせず，又は使用目的に反する動作をさせる行為による被害を防止するために必要な措置が講じられているものであること。	追加要求事項
七　計測制御系統施設の一部を安全保護回路と共用する場合には，その安全保護機能を失わないよう，計測制御系統施設から機能的に分離されたものとすること。	六　計測制御系の一部を安全保護装置と共用する場合には，その安全保護機能が失わないよう，計測制御系から機能的に分離されたものであること。	変更なし
－	七　発電用原子炉の運転中に，その能力を確認するための必要な試験ができるものであること。	変更なし
－	八　運転条件に応じて作動設定値を変更できるものであること。	変更なし

1.2　適合のための設計方針

一　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，原子炉停止（原子炉スクラム）系を自動的に作動させ燃料の許容設計限界を超えることがないよう設計する。

なお，安全保護系は，偶発的な制御棒引抜きのような反応度制御系のいかなる単一の誤動作に起因する異常な反応度印加が生じた場合でも，燃料の許容設計限界を超えないよう，中性子束高スクラム及び原子炉周期短スクラムにより原子炉を停止できるように設計とする。

二　安全保護系は，事故時にその異常な状態を検知し，原子炉停止（原子炉スクラム）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，非常用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)　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.　中性子束高（平均出力領域モニタ）
e.　中間領域における原子炉周期短（起動領域モニタ）
f.　中性子束計装動作不能（起動領域及び平均出力領域モニタ）
g.　スクラム排出容器水位高
h.　主蒸気隔離弁閉
i.　主蒸気止め弁閉
j.　蒸気加減弁急速閉
k.　主蒸気管放射能高
l.　地震加速度大
m.　手動
n.　モードスイッチ「停止」

(2)　工学的安全施設を作動させる安全保護系（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.　原子炉水位低，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，主復水器真空度低のいずれかの信号による主蒸気隔離弁閉鎖
b.　ドライウェル圧力高，原子炉水位低，原子炉建屋原子炉棟放射能高のいずれかの信号による常用換気系の閉鎖と非常用ガス処理系の起動
c.　原子炉水位低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.　原子炉水位低及びドライウェル圧力高の信号による自動減圧系の作動
e.　原子炉水位低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ディーゼル発電機及び非常用ディーゼル発電機の起動
f.　原子炉水位低又はドライウェル圧力高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チャンネルの保護系で構成し，機器又はチャンネルの単一故障あるいは使用状態からの単一取り外しを行っても保護機能を果たすよう設計する。

(1)　原子炉保護系は，検出器，トリップ接点，論理回路，スクラムパイロット弁等で構成し，基本的に二重の「1 out of 2」方式とする。

原子炉停止（原子炉スクラム）に関連する回路は，運転中すべて励磁状態にあり，電源の喪失，継電器断線，検出器を取り外した場合，回路が無励磁状態になり，チャンネル・トリップになるので，安全保護機能を失わない。

原子炉核計装は，安全保護系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設計とする。

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系の機能が維持できる。

(2)　工学的安全施設を作動させる検出器は，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，使用状態からの単一の取り外しを行っても他の検出器により，安全保護機能を維持できる。

四　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。

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系統を設ける。

(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。各トリップ系の論理回路は，盤内で独立して設ける。

(3)　原子炉保護系の電源は，分離・独立した母線から供給する。

五　安全保護系の駆動源として電気あるいは空気圧を使用する。この系統に使用する弁等は，フェイル・セイフとするか，又は故障と同時に現状維持（フェイル・アズ・イズ）になるようにし，この現状維持の場合でも，多重化された他の回路によって保護動作を行えるようにする。

フェイル・セイフとなる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

六　安全保護系は，不正アクセス行為その他の使用目的に沿うべき動作をさせず，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。

七　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，及び原子炉核計装の検出部が表示，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。

計装配管は，２系列で独立性があり，更に１系列内で安全保護系と共用している計測制御系の配管は，安全保護系と同等の設計としている。

また，原子炉核計装の検出部が表示，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。

2.　安全保護回路

2.1　安全保護回路の構成

安全保護回路は，原子炉計装あるいは安全保護系のプロセス計装からの信号を受信し，原子炉停止系統を自動的に作動させる信号を発生する原子炉保護系と，非常用炉心冷却系，非常用ディーゼル発電機，高圧炉心スプレイ系ディーゼル発電機，非常用ガス処理系，主蒸気隔離，原子炉格納容器隔離を作動させる信号を発生する工学的安全施設作動回路で構成されている。

これらの安全保護系の回路は，アナログ回路で構成されており，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。（添付資料１）

例として原子炉保護系の構成を図１に示す。

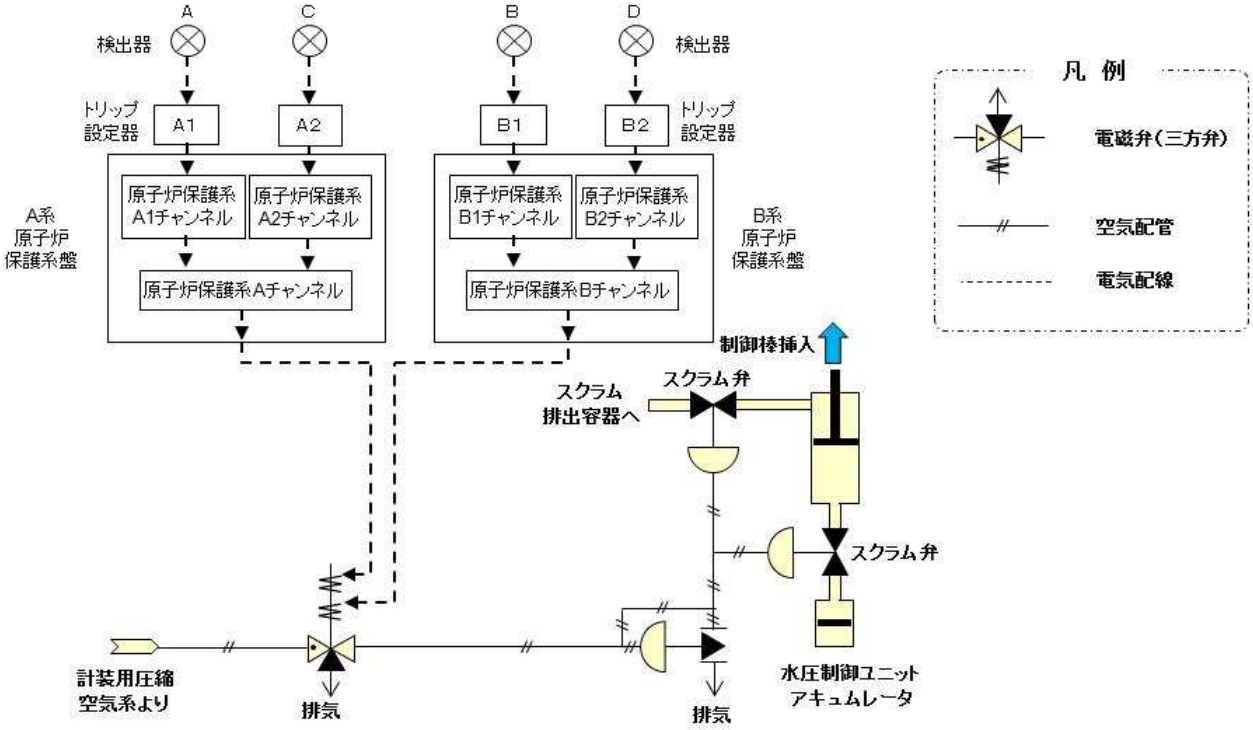

図１　原子炉保護系の構成例

2.2　外部からの不正アクセス行為防止について

安全保護系は，外部ネットワークと直接接続していない。外部システムと接続する必要のある計算機は，外部ネットワークとの間にファイアウォールを介して接続しており，外部からのデータ読み込み機能を設けないことでウィルスの侵入等を防止する設計とする。

また，外部からの人的妨害行為または破壊行為については，出入管理等により侵入等を防止している。

外部ネットワークとの接続構成の概要を図２に示す。

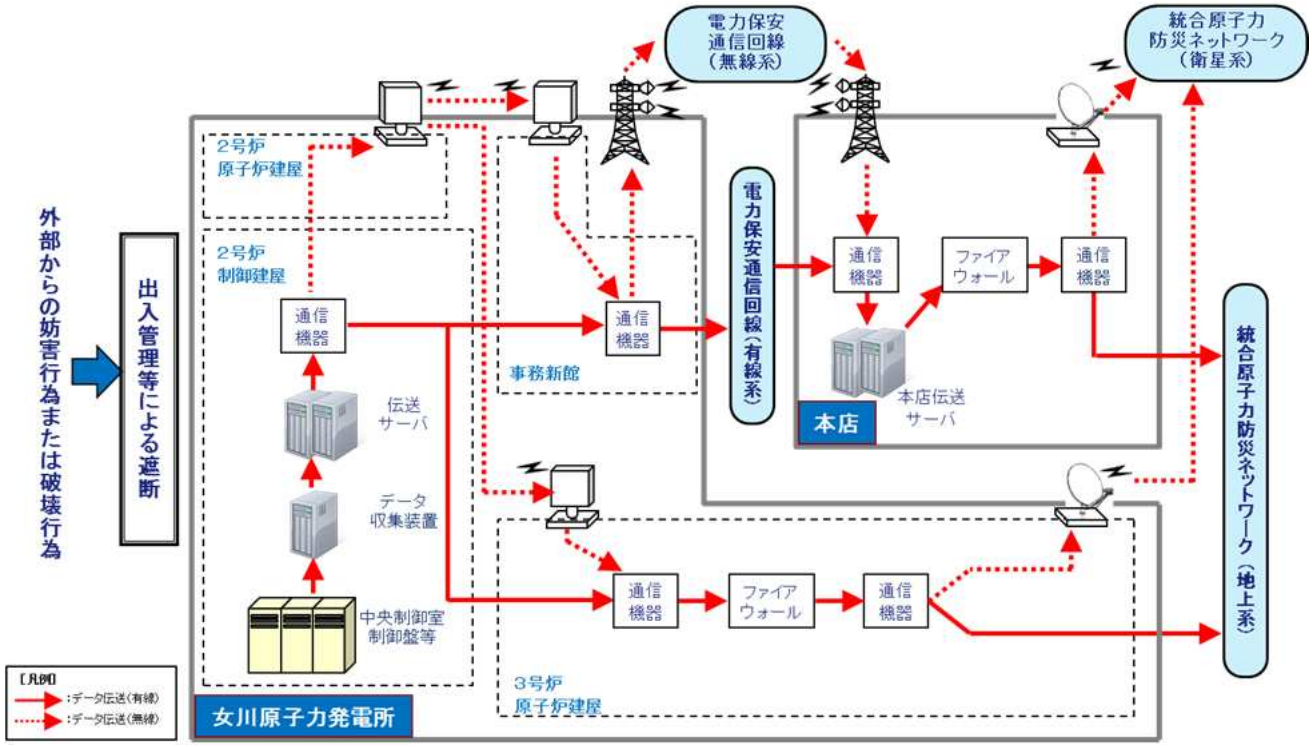

図２　外部ネットワークとの接続構成概要図

添付資料１

安全保護回路の構成について

アナログ型の安全保護回路はリレーや配線等のアナログ回路で構成されている。承認されていない動作や変更を防ぐための対応として，以下を実施している。

安全保護系の構成機器の設置エリアへの入域に対しては，出入管理を行っており，人的妨害行為や破壊行為を防止している。

保守点検時は，作業手順を承認した上で実施しており，点検後は定期事業者検査により安全保護回路が正常に動作することを確認している。

安全保護系の構成機器を表１－１および表１－２に示す。安全保護系の構成機器のうちデジタル処理部のある機器として起動領域モニタ（ＳＲＮＭ），平均出力領域モニタ（ＡＰＲＭ），プロセス放射線モニタ（ＰｒＲＭ）および主蒸気管トンネル温度の監視装置がある。

これら安全保護系への出力回路にデジタル処理部のある機器には，以下の対策を実施している。

・外部ネットワークと接続しない。

・計算機との接続にはアイソレータや補助リレーの離隔装置を用いることで外部との電気的な分離を図っているとともに，信号を計算機が受信するのみの一方向となっている。

・デジタル処理を行っている演算回路は現場で書き換えできない構造となっている。

表１－１　原子炉保護系の構成機器

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	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
中性子束高（平均出力領域モニタ）	アナログ	デジタル
中間領域における原子炉周期短（起動領域モニタ）	アナログ	デジタル
中性子束計装動作不能（起動領域モニタおよび平均出力領域モニタ）	アナログ	デジタル
スクラム排出容器水位高	アナログ	アナログ
	アナログ	
主蒸気隔離弁閉	アナログ	
主蒸気止め弁閉	アナログ	
蒸気加減弁急速閉	アナログ	
主蒸気管放射能高	アナログ	デジタル
地震加速度大	アナログ	
手動	アナログ	
モードスイッチ「停止」	アナログ	

表１－２　工学的安全施設作動系の構成機器

機能	原子炉スクラム信号の種類	検出器	設定器
主蒸気隔離弁閉鎖	原子炉水位低	アナログ	アナログ
	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
	主蒸気管トンネル温度高	アナログ	デジタル
	主復水器真空度低	アナログ	アナログ
非常用ガス処理系の起動	ドライウェル圧力高	アナログ	アナログ
	原子炉水位低	アナログ	アナログ
	原子炉建屋原子炉棟放射能高	アナログ	デジタル
	燃料取替エリア放射能高	アナログ	デジタル
高圧炉心スプレイ系，低圧炉心スプレイ系および低圧注水系の起動	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
自動減圧系の作動	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
高圧炉心スプレイ系ディーゼル発電機および非常用ディーゼル発電機の起動	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

機能	原子炉スクラム信号の種類	検出器	設定器
格納容器隔離弁閉鎖	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

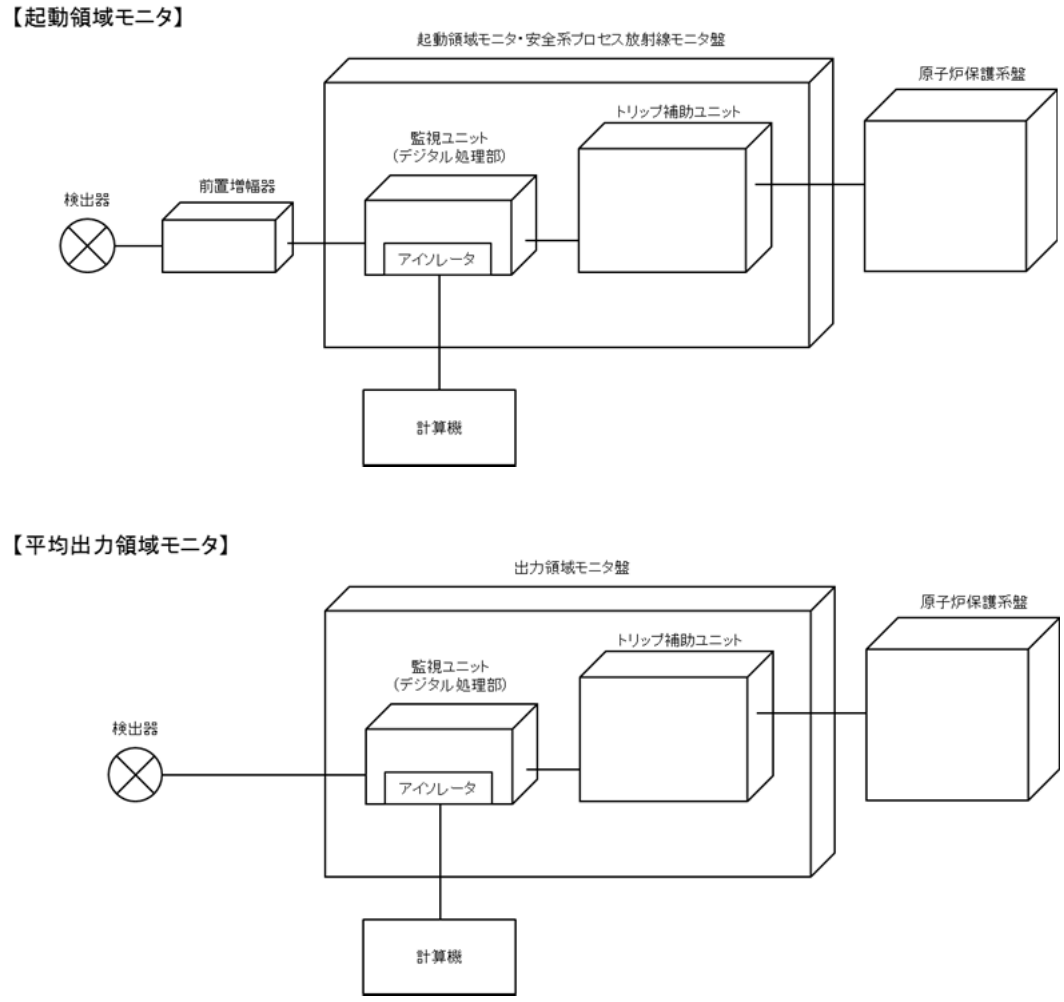

図１－１（１）　安全保護系　構成図

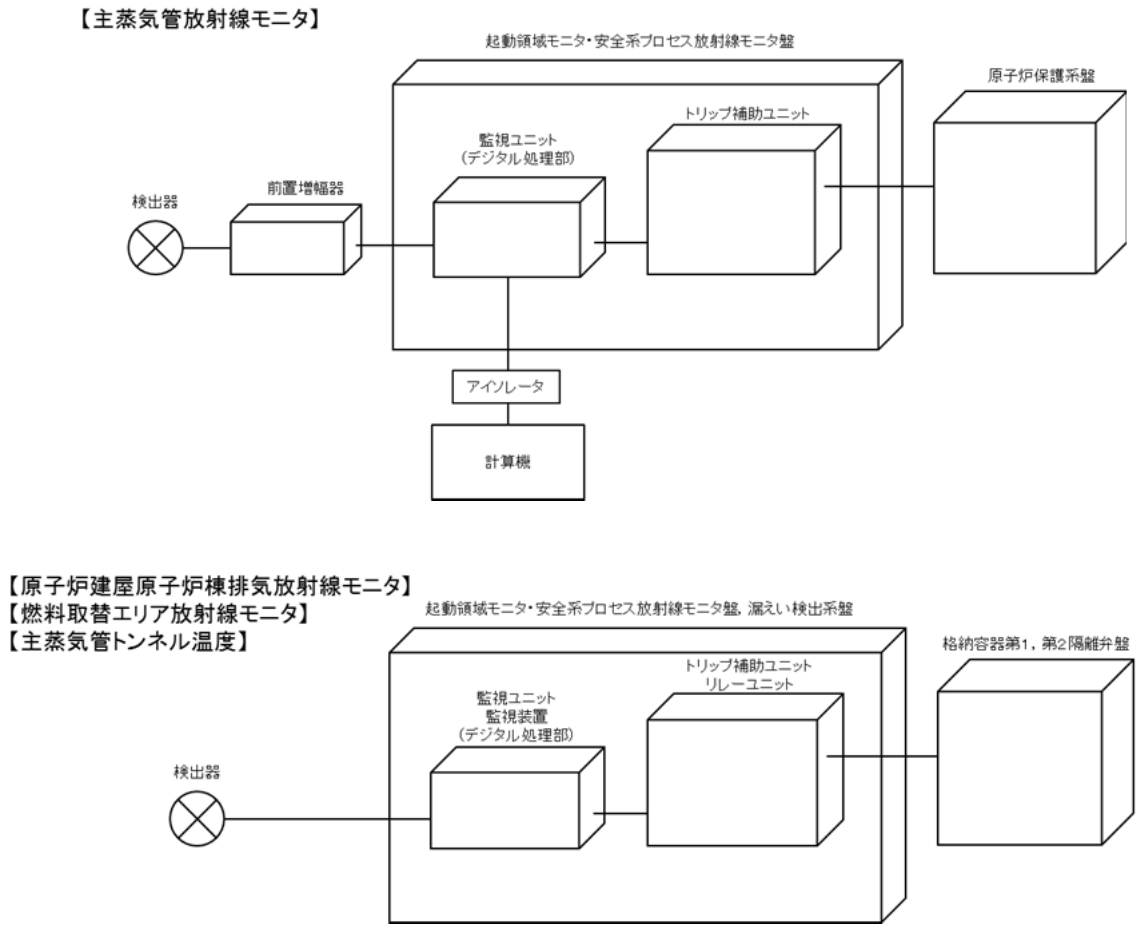

図１－１（２）　安全保護系　構成図

添付資料2

設置許可基準規則第二十四条および技術基準規則第三十五条への適合状況について

「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）

新規制基準の項目	適合状況
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。	（規制要求変更なし） 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，原子炉停止（原子炉スクラム）系を自動的に作動させ燃料の許容設計限界を超えることのない設計としている。 また，偶発的な制御棒引抜きのような反応度制御系のいかなる単一の誤動作に起因する異常な反応度印加が生じた場合でも，燃料の許容設計限界を超えないよう，中性子束高スクラム及び原子炉周期短スクラムにより原子炉を停止できる設計としている。
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こと。	（規制要求変更なし） 安全保護系は，事故時にその異常な状態を検知し，原子炉停止（原子炉スクラム）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，非常用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している。

「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）

新規制基準の項目	適合状況
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。	（規制要求変更なし） 安全保護系は，十分に信頼性のある少なくとも２チャンネルの保護系で構成し，機器又はチャンネルの単一故障あるいは使用状態からの単一取り外しを行っても保護機能を果たす設計としている。
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。	（規制要求変更なし） 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している。
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。	（規制要求変更なし） 安全保護系の駆動源として電気あるいは空気圧を使用する。この系統に使用する弁等は，フェイル・セイフとするか，又は故障と同時に現状維持（フェイル・アズ・イズ）になるようにし，この現状維持の場合でも，多重化された他の回路によって保護動作を行える設計としている。
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。	（新規要求事項） 安全保護系は，外部ネットワークと直接接続をしないこととしているとともに，安全保護系の回路はアナログ回路で構成されており，不正アクセス等による被害を受けることはない。 また，不正アクセス行為（人的行為）により影響を受けないよう出入管理などの対策を行っている。

新規制基準の項目	適合状況
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。	（規制要求変更なし） 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している。

「実用発電用原子炉及びその附属施設の技術基準に関する規則」

第三十五条　（安全保護装置）

新規制基準の項目	適合状況
発電用原子炉施設には，安全保護装置を次に定めるところにより施設しなければならない。 一　運転時の異常な過渡変化が発生する場合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。	（規制要求変更なし） 「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　第１項第一号と同じ
二　系統を構成する機械若しくは器具又はチャンネルは，単一故障がお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。	（規制要求変更なし） 「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　第１項第三号と同じ
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。	（規制要求変更なし） 「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　第１項第四号と同じ
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。	（規制要求変更なし） 「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　第１項第五号と同じ

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

新規制基準の項目	適合状況
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。	（新規要求事項） 「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　第１項第六号と同じ
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。	（規制要求変更なし） 「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　第１項第七号と同じ
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。	（規制要求変更なし） 安全保護系は，原子炉運転中に機能の健全性を確認できる設計としている。
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。	（規制要求変更なし） 安全保護系は，運転条件に応じて作動設定値を変更できる設計としている。

参考資料１

他工事による安全保護回路への影響について

重大事故等の対策として，原子炉停止機能喪失時における低圧注水による原子炉出力の急激な上昇を防止するため，自動減圧系作動阻止回路を設置することとしている。（図１）

自動減圧系作動阻止回路は，既存の自動減圧系の作動を阻止する機能を持つことから，自動減圧系作動阻止回路の誤動作により，自動減圧系の作動を阻害することのないよう，以下のとおり十分に信頼性のある回路構成とすることで，安全保護回路へ悪影響を及ぼさない設計とする。

・多重化された自動減圧系のＡ系，Ｂ系に対応して，それぞれ自動減圧系作動阻止回路を設け，Ａ系とＢ系の分離を図る。

・単一故障による誤動作および誤不動作の防止のため，２／３論理により動作する設計とする。（図２）

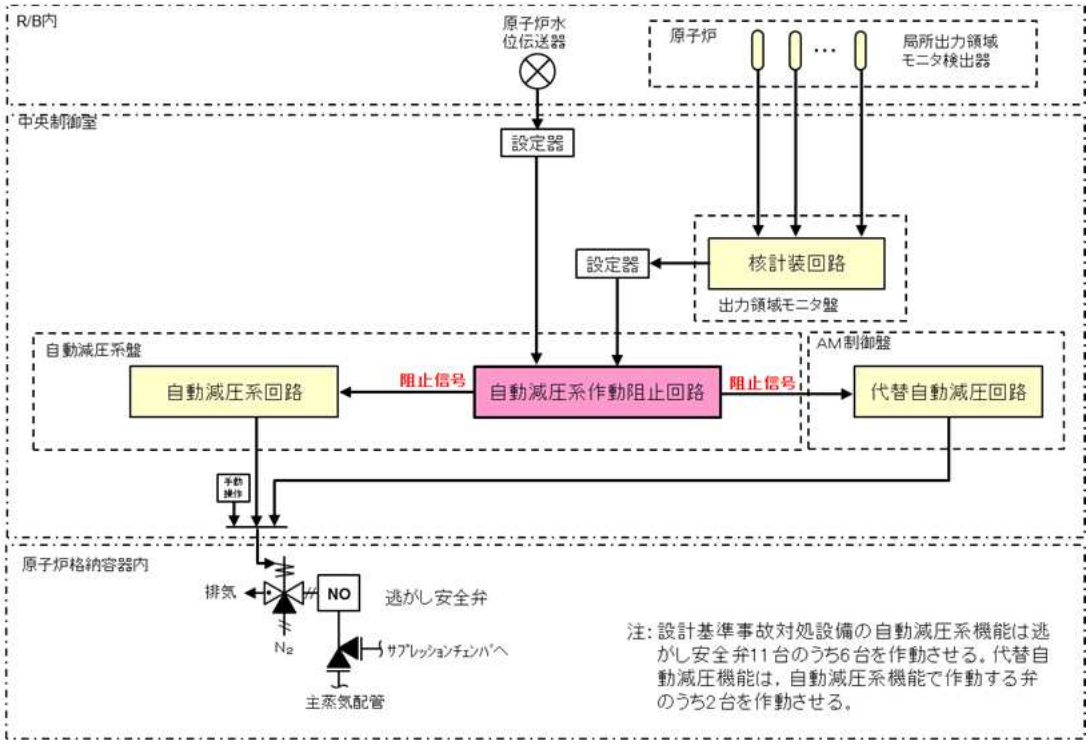

図１　自動減圧系作動阻止機能　概要図

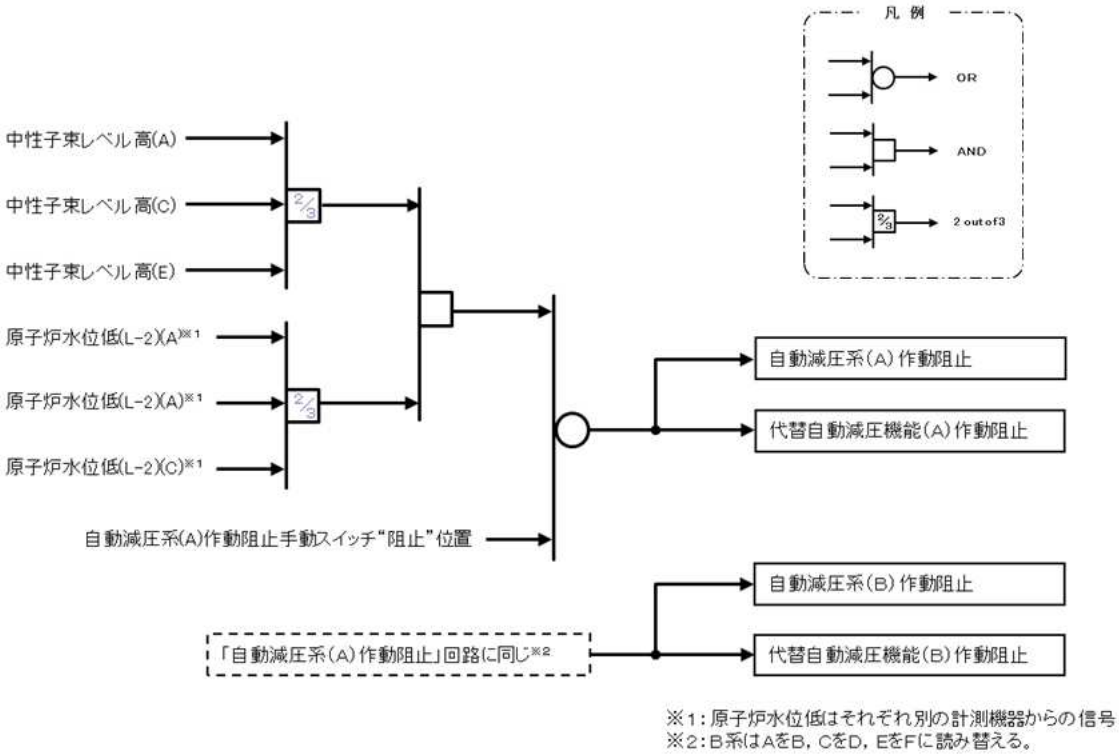

図２　自動減圧系作動阻止機能　論理回路