HTTR 原子炉施設
設置許可基準規則への適合性について
第 18 条（安全保護回路）

令和 2 年 6 月 12 日

日本原子力研究開発機構　大洗研究所
高温ガス炉研究開発センター
高温工学試験研究炉部

第 18 条：安全保護回路

＜目次＞

＜概　要＞

試験研究用等原子炉施設の設置許可基準規則の要求事項を明確化するとともに、それら要求に対するHTTR原子炉施設の適合性を示す。

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 18 条の要求事項を明確化する（表１）。

表１　設置許可基準規則第 11 条　要求事項

設置許可基準規則 第 18 条（安全保護回路）	備考
試験研究用等原子炉施設には、次に掲げるところにより、安全保護回路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、燃料の許容設計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必要な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、多重性又は多様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、試験研究用等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、試験研究用等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。	

1.2　設置許可申請書における記載

1.2.1　位置、構造及び設備

ロ．試験研究用等原子炉施設の一般構造

（３）　その他の主要な構造

（ｉ）原子炉施設は、（１）耐震構造、（２）耐津波構造に加え、次の基本方針のもとに安全設計を行う。

i.（安全保護回路）

安全保護回路は、運転時の異常な過渡変化が発生する場合において、その異常な状態を検知し、及び原子炉停止系統その他系統と併せて機能することにより、燃料の許容設計限界(燃料最高温度　1,600℃)を超えないとともに、設計基準事故が発生する場合において、その異常な状態を検知し、原子炉停止系統及び必要な工学的安全施設を自動的に作動させる設計とする。

安全保護回路を構成する機械若しくは器具又はチャンネルは、単一故障が起きた場合又は使用状態からの単一の取り外しを行った場合において、安全保護機能を失わないよう、多重性又は多様性を確保する設計とする。

安全保護回路を構成するチャンネルは、それぞれ互いに分離し、それぞれのチャンネル間において安全保護機能を失わないように独立性を確保する設計とする。

駆動源の喪失、系統の遮断その他の不利な状況が発生した場合においても、原子炉施設をより安全な状態に移行するか、又は当該状態を維持することにより、原子炉施設の安全上支障がない状態を維持できる設計とする。

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ことができる設計とする。

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設計とする。

ヘ　計測制御系統施設の構造及び設備

(2) 安全保護回路

安全保護回路は、原子炉停止系統を作動させる回路及び工学的安全施設を作動させる回路で構成する。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、及び原子炉停止系統その他系統と併せて機能することにより、燃料の許容設計限界(燃料最高温度 1,600℃)を超えないとともに、設計基準事故が発生する場合において、その異常な状態を検知し、原子炉停止系統及び必要な工学的安全施設を自動的に作動させる設計とする。

安全保護回路を構成する機械若しくは器具又はチャンネルは、単一故障が起きた場合又は使用状態からの単一の取り外しを行った場合において、安全保護機能を失わないよう、多重性又は多様性を確保する設計とする。

安全保護回路を構成するチャンネルは、それぞれ互いに分離し、それぞれのチャンネル間にお

いて安全保護機能を失わないように独立性を確保する設計とする。

駆動源の喪失、系統の遮断その他の不利な状況が発生した場合においても、原子炉施設をより安全な状態に移行するか、又は当該状態を維持することにより、原子炉施設の安全上支障がない状態を維持できる設計とする。

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設計とする。

(ⅰ) 原子炉停止回路の種類

原子炉停止系統を作動させる回路(原子炉保護設備)は、次に示す信号により原子炉をスクラムさせる回路であり、「2 out of 3」方式の論理回路で構成する。また、循環機 3 台停止試験及び炉容器冷却設備停止試験においては、「1 次加圧水冷却器ヘリウム流量低」及び「炉心差圧低」の信号についてあらかじめ定めた試験継続時間後にスクラム信号を発信させる回路を設ける。

広領域中性子束高
出力領域中性子束高
制御棒位置偏差大
中間熱交換器 1 次冷却材流量低
1 次加圧水冷却器ヘリウム流量低
1 次冷却材放射能高
原子炉出口冷却材温度高
中間熱交換器出口 1 次冷却材温度高
1 次加圧水冷却器出口ヘリウム温度高
炉心差圧低
1 次加圧水冷却器加圧水流量低
1 次冷却材・加圧水差圧高
1 次冷却材・加圧水差圧低
1 次・2 次ヘリウム差圧大
2 次ヘリウム流量低
地震加速度大

なお、手動操作で原子炉をスクラムさせることができる。

(ⅱ) その他の主要な安全保護回路の種類

安全保護回路として、次の工学的安全施設を作動させる回路(工学的安全施設作動設備)を設ける。

a. 原子炉格納容器内圧力高、原子炉格納容器内放射能高、1 次冷却材・加圧水差圧低、1 次ヘリウム純化設備流量高、サービスエリア放射能高のいずれかの信号により、原子炉格納容器を隔離し、非常用空気浄化設備を起動する回路

b. スクラム信号により補助冷却設備を起動する回路

c. 1 次冷却材・補助冷却水差圧低信号により、補助冷却器の隔離弁、1 次ヘリウム純化設備の隔離弁を閉鎖する回路

1.3　設置許可申請書の添付書類における記載

1.3.1　安全設計方針

（1）設計方針

1.　安全設計

1.1　安全設計の方針

1.1.6　計測制御系統施設設計の基本方針

(1)　運転、制御及び保護動作に必要な中性子束、温度、圧力等を測定する原子炉計装及びプロセス計装を設けるとともに、通常運転時に起こり得る運転条件の変化及び外乱に対して、自動的に原子炉を制御する原子炉制御設備を設ける。

(2)　通常運転時に異常又は故障が発生した場合は、これを早期に検知し所要の対策が講じられるように中性子束、温度、圧力、放射能等を常時連続的に監視し、異常時には警報を発する装置を設けるとともに、安全上設定した値を超える場合には、炉心及び原子炉冷却材圧力バウンダリの健全性が損なわれることのないよう、異常状態の発生を検知し、原子炉を停止するためのスクラムを行うため、原子炉保護設備を設ける。

　また、誤動作若しくは誤操作による異常又は故障の拡大を防止し設計基準事故に至らないよう制御棒の引抜きを阻止する等のインターロックを設ける。

(3)　原子炉保護設備は、必要な場合に確実に作動するように、多重性及び独立性を有し、単一故障によって、その機能を喪失しないように設計する。万一、駆動源が喪失した場合には、安全側に動作するなどのフェイルセーフ設計とする。また、その機能が喪失していないことを運転中に確認できるように設計する。

(4)　工学的安全施設を作動させる工学的安全施設作動設備を設ける。工学的安全施設作動設備は、必要な場合に確実に作動するように、多重性及び独立性を有し、単一故障によって、その機能を喪失しないように設計する。また、その機能が喪失していないことを運転中に確認できるように設計する。

(5)　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設計する。

1.1.7　工学的安全施設設計の基本方針

　原子炉施設の設計基準事故時に、大量の燃料の破損や原子炉施設外への放射性物質の放散を防止若しくは抑制して、原子炉施設周辺の一般公衆の安全を確保するために、補助冷却設備、炉容器冷却設備、原子炉格納施設及び非常用空気浄化設備からなる工学的安全施設を設け、次の方針に基づいて設計する。

(1)　工学的安全施設の作動が必要な際に、設計どおりの機能を発揮できるよう信頼性の高い設計とし、想定される単一故障に対しても対処できるよう十分な多重性及び独立性を有するようにする。

(2)　工学的安全施設が原子炉施設の寿命を通じて、必要な際にその機能を発揮できることを確認するため、施設の設置時及び運転開始後も原子炉運転中あるいは停止時に、その機能確認の試験及び検査が行えるようにする。

(3)　工学的安全施設には、必要な際に機能が発揮できるように、電源やその他の駆動源を常に確

保する。

（２）適合性

（安全保護回路）

第十八条　試験研究用等原子炉施設には、次に掲げるところにより、安全保護回路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、燃料の許容設計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必要な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、多重性又は多様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、試験研究用等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、試験研究用等原子炉施設の安全上支障がない状態を維持できるものとすること。

六　不正アクセス行為その他の電子計算機に使用目的に沿うべき動作をさせず、又は使用目的に反する動作をさせる行為による被害を防止することができるものとすること。

七　計測制御系統施設の一部を安全保護回路と共用する場合には、その安全保護機能を失わないよう、計測制御系統施設から機能的に分離されたものとすること。

適合のための設計方針

一　安全保護系は、予想される各種の運転時の異常な過渡変化に対処し得る複数の原子炉スクラム信号及び工学的安全施設作動信号を設け、運転時の異常な過渡変化時に、原子炉スクラム設定値を超えた場合には、その異常を自動的に、かつ、速やかにこれを検出し、原子炉停止系統を作動させて炉心を臨界未満にするとともに、補助冷却設備を作動させて原子炉停止後の炉心の核分裂生成物の崩壊熱及びその他の残留熱を除去することにより、燃料の許容設計限界を超えないよう設計する。

二　安全保護系は、設計基準事故時に異常な状態を検知し、原子炉スクラム設定値を超えた場合には、これを検出し、原子炉停止系統及び必要な工学的安全施設の作動を自動的に開始させる安全保護機能を有する設計とする。

三　安全保護系は、使用状態からの単一の取外しを行っても、あるいは異常状態時において、チャンネル又はトレインの単一故障を想定しても安全保護機能を失うことがないよう、チャンネル及びトレインを次のように多重化する。

(1) チャンネルは偽の信号発生等による誤動作を防止することも考慮して「2 out of 3」構成とする。

(2) トレインは「1 out of 2」構成とする。

四　安全保護系を構成するチャンネルに対しては、各チャンネル相互を分離し、独立性を図る設計とする。具体的には、次のとおりである。

(1) 計装用配管は、原子炉格納容器貫通部を含めてチャンネルごとに分離、独立した設計とする。

(2) 各チャンネルに専用のケーブルトレイ、計器ラック等を設けるとともに、安全保護系の論理回路はトレインごとに独立した設計とする。

(3) 各チャンネルの電源は、無停電電源よりそれぞれ独立に供給する設計とする。

五　安全保護系の双安定回路、原子炉スクラムしゃ断器等は、駆動源の喪失、系のしゃ断に対して、原子炉をスクラムさせる方向に作動するように設計する。

その他の安全保護回路は、駆動源の喪失、系のしゃ断に対して安全保護動作が作動するか又はそのまま現在の状態を維持する。この現状維持の場合でも多重化された他の回路が保護動作を行い、安全上支障がない設計とする。

六　安全保護系回路は、インターロック回路を含めリレーやスイッチング素子等の電気部品を用いた制御機器で構成されており、ソフトウェアを用いた装置を使用していないこと、原子炉建家及び中央制御室の出入管理並びに盤の施錠管理により物理的アクセスを制限していることから、外部ネットワークからの侵入防止等のサイバーセキュリティを考慮する必要はない。

七　安全保護系は、安全保護機能を失うような影響を受けないように、安全保護系以外の計測制御系から分離した設計とする。安全保護系の一部から、安全保護系以外の計測制御系の信号を取出す場合には、信号の分岐箇所に絶縁増幅器を使用し、出力側(安全保護系以外の計測制御系)で回路の短絡、開放等の故障が生じても入力側(安全保護系)へ影響を与えない設計とする。

1.3.2　気象等

該当無し

1.3.3　設備等

9.5　原子炉保護設備

9.5.1　概　要

安全保護系である原子炉保護設備は、安全保護系へ信号を送る原子炉計装及び安全保護系のプロセス計装から信号により、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を保護するため、制御棒を挿入し、原子炉を自動停止させる設備である。

原子炉保護設備は、安全保護系へ信号を送る原子炉計装及び安全保護系のプロセス計装から信号を受信し、原子炉スクラム信号及びインターロック回路動作信号を発生する 2 トレインの論理回路と原子炉スクラム信号により自動的に開く原子炉スクラムしゃ断器とで構成する。

原子炉保護設備への電源は、無停電電源からそれぞれ独立に給電し、配線、盤等は、不燃性又は難燃性材料を使用する。

9.5.2　設計方針

原子炉保護設備は、通常運転時、異常状態時、保修時及び試験時において、その安全保護機能が喪失しないように、次の方針により設計する。

(1)　単一故障が起こっても、あるいは使用状態からの単一の取外しを行っても、安全保護機能を喪失しないように多重性を有するようにする。

(2)　トレインは相互に分離し、トレイン間の独立性を考慮するようにする。

(3)　電源の喪失又は系のしゃ断に対して、安全保護機能を喪失しないようにする。

(4)　原子炉保護設備の信号を警報装置等へ取出して使用する場合には、警報装置等の故障が安全保護系の機能を損なわないようにする。

(5)　原子炉の運転中に定期的に試験を行い、機能が喪失していないことを確認できるようにする。

(6)　自動的に作動し、また、必要な場合には手動でも作動できるようにする。

(7)　作動状況が確認できるようにする。

(8)　配線、盤等は、不燃性又は難燃性材料を使用するようにする。ただし、不燃性又は難燃性の材料が使用できない場合は、金属製の盤への格納等により、火災の延焼を防止するための措置を講ずる。

(9)　電源は、無停電電源から給電するようにする。

9.5.3　主要設備

9.5.3.1　原子炉スクラムしゃ断器

原子炉保護設備は、第9.5.1図に示したような回路で構成する。原子炉スクラム信号を発するロジックトレインは、並列に2系統設け、それぞれが直列2台の制御棒駆動装置の電磁クラッチの励磁電源をしゃ断する装置(原子炉スクラムしゃ断器)に接続する。各ロジックトレインは、独立に原子炉スクラム信号を発生することができる。

原子炉のスクラムは、2系統のロジックトレインのいずれか1系統の原子炉スクラム信号を受け、原子炉スクラムしゃ断器を開にして、電磁クラッチを切離し、制御棒を挿入することにより行われる。

原子炉のスクラムは、まず可動反射体領域へ制御棒を挿入し、次いで炉心が所定の温度以下に下がるのを待って(原子炉出口冷却材温度が約750℃以下)、あるいは所定の時間間隔をおいて、燃料領域へ制御棒を挿入する。ただし、1次冷却材・加圧水差圧低の信号及び原子炉格納容器内圧力高の信号により減圧事故を検知した場合には、全制御棒を同時に挿入するようにする。

9.5.3.2　原子炉スクラム信号

原子炉スクラム信号としては、次のものがあり、これらはいずれも「2 out of 3」信号で原子炉をスクラムさせる。原子炉スクラム信号のうち、原子炉の運転を継続するためにブロックする必要のあるものは、パーミッシブ信号によりブロックする。また、特殊運転

時におけるスクラム設定値の変更及びスクラム遅延については、原子炉制御設備である運転モード選択装置から行う。

原子炉保護設備の信号を警報装置等へ取出して使用する場合には、絶縁増幅器により絶縁し、警報装置等で生じた故障が原子炉保護設備へ影響を与えることがないようにする。

原子炉スクラム信号を第9.5.1表及び第9.5.2図に、原子炉スクラム信号の主な測定点を第9.5.3図に示す。また、パーミッシブ信号を第9.5.2表に示す。

(1) 広領域中性子束高

広領域中性子束高は、原子炉起動時及び停止時の中性子束の異常な上昇に対し、原子炉をスクラムする。

このスクラム信号は、出力領域中性子束がパーミッシブーB(P-B：以下同様に記す。)の設定値以上になると手動でブロックでき、P-B の設定値以下になると自動的にブロックが解除される。

(2) 出力領域中性子束高(高設定、低設定)

出力領域中性子束高には、高設定と低設定がある。原子炉の出力運転時の中性子束の異常な上昇に対し、通常の出力運転状態では、定格出力以上に設定した高設定により、起動時等の低出力運転状態では、定格出力以下の低設定により原子炉をスクラムする。

低設定は、出力領域中性子束が、P-B の設定値以上になると手動でブロックでき、P-B の設定値以下になると自動的にブロックが解除される。

(3) 制御棒位置偏差大

制御棒位置偏差大は、制御棒の相対位置に異常な偏差が生じた場合に、原子炉をスクラムする。

このスクラム信号は、出力領域中性子束が P-C の設定値以上になると自動的にブロックが解除され、P-C の設定値以下になると手動でブロックできる。

(4) 中間熱交換器1次冷却材流量低

中間熱交換器1次冷却材流量低は、並列運転時における中間熱交換器1次冷却材流量の異常な低下に対して、原子炉をスクラムする。

このスクラム信号は、広領域中性子束が P-A の設定値以上になると自動的にブロックが解除され、P-A の設定値以下になると手動でブロックできる。

(5) 1次加圧水冷却器ヘリウム流量低

1 次加圧水冷却器ヘリウム流量低は、1 次加圧水冷却器の 1 次冷却材流量の異常な低下に対して、原子炉をスクラムする。

このスクラム信号は、広領域中性子束が P-A の設定値以上になると自動的にブロックが解除され、P-A の設定値以下になると手動でブロックできる。

(6) 1次冷却材放射能高

1 次冷却材放射能高は、燃料破損等による 1 次冷却材中の循環放射能の異常な上昇に対して、原子炉をスクラムする。

(7) 中間熱交換器出口1次冷却材温度高

中間熱交換器出口1次冷却材温度高は、並列運転時における2次ヘリウム冷却設備の除熱能力の低下、又は中間熱交換器1次冷却材流量の増大による中間熱交換器出口1次冷却

材温度の異常な上昇に対して、原子炉をスクラムする。

(8) 1次加圧水冷却器出口ヘリウム温度高

1 次加圧水冷却器出口ヘリウム温度高は、1 次加圧水冷却器出口ヘリウム温度の異常な上昇に対して、原子炉をスクラムする。

(9) 原子炉出口冷却材温度高

原子炉出口冷却材温度高は、原子炉出口冷却材温度の異常な上昇に対して、原子炉をスクラムする。

(10) 炉心差圧低

炉心差圧低は、1 次冷却設備の二重管の内管破損等による炉心有効流量の低下を炉心差圧で検知し、原子炉をスクラムする。

このスクラム信号の設定値は、原子炉出力に対応し、可変設定する。

また、このスクラム信号は、広領域中性子束が P-A の設定値以上になると自動的にブロックが解除され、P-A の設定値以下になると手動でブロックできる。

(11) 1次加圧水冷却器加圧水流量低

1 次加圧水冷却器加圧水流量低は、1 次加圧水冷却器の加圧水流量の異常な低下に対して、原子炉をスクラムする。

このスクラム信号は、広領域中性子束が P-A の設定値以上になると自動的にブロックが解除され、P-A の設定値以下になると手動でブロックできる。

(12) 1次冷却材・加圧水差圧高

1次冷却材・加圧水差圧高は、1次冷却材と加圧水の差圧が異常に大きくなった場合に、原子炉をスクラムする。

このスクラム信号は、広領域中性子束が P-A の設定値以上になると自動的にブロックが解除され、P-A の設定値以下になると手動でブロックできる。

(13) 1次冷却材・加圧水差圧低

1次冷却材・加圧水差圧低は、1次冷却材と加圧水の差圧が異常に小さくなった場合に、原子炉をスクラムする。

このスクラム信号は、広領域中性子束が P-A の設定値以上になると自動的にブロックが解除され、P-A の設定値以下になると手動でブロックできる。

(14) 1次・2次ヘリウム差圧大

1 次・2 次ヘリウム差圧大は、並列運転時における 1 次冷却材と 2 次ヘリウムの差圧が異常に大きくなった場合に、原子炉をスクラムする。

このスクラム信号は、広領域中性子束が P-A の設定値以上になると自動的にブロックが解除され、P-A の設定値以下になると手動でブロックできる。

(15) 2次ヘリウム流量低

2 次ヘリウム流量低は、並列運転時における 2 次冷却材(ヘリウム)流量の異常な低下に対して、原子炉をスクラムする。

このスクラム信号は、広領域中性子束が P-A の設定値以上になると自動的にブロックが解除され、P-A の設定値以下になると手動でブロックできる。

(16) 地震加速度大(水平方向加速度、垂直方向加速度)

地震加速度大は、水平方向加速度大と垂直方向加速度大があり、一定の大きさ以上の地震が発生した時に、原子炉をスクラムする。

(17) 手　動

必要な場合、中央制御室の原子炉スクラムスイッチ2個のうち、いずれか1個の操作により、原子炉をスクラムすることができる。

9.5.3.3 原子炉スクラム時のインターロック

(1) 原子炉スクラム信号により補助冷却設備起動信号が発せられ、1 次冷却設備等の機器を停止させるとともに、補助冷却設備を起動し、残留熱除去を行う。

減圧事故及び補助冷却器伝熱管破損事故の場合、補助冷却設備起動信号は、1 次冷却材・補助冷却水差圧低信号により自動的に阻止され、炉容器冷却設備による残留熱除去を行う。

(2) 原子炉スクラム信号発生後、制御棒駆動装置の電動機の電源をしゃ断する。

9.5.4 評　価

(1) 単一故障

原子炉保護設備を構成する論理回路には多重性をもたせて保護動作を行う。即ち、「2 out of 3」の論理回路は、配線も含めて 2 トレイン構成としている。これらのトレインは、電気的、物理的に分離しているので、単一のトレインの故障で原子炉保護設備の機能を失うことはない。

(2) 独立性

原子炉保護設備は、相互干渉が起こらないよう火災防護上の配慮を行い、不燃性又は難燃性材料を使用するようにしている。不燃性又は難燃性の材料が使用できない場合は、金属製の盤への格納等により、火災の延焼を防止するための措置を講ずることとしている。

論理回路、配線等はトレインごとに独立したラックに収納するようにしている。

また、電源は無停電電源から独立に給電しており、短時間の商用電源喪失に対しても原子炉保護設備の機能を喪失することのない設計としている。

(3) フェイルセーフ

原子炉保護設備は、電源の喪失又は系のしゃ断に対して、原子炉保護設備の機能を喪失することのない設計としている。

(4) 分離性

原子炉保護設備の信号を警報装置等へ取出して使用する場合には、絶縁増幅器により絶縁して、警報装置等の故障が原子炉保護設備の機能を損なわないようにしている。

(5) 運転中試験

原子炉保護設備は、原子炉運転中に論理回路及び原子炉スクラムしゃ断器に関して試験することができる。論理回路は、テストスイッチを操作して、安全保護系のプロセス計装の各チャンネルの双安定回路の信号により、正常に動作することを確認できる。

原子炉スクラムしゃ断器は、原子炉スクラムバイパスしゃ断器を投入して、それぞれ原子炉スクラムしゃ断器ごとに試験することができる。

(6) 手動操作

原子炉の安全を確保するため、原子炉の急速な停止が必要な場合に、手動でも原子炉保護動

作を行えるように、中央制御室に原子炉スクラムスイッチを2個設けており、いずれか1個のスイッチ操作により原子炉をスクラムすることができる。

(7) 作動状況の確認

原子炉保護設備の作動状況は、中央制御室の警報、表示によって確認することができる。

9.6 工学的安全施設作動設備

9.6.1 概 要

安全保護系である工学的安全施設作動設備は、1次冷却設備の二重管破断事故あるいは2次冷却材喪失事故等に際して、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を保護し、原子炉施設外への多量の放射性物質の放散を抑制又は防止するための設備を作動するものである。

工学的安全施設作動設備は、安全保護系へ信号を送る原子炉計装及び安全保護系のプロセス計装から信号を受けて、工学的安全施設を作動させる2トレインの論理回路で構成する。

工学的安全施設作動設備への電源は、無停電電源からそれぞれ独立に給電し、配線、盤等は不燃性又は難燃性材料を使用する。

9.6.2 設計方針

工学的安全施設作動設備は、次の方針により設計する。

(1) 単一故障が起こっても、あるいは使用状態からの単一の取外しを行っても、安全保護機能を喪失しないように多重化を有するようにする。

(2) トレインは相互に分離し、トレイン間の独立性を考慮するようにする。

(3) 電源の喪失又は系のしゃ断に対して、安全保護機能を喪失しないようにする。

(4) 工学的安全施設作動設備の信号を警報装置等へ取出して使用する場合には、警報装置等の故障が安全保護系の機能を損なわないようにする。

(5) 原子炉の運転中に定期的に試験を行い、機能が喪失していないことを確認できるようにする。

(6) 自動的に作動し、また、必要な場合には手動でも作動できるようにする。

(7) 作動状況が確認できるようにする。

(8) 配線、盤等は、不燃性又は難燃性材料を使用するようにする。ただし、不燃性又は難燃性の材料が使用できない場合は、金属製の盤への格納等により、火災の延焼を防止するための措置を講ずる。

(9) 電源は、無停電電源から給電するようにする。

9.6.3 主要設備

工学的安全施設作動信号としては次のものがあり、これらをまとめて第9.6.1表及び第9.6.1図に、また、工学的安全施設作動信号の主な測定点を第9.5.3図に示す。

工学的安全施設作動信号を警報装置等へ取出して使用する場合には、絶縁増幅器により絶縁し、警報装置等で生じた故障が工学的安全施設作動設備に影響を与えることがないようにする。

(1) 原子炉格納容器隔離信号

原子炉格納容器隔離信号は、1 次冷却設備の二重管破断事故等による放射性物質の環境への放出を防止するため、下記の信号の「2 out of 3」信号により、原子炉格納容器の隔離弁を閉止するとともに、原子炉建家Ⅰ系換気空調装置の給気系統及び排気 A 系統を停止し、非常用空気浄化設備を起動する。

原子炉格納容器内圧力高
原子炉格納容器内放射能高
1 次冷却材・加圧水差圧低
1 次ヘリウム純化設備流量高
サービスエリア放射能高

ただし、1 次冷却材・加圧水差圧低の信号は、広領域中性子束が P-A の設定値以上になると自動的にブロックが解除され、P-A の設定値以下になると手動でブロックできる。

また、中央制御室の操作スイッチ 2 個のうち 1 個を手動で操作すれば、原子炉格納容器隔離信号を発することができる。

原子炉格納容器隔離信号発生時の隔離弁の開閉状態を第 9.6.2 図に示す。

(2) 補助冷却設備起動信号

補助冷却設備起動信号は、原子炉スクラム時に残留熱除去を行うため、原子炉スクラム信号により、補助ヘリウム循環機の起動及び補助冷却水系の流量を待機運転の流量から定格流量にする。ただし、補助冷却設備起動信号は、減圧事故及び補助冷却器の伝熱管破損事故時には、1 次冷却材・補助冷却水差圧低信号により阻止する。原子炉運転中の原子炉スクラムしゃ断器の試験時には、原子炉スクラムバイパスしゃ断器が閉で補助冷却設備起動信号を阻止する。

また、中央制御室の各々2 個からなる 2 組の操作スイッチのうち、1 組の操作スイッチを同時に操作すれば、補助冷却設備起動信号を発することができる。

(3) 補助冷却水系隔離信号

補助冷却水系隔離信号は、補助冷却器伝熱管破断時に補助冷却水の 1 次冷却材中への侵入を防止するため、1 次冷却材・補助冷却水差圧低の信号の「2 out of 3」信号により、補助ヘリウム循環機及び補助冷却水循環ポンプの停止並びに補助冷却水系の原子炉格納容器の隔離弁及び 1 次ヘリウム純化設備に接続する原子炉冷却材圧力バウンダリの隔離弁を閉止する。ただし、1 次冷却材・補助冷却水差圧低の信号は、広領域中性子束が P-A の設定値以上になると自動的にブロックが解除され、P-A の設定値以下になると手動でブロックできる。

また、中央制御室の各々2 個からなる 2 組の操作スイッチのうち、1 組の操作スイッチを同時に操作すれば、補助冷却水系隔離信号を発することができる。

9.6.4 評　価

(1) 単一故障

工学的安全施設作動設備を構成する論理回路には、多重性をもたせて保護動作を行う。即ち、「2 out of 3」等の論理回路は、配線をも含めて 2 トレイン構成としている。これらのトレインは、電気的、物理的に分離しているので、単一のトレインの故障で機能を失うことはない。

(2) 独立性

工学的安全施設作動設備は、相互干渉が起こらないように火災防護上の配慮を行い、不燃性又は難燃性材料を使用している。ただし、不燃性又は難燃性の材料が使用できない場合は、金属製の盤への格納等により、火災の延焼を防止するための措置を講ずることとしている。論理回路、配線等はトレインごとに独立したラックに収納するようにしている。

また、電源は無停電電源から独立に給電しており、短時間の商用電源喪失に対しても機能を喪失することのない設計としている。

(3) フェイルセーフ

工学的安全施設作動設備の構成は、電源の喪失又は系のしゃ断に対して、安全保護機能を喪失しない設計としている。

(4) 分離性

工学的安全施設作動設備の信号を警報装置等へ取出して使用する場合には、絶縁増幅器により絶縁して、警報装置等の故障が工学的安全施設作動設備の機能を損なわないようにしている。

(5) 運転中試験

工学的安全施設作動設備は、原子炉運転中にテストスイッチを用いて、安全保護系のプロセス計装の各チャンネルの双安定回路の信号により、論理回路が正常に動作することを確認できる。

(6) 手動操作

原子炉施設の安全を確保するため、工学的安全施設の急速な作動が必要な場合に、手動でも工学的安全施設を作動することができるように、中央制御室に手動スイッチを設け、次の作動信号をそれぞれ発することができる。

a. 原子炉格納容器隔離信号
b. 補助冷却設備起動信号
c. 補助冷却水系隔離信号

(7) 作動状況の確認

工学的安全施設の作動状況は、中央制御室の警報、表示によって確認することができる。

２．HTTR 原子炉施設　安全保護回路

（適合性説明資料）

HTTR原子炉施設

第18条　安全保護回路

（第六号　安全保護回路に対する不正アクセス行為の防止）

目次

1. 要求事項(1／2)

要求事項

(安全保護回路)

第十八条　試験研究用等原子炉施設には、次に掲げるところにより、安全保護回路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、燃料の許容設計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必要な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、多重性又は多様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、試験研究用等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、試験研究用等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. 要求事項(2／2)

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、試験研究用等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求めている。

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3号に規定する「多様性を確保する」とは、同一事象に対する安全保護動作が、異なるパラメータからの信号により機能することを含む。

4　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。

5　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。

6　第5号に規定する「試験研究用等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、試験研究用等原子炉施設の安全上支障がない状態を維持できる」とは、安全保護回路が単一故障した場合においても、試験研究用等原子炉施設をより安全な状態に移行することにより、最終的に試験研究用等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を起こしてそのままの状態にとどまった場合においても試験研究用等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。

7　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ィ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ことをいう。

8　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、誤動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。

2. 要求事項に対する対応(1/4)

基本的な考え方

安全保護回路のための措置(第18条第1号関係)

(従来の設計方針と同様)

安全保護系は、予想される各種の運転時の異常な過渡変化に対処し得る複数の原子炉スクラム信号及び工学的安全施設作動信号を設け、運転時の異常な過渡変化時に、原子炉スクラム設定値を超えた場合には、その異常を自動的に、かつ、速やかにこれを検出し、原子炉停止系統を作動させて炉心を臨界未満にするとともに、補助冷却設備を作動させて原子炉停止後の炉心の核分裂生成物の崩壊熱及びその他の残留熱を除去することにより、燃料の許容設計限界を超えないよう設計している。
(詳細は参考資料1を参照)

安全保護回路のための措置(第18条第2号関係)

(従来の設計方針と同様)

安全保護系は、設計基準事故時に異常な状態を検知し、原子炉スクラム設定値を超えた場合には、これを検出し、原子炉停止系統及び必要な工学的安全施設の作動を自動的に開始させる安全保護機能を有する設計としている。
(詳細は参考資料1を参照)

2. 要求事項に対する対応(2/4)

安全保護回路のための措置(第18条第3号関係)

(従来の設計方針と同様)

安全保護系は、使用状態からの単一の取外しを行っても、あるいは異常状態時において、チャンネル又はトレインの単一故障を想定しても安全保護機能を失うことがないよう、チャンネル及びトレインを次のように多重化している。
(1) チャンネルは偽の信号発生等による誤動作を防止することも考慮して「2 out of 3」構成としている。
(2) トレインは「1 out of 2」構成としている。
(詳細は参考資料2を参照)

安全保護回路のための措置(第18条第4号関係)

(従来の設計方針と同様)

安全保護系を構成するチャンネルに対しては、各チャンネル相互を物理的及び電気的に分離し、独立性を図る設計としている。具体的には、次のとおりである。
(1) 計装用配管は、原子炉格納容器貫通部を含めてチャンネルごとに分離、独立した設計としている。
(2) 各チャンネルに専用のケーブルトレイ、計器ラック等を設けるとともに、安全保護系の論理回路はトレインごとに独立した設計としている。
(3) 各チャンネルの電源は、無停電電源によりそれぞれ独立に供給する設計としている。
(詳細は参考資料2を参照)

2. 要求事項に対する対応(3/4)

安全保護回路のための措置(第18条第5号関係)

(従来の設計方針と同様)

安全保護系の双安定回路、原子炉スクラムしゃ断器等は、駆動源の喪失、系のしゃ断に対して、原子炉をスクラムさせる方向に作動するように設計している。

その他の安全保護回路は、駆動源の喪失、系のしゃ断に対して安全保護動作が作動するか又はそのまま現在の状態を維持する。この現状維持の場合でも多重化された他の回路が保護動作を行い、安全上支障がないような設計としている。

(詳細は参考資料2を参照)

安全保護回路のための措置(第18条第6号関係)

HTTRの安全保護回路は、リレーやスイッチング素子等の電気部品を用いた制御機器で構成されており、電子計算機やソフトウェアを用いた装置を使用していない。

したがって、HTTRの安全保護回路は、電子計算機を使用した装置で懸念される外部ネットワークからの侵入やコンピュータウィルスの混入による誤動作を考慮する必要はない。

(詳細は参考資料2を参照)

2. 要求事項に対する対応(4/4)

安全保護回路のための措置(第18条第7号関係)

(従来の設計方針と同様)

安全保護系は、安全保護機能を失うような影響を受けないように、安全保護系以外の計測制御系から分離した設計としている。安全保護系の一部から、安全保護系以外の計測制御系の信号を取出す場合には、信号の分岐箇所に絶縁増幅器を使用し、出力側(安全保護系以外の計測制御系)で回路の短絡、開放等の故障が生じても入力側(安全保護系)へ影響を与えない設計としている。

(詳細は参考資料3を参照)

3. 設置許可基準への適合状況(1/4)

新規制基準の条文	適合状況
(安全保護回路) 第十八条　試験研究用等原子炉施設には、次に掲げるところにより、安全保護回路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、燃料の許容設計限界を超えないようにできるものとすること。 【解釈】 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、試験研究用等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求めている。 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必要な工学的安全施設を自動的に作動させるものとすること。	一について 安全保護系は、予想される各種の運転時の異常な過渡変化に対処し得る複数の原子炉スクラム信号及び工学的安全施設作動信号を設け、運転時の異常な過渡変化時に、原子炉スクラム設定値を超えた場合には、その異常を自動的に、かつ、速やかにこれを検出し、原子炉停止系統を作動させて炉心を臨界未満にするとともに、補助冷却設備を作動させて原子炉停止後の炉心の核分裂生成物の崩壊熱及びその他の残留熱を除去することにより、燃料の許容設計限界を超えないよう設計としている。 二について 安全保護系は、設計基準事故時に異常な状態を検知し、原子炉スクラム設定値を超えた場合には、これを検出し、原子炉停止系統及び必要な工学的安全施設の作動を自動的に開始させる安全保護機能を有する設計としている。

3. 設置許可基準への適合状況(2/4)

新規制基準の条文	適合状況
三　安全保護回路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、多重性又は多様性を確保するものとすること。 【解釈】 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3号に規定する「多様性を確保する」とは、同一事象に対する安全保護動作が、異なるパラメータからの信号により機能することを含む。 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】 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。	三について 安全保護系は、使用状態からの取り外しを行っても、あるいは異常状態時において、チャンネル又はトレインの単一故障を想定しても安全保護機能を失うことがないよう、チャンネル及びトレインを次のように多重化している。 (1) チャンネルは偽の信号発生等による誤動作を防止することも考慮して「2 out of 3」構成としている。 (2) トレインは「1 out of 2」構成としている。 四について 安全保護系を構成するチャンネルに対しては、各チャンネル相互を物理的及び電気的に分離し、独立性を図る設計としている。具体的には、次のとおりである。 (1) 計装用配管は、原子炉格納容器貫通部を含めてチャンネルごとに分離、独立した設計としている。 (2) 各チャンネルに専用のケーブルトレイ、計器ラック等を設けるとともに、安全保護系の論理回路はトレインごとに独立した設計としている。 (3) 各チャンネルの電源は、無停電電源によりそれぞれ独立に供給する設計としている。

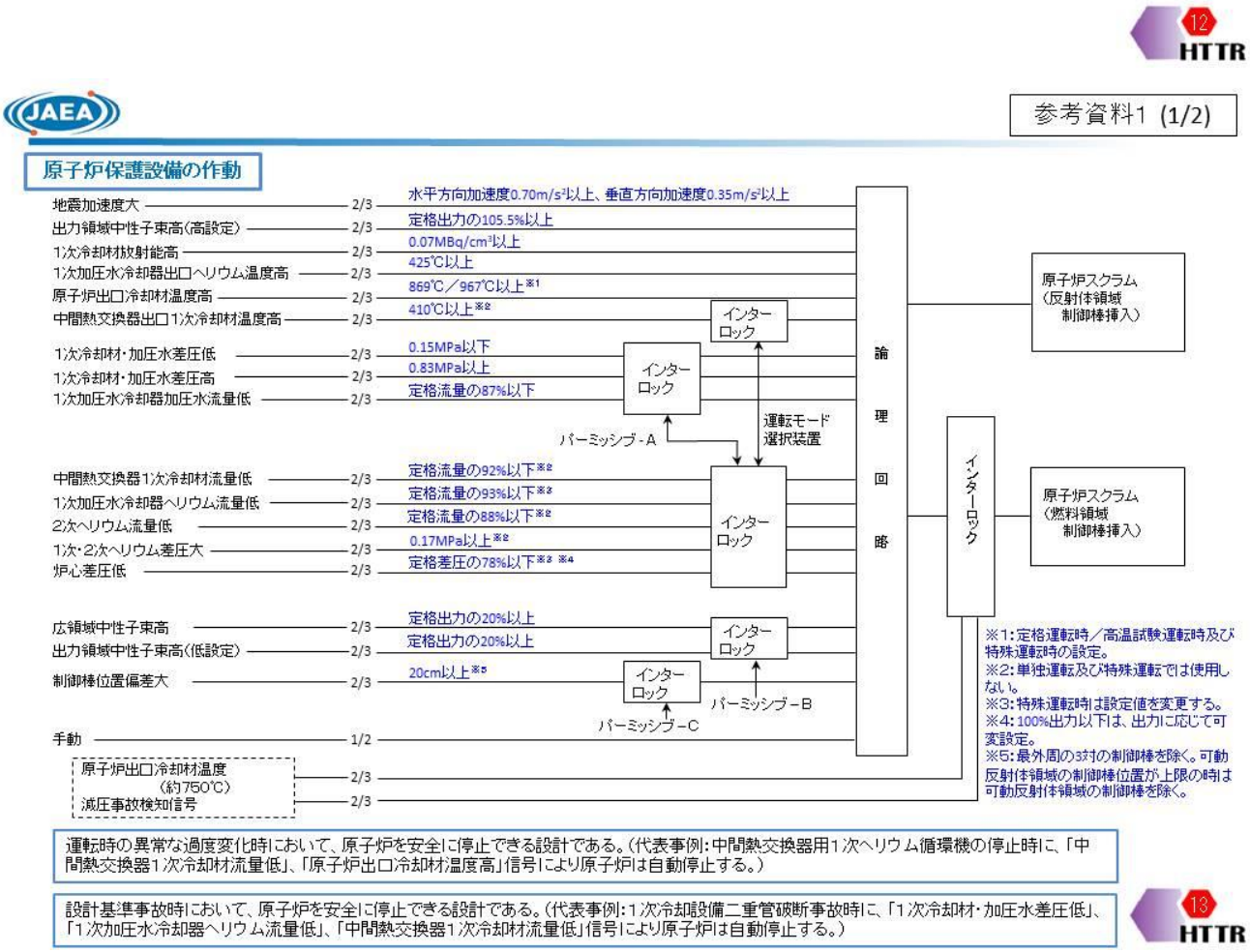
3. 設置許可基準への適合状況(3/4)

新規制基準の条文	適合状況
五　駆動源の喪失、系統の遮断その他の不利の状況が発生した場合においても、試験研究用等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、試験研究用等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。 【解釈】 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。 第5号に規定する「試験研究用等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、試験研究用等原子炉施設の安全上支障がない状態を維持できる」とは、安全保護回路が単一故障した場合においても、試験研究用等原子炉施設をより安全な状態に移行することにより、最終的に試験研究用等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を起こしてそのままの状態にとどまった場合においても試験研究用等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。	五について 安全保護系の双安定回路、原子炉スクラムしゃ断器等は、駆動源の喪失、系のしゃ断に対して、原子炉をスクラムさせる方向に作動するように設計している。 その他の安全保護回路は、駆動源の喪失、系のしゃ断に対して安全保護動作が作動するか又はそのまま現在の状態を維持する。この現状維持の場合でも多重化された他の回路が保護動作を行い、安全上支障がないような設計としている。
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。 【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ィ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ことをいう。	六について 安全保護回路は、リレーやスイッチング素子等の電気部品を用いた制御機器で構成されており、ソフトウェアを用いた装置を使用していないことから、外部ネットワークからの侵入防止等のサイバーセキュリティを考慮する必要はない。

3. 設置許可基準への適合状況(4/4)

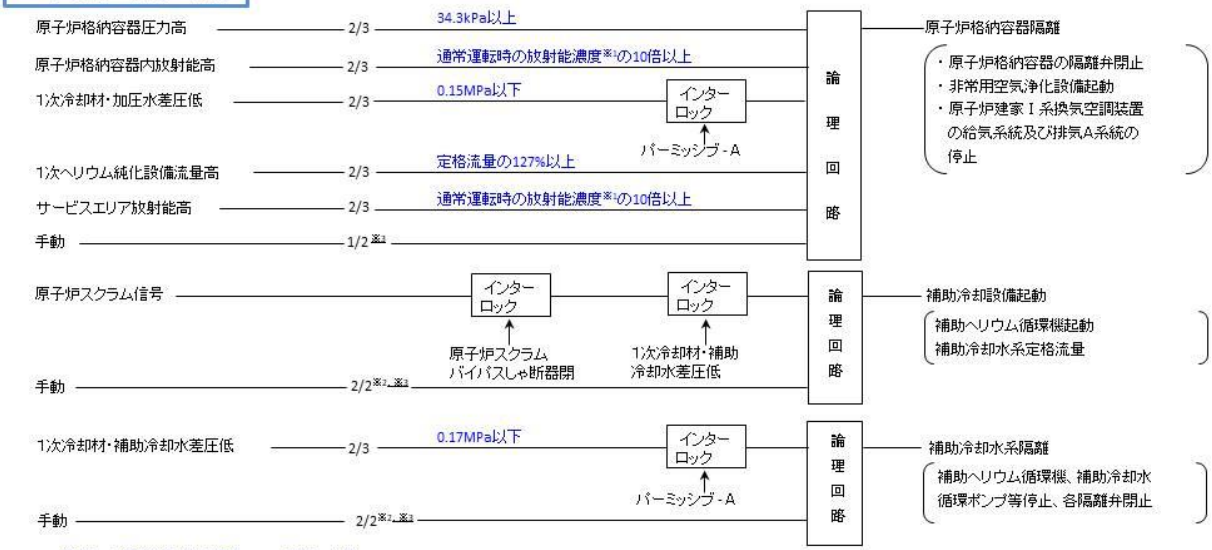
新規制基準の条文	適合状況
七　計測制御系統施設の一部を安全保護回路と共用する場合には、その安全保護機能を失わないよう、計測制御系統施設から機能的に分離されたものとすること。 【解釈】 第7号に規定する「安全保護機能を失わない」とは、接続された計測制御系統施設の機器又はチャンネルに単一故障、誤動作若しくは使用状態からの単一の取り外しが生じた場合においても、これにより悪影響を受けない部分の安全保護回路が第1号から第6号を満たすことをいう。	七について 安全保護系は、安全保護機能を失うような影響を受けないように、安全保護系以外の計測制御系から分離した設計としている。安全保護系の一部から、安全保護系以外の計測制御系の信号を取出す場合には、信号の分岐箇所に絶縁増幅器を使用し、出力側(安全保護系以外の計測制御系)で回路の短絡、開放等の故障が生じても入力側(安全保護系)へ影響を与えない設計としている。

参考資料


12
HTTR
参考資料1 (1/2)
原子炉保護設備の作動
地震加速度大 2/3 水平方向加速度0.70m/s²以上、垂直方向加速度0.35m/s²以上
出力領域中性子束高(高設定) 2/3 定格出力の105.5%以上
1次冷却材放射能高 2/3 0.07MBq/cm³以上
1次加圧水冷却器出口ヘリウム温度高 2/3 425℃以上
原子炉出口冷却材温度高 2/3 869℃／967℃以上※1
中間熱交換器出口1次冷却材温度高 2/3 410℃以上※2
インターロック
1次冷却材・加圧水差圧低 2/3 0.15MPa以下
1次冷却材・加圧水差圧高 2/3 0.83MPa以上
1次加圧水冷却器加圧水流量低 2/3 定格流量の87%以下
インターロック
パーミッシブ-A
運転モード選択装置
中間熱交換器1次冷却材流量低 2/3 定格流量の92%以下※2
1次加圧水冷却器ヘリウム流量低 2/3 定格流量の93%以下※2
2次ヘリウム流量低 2/3 定格流量の88%以下※2
1次・2次ヘリウム差圧大 2/3 0.17MPa以上※2
炉心差圧低 2/3 定格差圧の78%以下※3 ※4
インターロック
広領域中性子束高 2/3 定格出力の20%以上
出力領域中性子束高(低設定) 2/3 定格出力の20%以上
インターロック
制御棒位置偏差大 2/3 20cm以上※5
インターロック
パーミッシブ-B
パーミッシブ-C
手動 1/2
原子炉出口冷却材温度(約750℃)減圧事故検知信号 2/3
2/3
論理回路
インターロック
原子炉スクラム(反射体領域制御棒挿入)
原子炉スクラム(燃料領域制御棒挿入)
※1:定格運転時／高温試験運転時及び特殊運転時の設定。
※2:単独運転及び特殊運転では使用しない。
※3:特殊運転時は設定値を変更する。
※4:100%出力以下は、出力に応じて可変設定。
※5:最外周の3対の制御棒を除く。可動反射体領域の制御棒位置が上限の時は可動反射体領域の制御棒を除く。
運転時の異常な過度変化時において、原子炉を安全に停止できる設計である。(代表事例:中間熱交換器用1次ヘリウム循環機の停止時に、「中間熱交換器1次冷却材流量低」、「原子炉出口冷却材温度高」信号により原子炉は自動停止する。)
設計基準事故時において、原子炉を安全に停止できる設計である。(代表事例:1次冷却設備二重管破断事故時に、「1次冷却材・加圧水差圧低」、「1次加圧水冷却器ヘリウム流量低」、「中間熱交換器1次冷却材流量低」信号により原子炉は自動停止する。)
13
HTTR

参考資料1 (2/2)

工学的安全施設の作動



※1: 燃料の初期(製造時)破損率0.2%に換算した値。

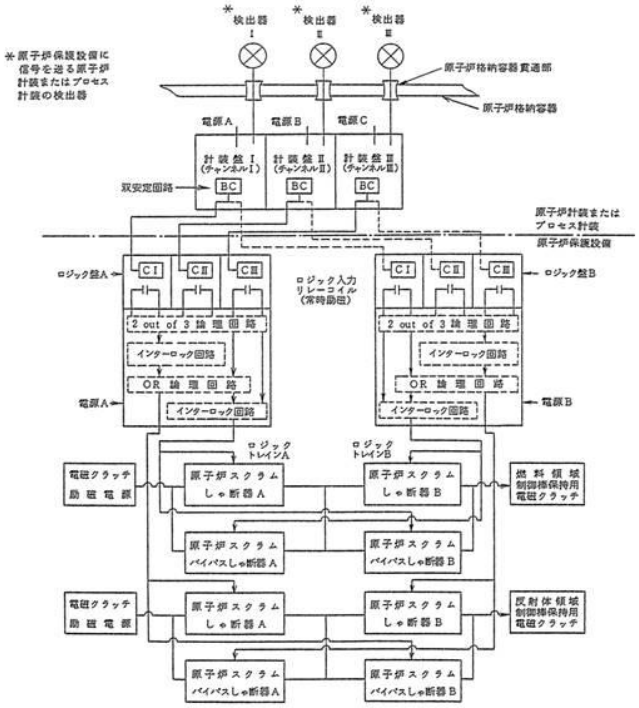
※2: 2個で1組からなる2組(A系、B系)の操作スイッチのうち、いずれか1組(A系またはB系)のスイッチ操作による。

※3: 手動による原子炉格納容器の隔離は、動作しないことが非安全側であることから2個のスイッチのうち1個を操作すれば動作する設計である。また、手動による補助冷却設備の起動、手動による補助冷却水系の隔離は誤操作により動作することを回避するため、各々の2個のスイッチの両方を操作しなければ動作しない設計である。但し、補助冷却設備手動起動、補助冷却水系手動隔離のスイッチは動作させたいときに動作しないという故障を避けるために2組設けている。

運転時の異常な過度変化時において、原子炉を自動停止するとともに、補助冷却設備を自動的に作動させる設計である。

設計基準事故時において、安全保護回路から異常なパラメータを検知し、工学的安全施設を自動的に作動させる設計である。(代表事例:1次冷却設備二重管破断事故時に、「原子炉格納容器内圧力高」、「原子炉格納容器内放射能高」の工学的安全施設作動信号により、原子炉格納容器隔離弁、非常用空気浄化設備等の工学的安全施設を自動的に作動させる。)

参考資料2



安全保護系の多重性・独立性

・チャンネルは「2 out of 3」構成としている。
・トレインは「1 out of 2」構成としている。
・各チャンネルは物理的及び電気的に分離した設計としている。

故障時の機能

・双安定回路、原子炉スクラムしゃ断器等は、駆動源の喪失、系のしゃ断に対して、原子炉をスクラムさせる方向に作動するように設計している。

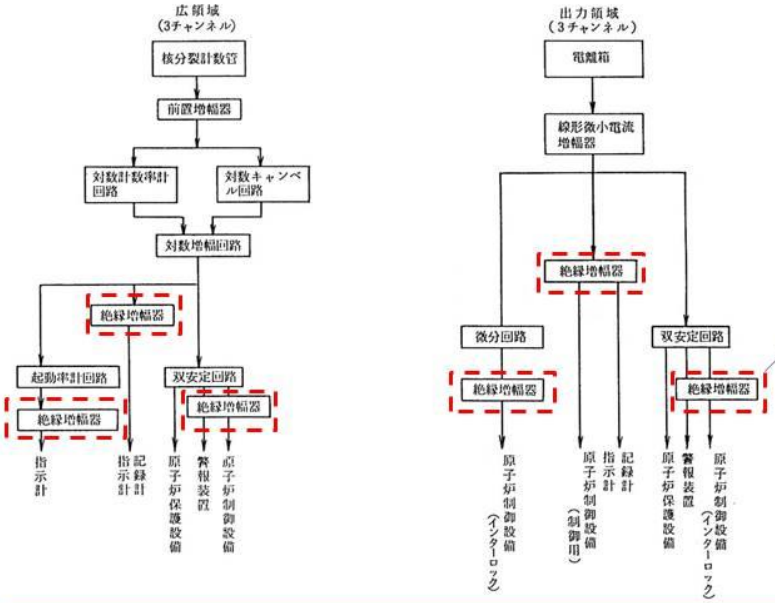
・その他の安全保護回路は、駆動源の喪失、系のしゃ断に対して、安全保護動作が作動するか又はそのまま現在の状態を維持する。この現状維持の場合でも、多重化された他の回路が保護動作を行い、安全上支障がないような設計としている。

不正アクセスの防止

・リレーやスイッチング素子等の電気部品を用いた制御機器で構成されており、外部ネットワークからの侵入やコンピュータウィルスの混入による誤動作を考慮する必要はない。

安全保護系以外の計測制御系との分離

安全保護系以外の計測制御系との分離の例（中性子計装）



絶縁増幅器で安全保護系以外の計測制御系を分離

安全保護系の信号を安全保護系以外の計測制御系に伝送する場合は絶縁増幅器を使用し、出力側(安全保護系以外の計測制御系)で故障が生じても、入力側(安全保護系)に影響を与えない設計としている。

2019 年 3 月 26 日審査会合コメント

安全保護回路は、リレーやスイッチング素子等の電気部品を用いた制御器で構成され、ソフトウェアを用いていないとのことであるが、原子炉制御設備にはソフトウェアを用いた電子計算機を使用しているということでもあるので、インターロック回路も含めてソフトウェアを用いない設計となっているのかを明らかにして説明すること。

インターロック回路を含む安全保護回路の構築については、安全保護系のプロセス計装からの信号に対し、リレーによる絶縁及び制御カードによる信号処理を行っている。具体的には、原子炉計装又はプロセス計装からのバイステーブル作動信号が安全保護ロジック盤のロジック入力リレーに入力され、その信号が 2/3 論理判定回路、前述のインターロック回路等の機能を有した制御カードで信号処理された後、ロジック出力リレーにより原子炉スクラム遮断器及び安全保護シーケンス盤へ信号を出力している。2/3 論理判定回路、インターロック回路等の機能を有する制御カードについては、トランジスタ等の半導体素子の電気部品で構成されておりソフトウェアは使用していない。

2019 年 3 月 26 日審査会合コメント

安全保護回路はソフトウェアを使用していないので外部ネットワーク等からの侵入防止等のサイバーセキュリティは不要としているが、設備への接近性など物理的な防護措置も含めてどのように対処しているかを説明すること。

原子炉停止信号を発信する安全保護ロジック盤、工学的安全施設の作動信号を発信する安全保護シーケンス盤の論理回路については、ソフトウェアを使用していないことから、外部ネットワーク等からの侵入防止等のサイバーセキュリティは不要ではあるものの、1)HTTR 原子炉建家及び中央制御室に立ち入る者に対する入域管理、2)盤の施錠及び鍵管理により、外部からの人的妨害行為又は破壊行為を防止している。

2019 年 3 月 26 日審査会合コメント

通常運転時と異なる安全性実証試験時の特殊運転において、安全保護回路の機能をどのように制限するのか、その後の復帰の具体的な条件も含めて施設に影響がないかを説明すること。

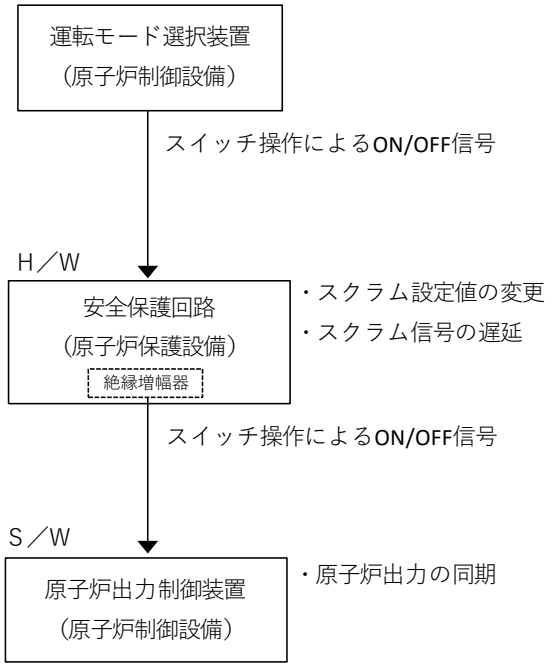
特殊運転モードへの移行又は試験後の復帰は、中央制御盤に設置されている運転モード選択装置に連動して、制御棒の引抜き防止及びスクラム設定値の変更等の必要な措置を設定あるいは解除することで運転員の誤操作防止を図っている。特殊試験の解除にあたっては、原子炉出力制御系の設定値と原子炉出力の計測値との偏差を許容範囲内とすることが条件となっており、原子炉出力制御系の設定値と原子炉出力の計測値との偏差が許容範囲内となるような同期回路を設けることで、制御系に過大な外乱を与えることを抑制している。

2019 年 5 月 22 日審査会合コメント

特殊運転時における安全保護回路の機能に対する制限の方法について具体的に説明すること。また、ソフトウェアで構築する同期回路が安全保護回路の機能に影響しないことを説明すること。

特殊運転への移行及び試験後の通常運転への復帰は、原子炉制御設備である運転モード選択装置のスイッチ操作に連動して行う。運転モード選択装置の操作信号を受け、半導体素子等の電気部品のみで構成される原子炉保護設備の安全保護回路において自動的にスクラム設定値の変更、スクラム信号の遅延等、通常運転時への復帰が行われる。また、運転モード選択装置の操作信号により、原子炉出力制御系が手動モードに切り替わる。手動モードに切り替わることで、原子炉出力制御系に係る自動モードの原子炉出力目標値が保持される。保持されている自動モードの原子炉出力目標値と特殊運転終了時の原子炉出力との偏差により、通常運転への復帰時に原子炉出力制御系に大きな外乱が印加されることとなる。これを防止するために、特殊運転の開始に伴い、自動モードの原子炉出力目標値を原子炉出力に同期させる同期回路が作動する。なお、同期回路の故障が安全保護動作に影響を及ぼすことはなく、原子炉出力目標値と原子炉出力の偏差が許容範囲を逸脱した場合においては、中央制御盤に警報が発信されることで運転員が同期回路の異常を早期に認識できる。さらに、運転モード選択装置の操作により通常運転に復帰させる際は、原子炉出力目標値と原子炉出力が同期していることを運転員が確認する旨を運転マニュアルに記載している。

この同期回路は、原子炉制御設備である原子炉出力制御装置にてソフトウェアにより構築され、外部ネットワークには接続されていない。なお、スクラム設置値の変更等の機能を有する安全保護回路はハードウェアで構築されているため、ソフトウェアで構築する同期回路の異常等が安全保護回路の機能に影響することはない。



運転モード選択装置に係る信号の流れ

参考資料

計測制御系統施設において使用される双安定回路の機能

２つの安定状態を持ち、入力された状態を保持し、ある条件が成立するまで出力を保持する回路であり、一般的にはフリップフロップ回路とも呼ばれている。HTTR においては、安全保護系信号を発信する検出器からの信号に対し、安全保護系計装盤内の判別回路にて異常信号の判定を行ない、安全保護回路での２out of 3 論理回路により保護動作信号を発信する。この安全保護系計装盤内の判別回路を双安定回路という。

コメント事項

商用電源喪失時には、どのような原子炉トリップ信号で原子炉停止に至るのか。 （低出力低流量で運転していた場合に原子炉トリップ信号がでないことはないか）

【回答】

商用電源喪失時は、商用電源から給電されるヘリウム循環機及び加圧水循環ポンプが停止する。これらにより、「1 次加圧水冷却器ヘリウム流量低」及び「炉心差圧低」等の流量・差圧に係る原子炉スクラム信号が発信する。なお、広領域中性子束 40000cps 以下の低出力状態においては、原子炉起動前及び停止後の冷却系の運転を継続する必要があること、スクラム信号を阻止することによる炉心への影響がないことから、流量・差圧に係る原子炉スクラム信号をブロック（P-A ブロック）する。従って、P-A ブロック時に商用電源が喪失した場合、原子炉スクラム信号は発信されない。なお、商用電源喪失による異常の有無の確認を目的に、原子炉を手動スクラムすることを運転手引に定めている。