資料1-2

本資料のうち，枠囲みの内容は機密事項に属しますので公開できません。

柏崎刈羽原子力発電所 6号及び7号炉

安全保護回路について

平成27年6月

東京電力株式会社

第二十四条：安全保護回路

〈目　　次〉

1.　基本方針・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 1
1.1　要求事項の整理・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 1
1.2　適合のための設計方針・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 3

2.　安全保護回路・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 6
2.1　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・・・・・・・・・・ 6
2.2　安全保護系盤の概要・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 9
2.3　物理的分離及び電気的分離について・・・・・・・・・・・・・・・・・・・・・・・ 10
2.4　外部からの不正アクセス行為防止について・・・・・・・・・・・・・・・・・・・ 11
2.5　安全保護系盤制御装置のソフトウェア管理方法について・・・・・・・・・・・・ 12
2.6　想定脅威に対する対策について・・・・・・・・・・・・・・・・・・・・・・・・・ 13
2.7　安全保護系の検証及び妥当性確認について・・・・・・・・・・・・・・・・・・・ 14

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　ディジタル型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
別紙6　ディジタル型安全保護回路について，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

〈概　　要〉

１．において，安全保護回路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柏崎刈羽原子力発電所６号炉及び７号炉における適合性を示す。

２．において，安全保護回路について，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。

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二十四条及び技術基準規則第三十五条において，追加要求事項を明確化する（第1.1表）。

第 1.1 表　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 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
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
－	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，原子炉緊急停止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。

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周期短により原子炉を停止できるように設計する。

二　安全保護系は，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，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. 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. 炉心流量急減
   h. 制御棒駆動機構充てん水圧力低
   i. 主蒸気隔離弁閉
   j. タービン主蒸気止め弁閉
   k. タービン蒸気加減弁急速閉
   l. 主蒸気管放射能高
   m. 地震加速度大
   n. 手動
   o. モード・スイッチ「停止」
2. 工学的安全施設を作動させる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，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，原子炉区域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注水系，原子炉隔離時冷却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同時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，以下に示す設計方針に基づき多重性を有するチャンネル構成とし，機器又はチャンネルの単一故障が起こっても，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。

具体例は下記のとおりである。

1. 原子炉緊急停止系の作動回路は，検出器，トリップ・チャンネル，主トリップ継電器等で構成し「2 out of 4」方式とする。

検出器は4区分に分け，一つの区分には，一つの測定変数に対して1個以上の検出器を設ける。また，トリップ・チャンネルは4チャンネル設ける。

各トリップ・チャンネルは，四つの区分の検出器からの信号を入力し，2区分以上の検出器の動作によりトリップする。各トリップ・チャンネルからの信号は，対応するトリップ・チャンネルに属する主トリップ継電器に入力され，二つ以上のトリップ・チャンネルがトリップした場合，原子炉はスクラムする。

したがって，機器またはチャンネルの単一故障が起こっても，使用状態からの単一の取り外しを行っても安全保護系の機能は維持できる。

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取り外しを行っても他の検出器により，安全保護機能は維持できる。

四　安全保護系は，その系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，独立牲を持つ設計とする。

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4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。各トリップチャンネルの論理回路は，盤内で独立して設ける。
3. 安全保護系作動回路の電源は，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
(1) スクラム
(2) 主蒸気隔離弁閉
(3) 格納容器ベント弁閉

2.　制御用空気喪失
(1) スクラム
(2) 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は，系の現状維持をもたらすものである。

系の遮断やその他，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を十分に安全な状態に導くよう設計する。

六　安全保護系は，以下のとおり，外部からの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している。

(1) 安全保護系は，直接社外のネットワークとは接続しない設計としており，外部システムと接続する必要があるデータについては，防護装置を介しての接続とするとともに，安全保護系盤の信号を一方向（送信機能のみ）通信に制限することで機能的に分離する設計とする。

(2) 安全保護系の回路には，安全保護上要求される機能を正しく確実に実現するために，設計，製作等の各段階において，検証及び妥当性確認を実施したソフトウェアを使用している。

(3) 不正な変更等による承認されていない動作や変更を防ぐため，発電所の出入管理により，物理的アクセスを制限するとともに，安全保護系盤制御装置の保守ツール接続コネクタ部に対して施錠を行い，関係者以外のアクセスを防止する設計とする。

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等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，4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　安全保護系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こと。』に対して，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）は下記の対策を実施している。

(1) 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。

(2) 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

緊急時対策支援システム伝送装置は，防護装置を介しての接続とするとともに，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。

(3) 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，安全保護系盤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，安全保護系盤制御装置の保守ツール接続コネクタ部を施錠すること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。

(4) システムの導入段階，更新段階又は試験段階で承認されていない動作や変更を防ぐ対策

「安全保護系へのディジタル計算機の適用に関する規程（JEAC4620）」及び「ディジタル安全保護系の検証及び妥当性確認に関する指針（JEAG4609）」に準じて設計，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，固有のソフトウェアを使用（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。（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）

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

ウイルスの侵入防止対策も含め，当社の安全保護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。

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。

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

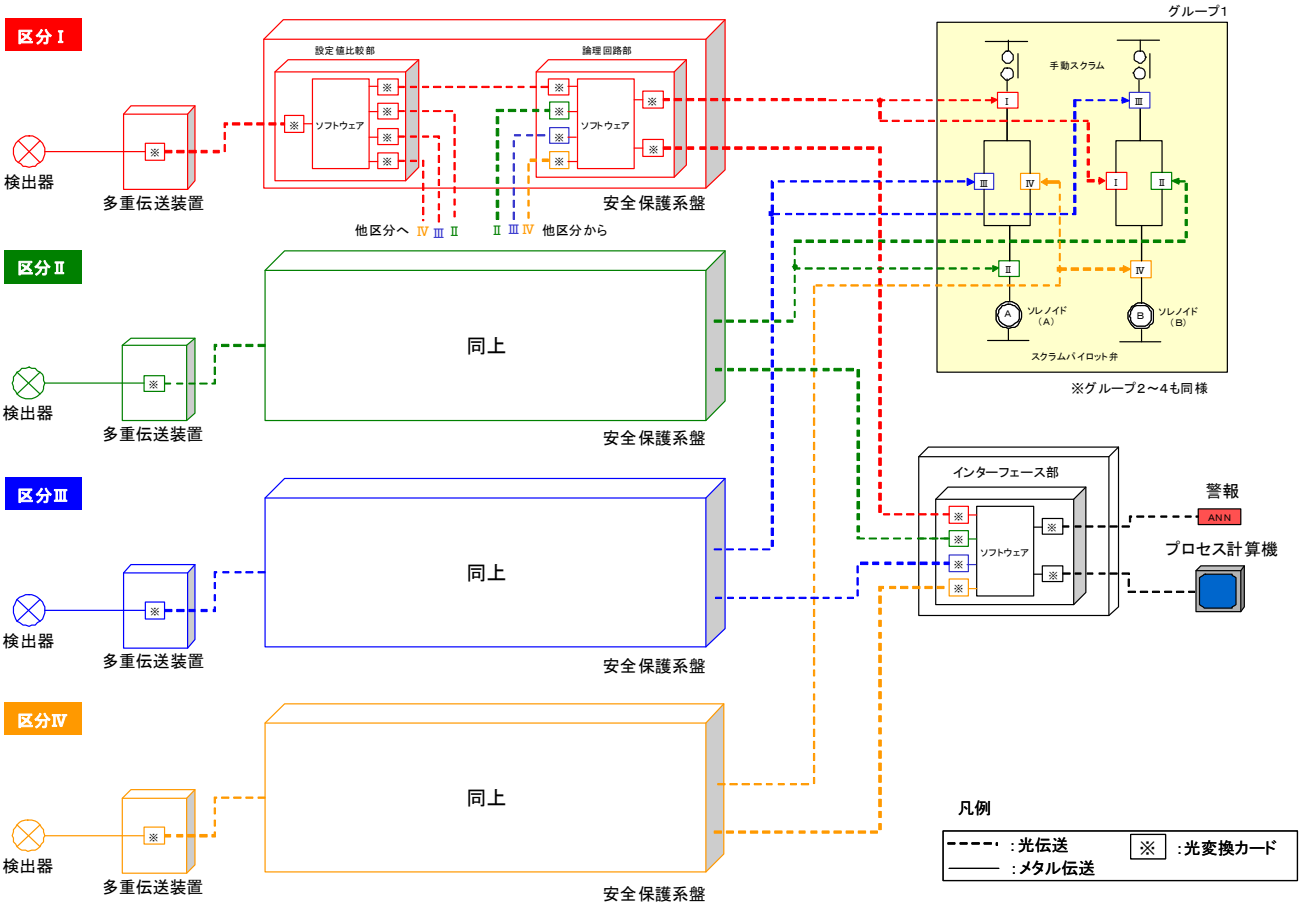
項目	当社の要求	供給者の対応
開発・改造に関する設計上の要求		
媒体の管理		
保守に関する要求		
教育		
設定及び設定変更管理		
作業実施		

：防護上の観点から公開できません

2.2　安全保護系盤の概要

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。

ディジタル設備の適用に当たっては，「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）に準じた検証及び妥当性確認を行っている。

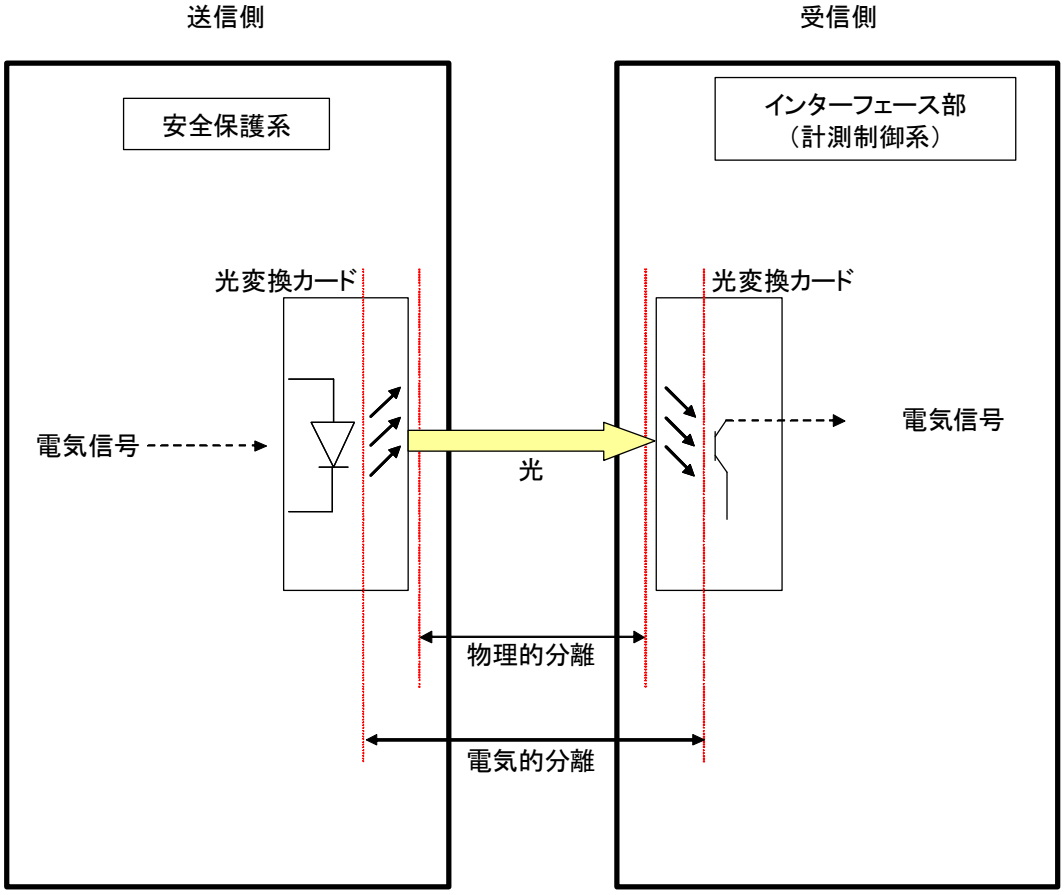


第 2.2 図　安全保護系盤構成図（例：原子炉緊急停止信号）

安全保護系は，相互干渉が起こらないように，物理的，電気的独立性を持たせている。盤内のソフトウェアは区分毎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，区分毎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。

2.3　物理的分離及び電気的分離について

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。

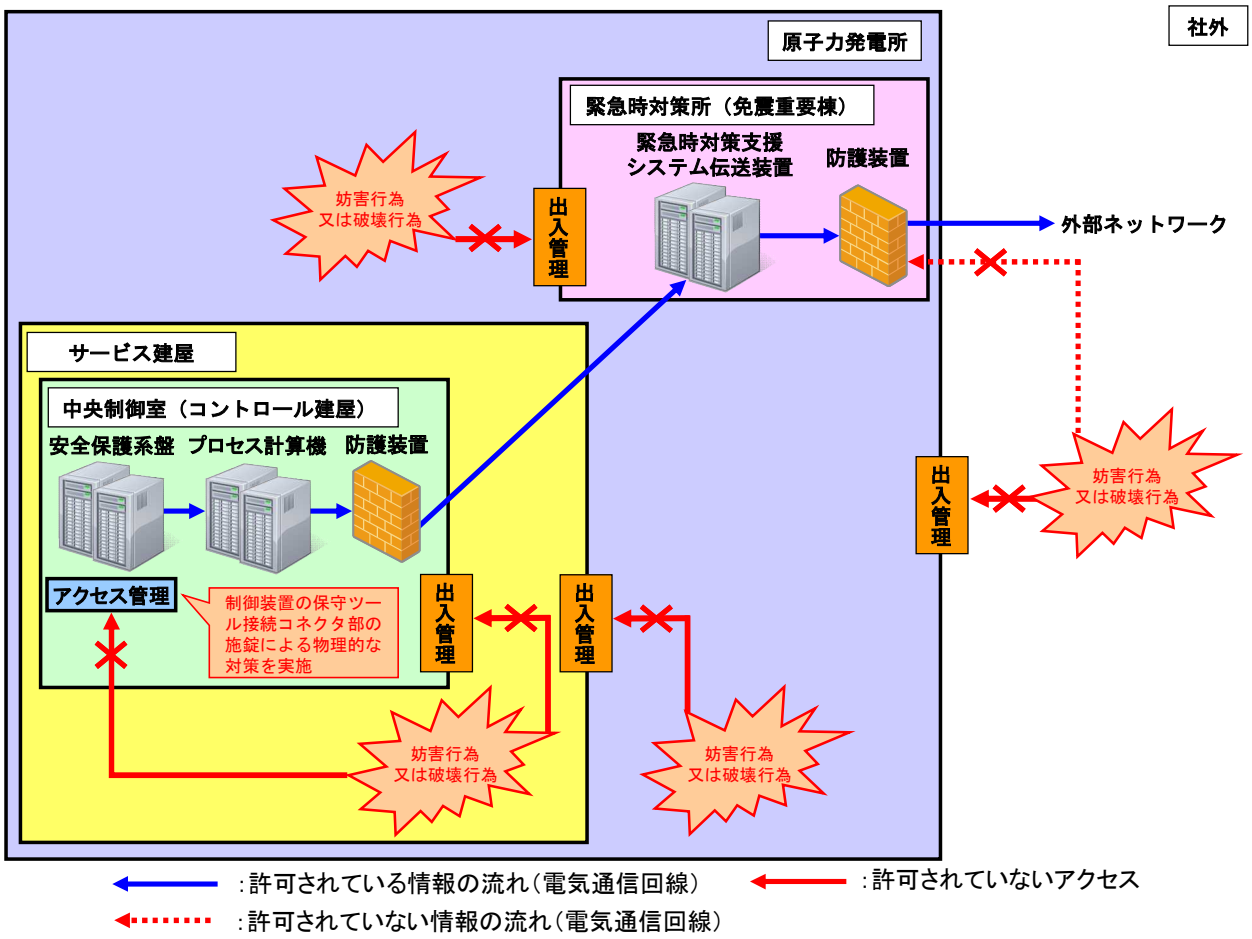


第 2.3 図　通信における分離概念図

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ソフトウェア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。

原子力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または破壊行為を防止している。また，安全保護系盤制御装置の保守ツール接続コネクタ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。

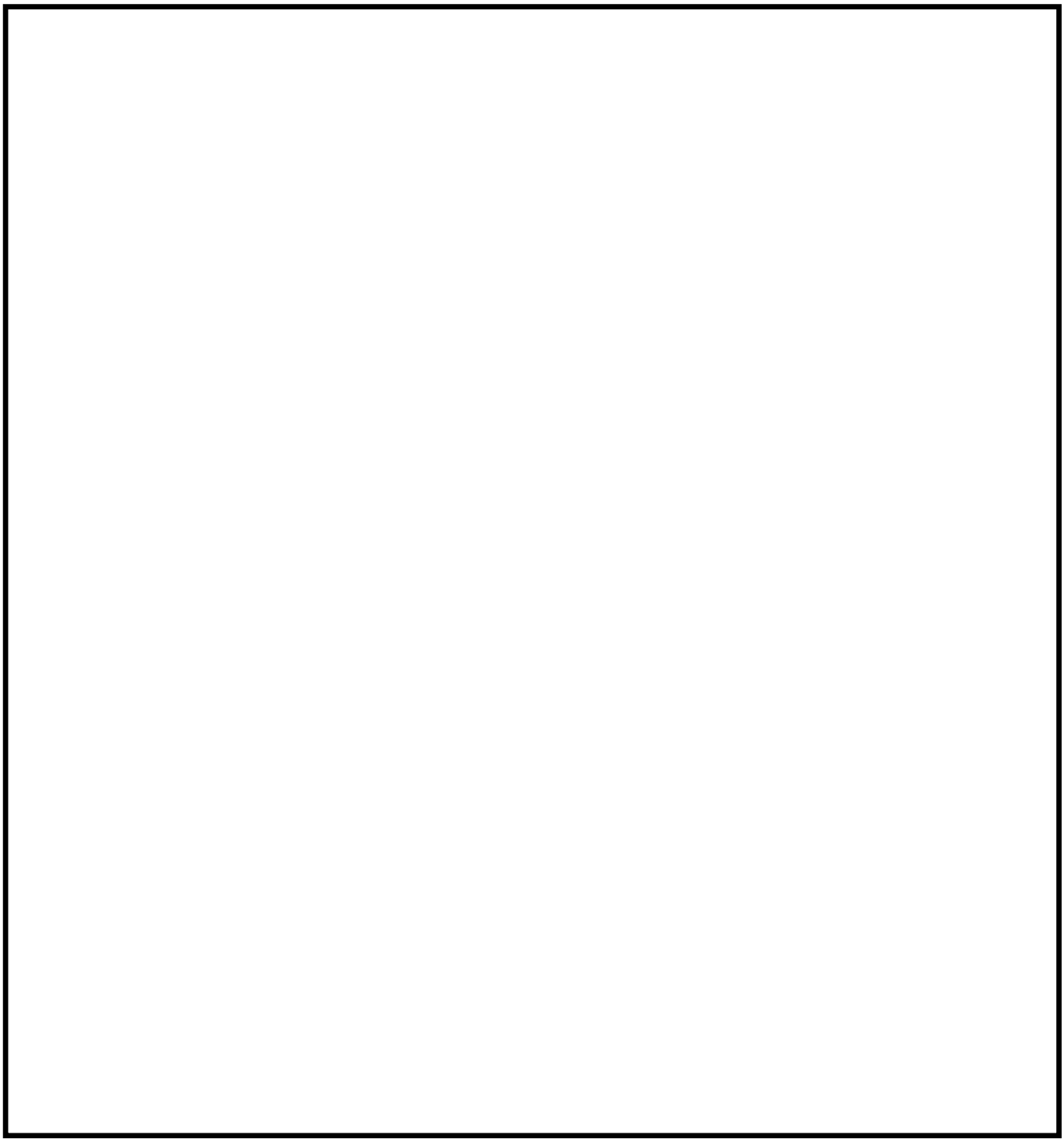


第 2.4 図　ネットワーク概略図

2.5　安全保護系盤制御装置のソフトウェア管理方法について

安全保護系盤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，保守ツール使用時は安全保護系盤制御装置の保守ツール接続コネクタ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。安全保護系盤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。

なお，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。



第 2.5 図　安全保護系盤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

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）

想定脅威	対策

：防護上の観点から公開できません

2.7　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 2.7-1 表 ライフサイクルプロセスにおける各段階での対策

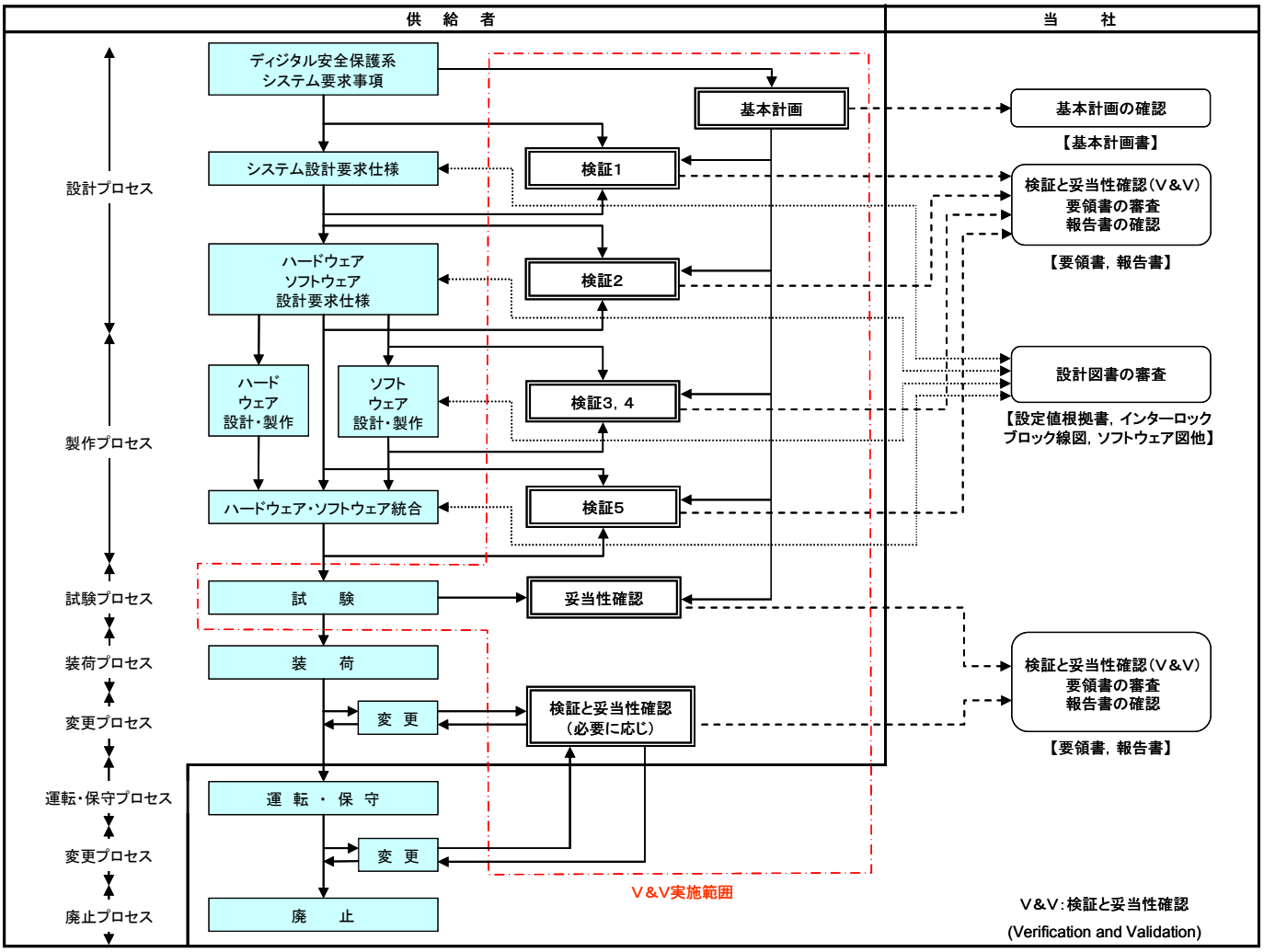
段階	内容	対策
設計プロセス	安全保護系設備に対するシステムの要求事項からソフトウェア設計仕様を作成する。	
製作プロセス	安全保護系設備ソフトウェア設計要求仕様より安全保護系設備ソフトウェアを製作する。	
試験プロセス	製作された安全保護系設備ソフトウェアに対して，ハードウェアを統合し，その統合したシステムが設計要求通り製作されていることを試験により確認する。	
装荷プロセス	実機へ安全保護系設備ソフトウェアを実装する。	
変更プロセス	安全保護系設備ソフトウェアの変更が生じた場合，変更仕様を決定し，変更を行うライフサイクルプロセスから，変更の実施内容に応じて必要とされる各々のプロセスを順次実施する。	

：防護上の観点から公開できません

ディ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，「安全保護系へのディジタル計算機の適用に関する規程」（JEAC4620）及び「ディジタル安全保護系の検証及び妥当性確認に関する指針」（JEAG4609）に基づき，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。



第 2.7 図　ディ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 2.7-2 表　検証項目及び検証内容

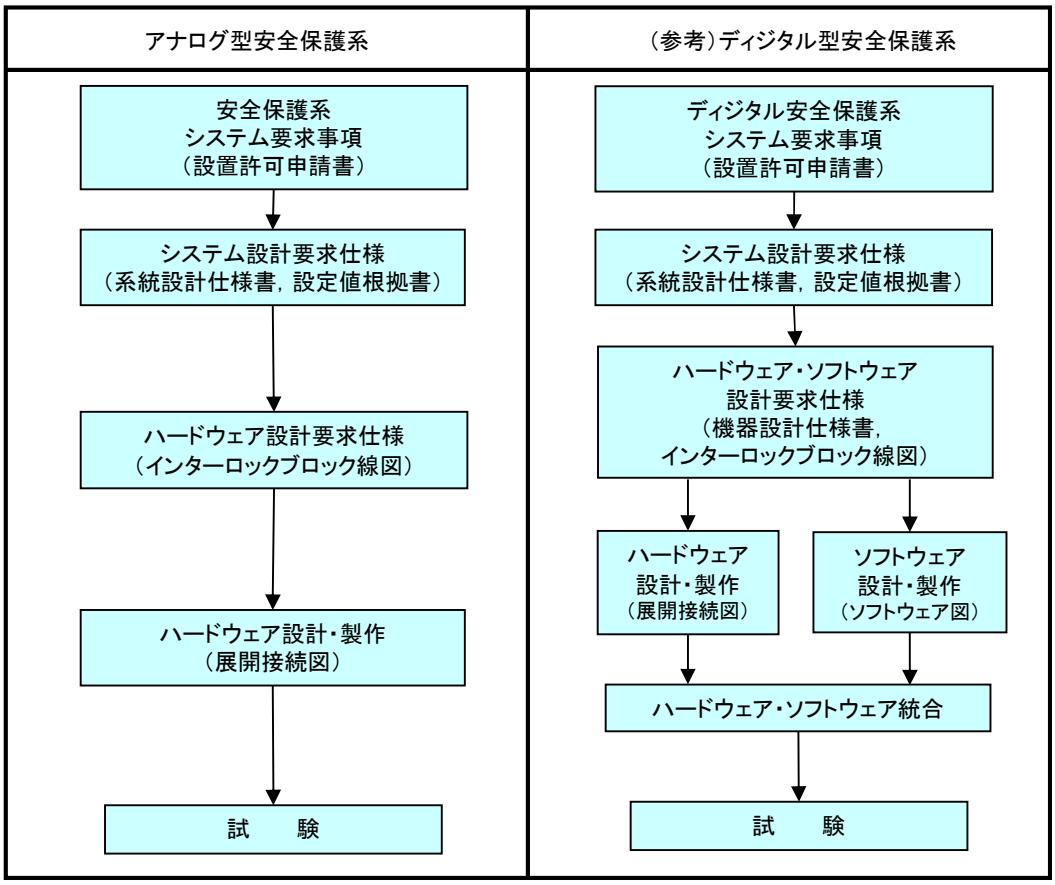
検証項目	検証内容
検証 1	ディジタル安全保護系システム要求事項が正しくシステム設計要求仕様に反映されていることを検証する。
検証 2	システム設計要求仕様が正しくハードウェア・ソフトウェア設計要求仕様に反映されていることを検証する。
検証 3	ソフトウェア設計要求仕様が正しくソフトウェア設計に反映されていることを検証する。
検証 4	ソフトウェア設計通りに正しくソフトウェアが製作されていることを検証する。
検証 5	ハードウェアとソフトウェアを統合してハードウェア・ソフトウェア設計要求仕様通りのシステムとなっていることを検証する。
妥当性確認	ハードウェアとソフトウェアを統合して検証された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

以上

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。



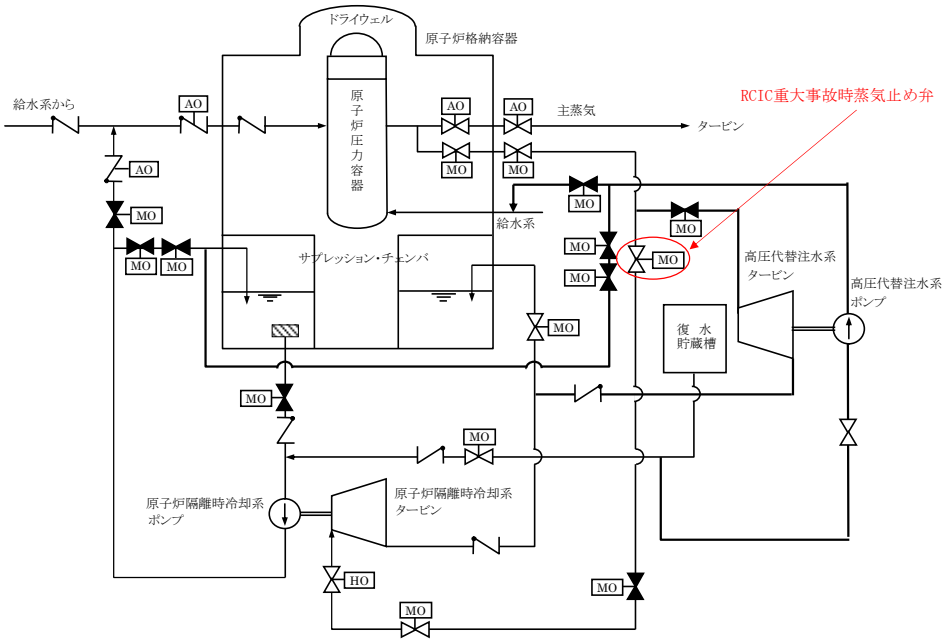
第１図　安全保護系の設計・製作・試験の流れ（例）

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

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に伴い，ディ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あるが，「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，試験等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。

「参考 1：6 号炉及び 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，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。
- RCIC 起動失敗，または機能喪失時に，RCIC 蒸気入口弁操作不能（開状態で停止）で HPAC 起動後も 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，RCIC 重大事故時蒸気止め弁を設置しており，この弁操作を 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。



第 1 図　高圧代替注水系(HPAC)の系統概要

「参考 2：6 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。

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ィジタル型制御装置を使用している（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）。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　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」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) 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。

(2) 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

緊急時対策支援システム伝送装置は，防護装置を介しての接続とするとともに，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。

(3) 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。

(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

アナログ型安全保護回路は別紙１の通り。

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。また，固有のソフトウェアを使用（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。

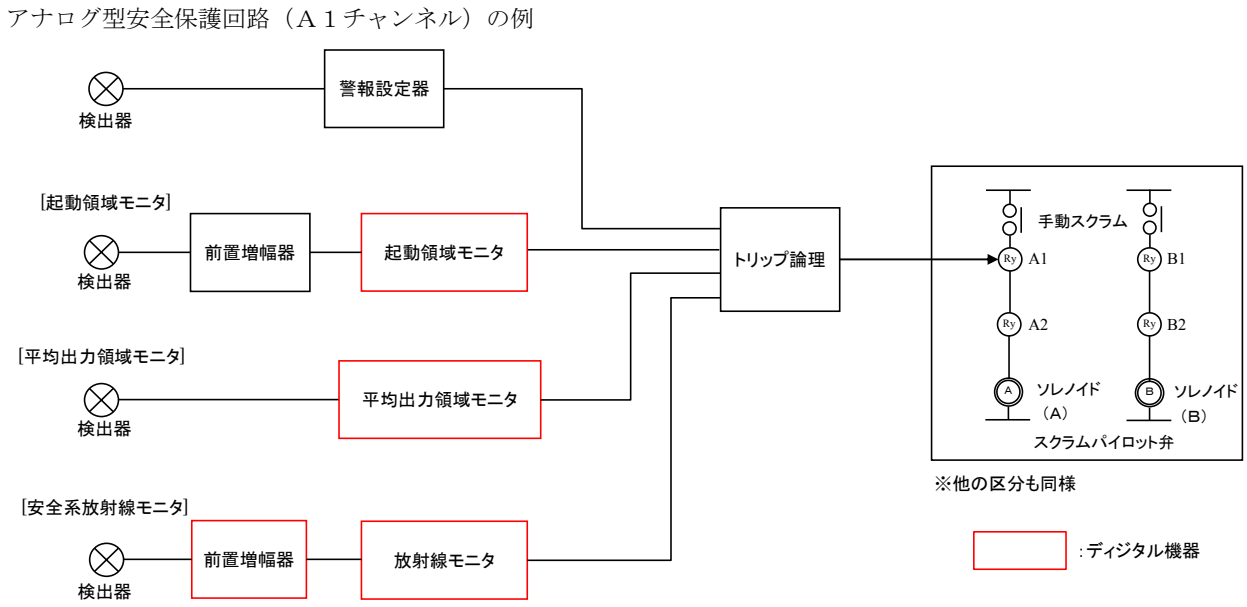
(5) 耐ノイズ・サージ対策

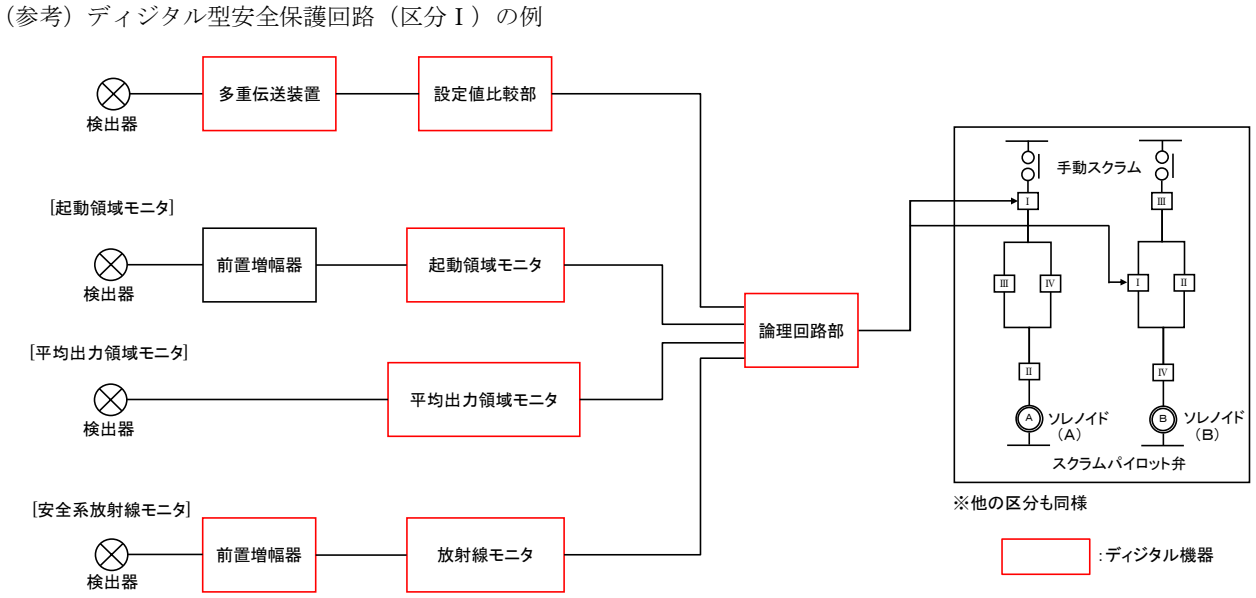
安全保護系は，雷・誘導サージ・電磁波障害等による擾乱に対して，制御盤へ入線する電源受電部にラインフィルタや絶縁回路を設置，外部からの信号入出力部にラインフ

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

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。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。





第１図　安全保護回路の構成例（原子炉緊急停止系）

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

安全保護系盤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。

- 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盤制御装置の保守ツール接続コネクタ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。
- 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。
- 保守ツール接続コネクタ部の鍵は，当直長の許可を得た上で，貸し出しを行っている。

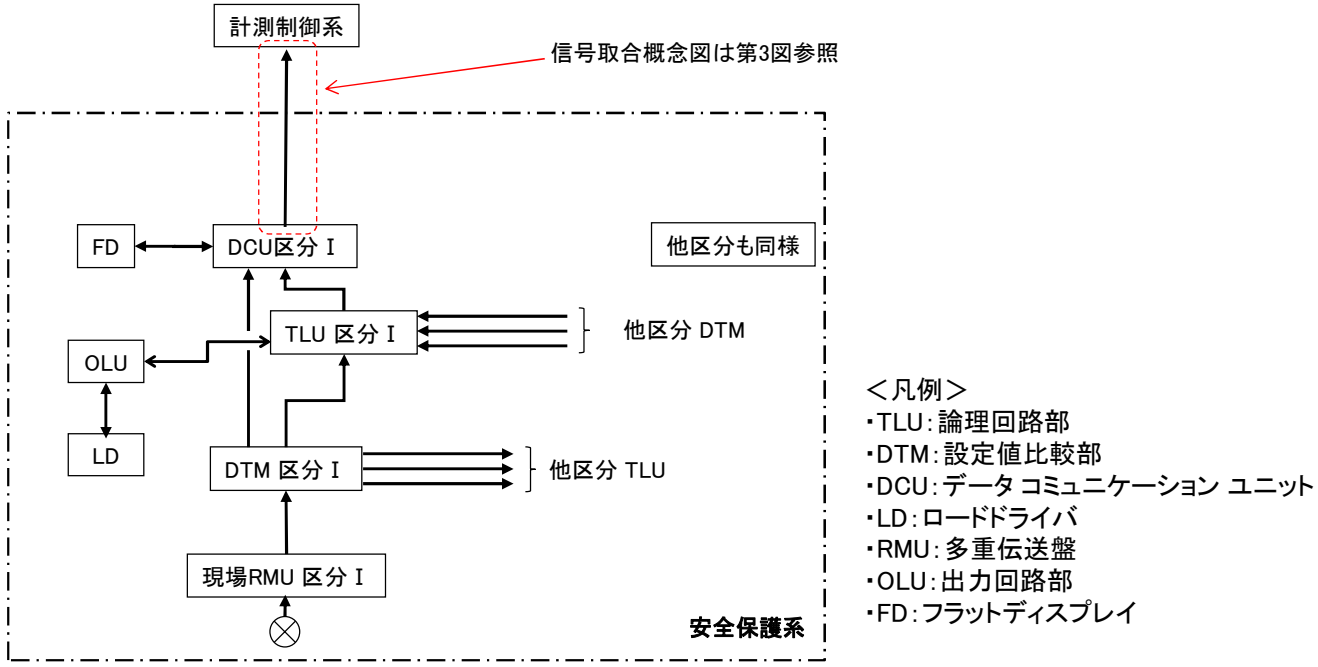
- ソフトウェア変更に係わる者は，情報セキュリティ教育（１回／年）を受講している。

：防護上の観点から公開できません

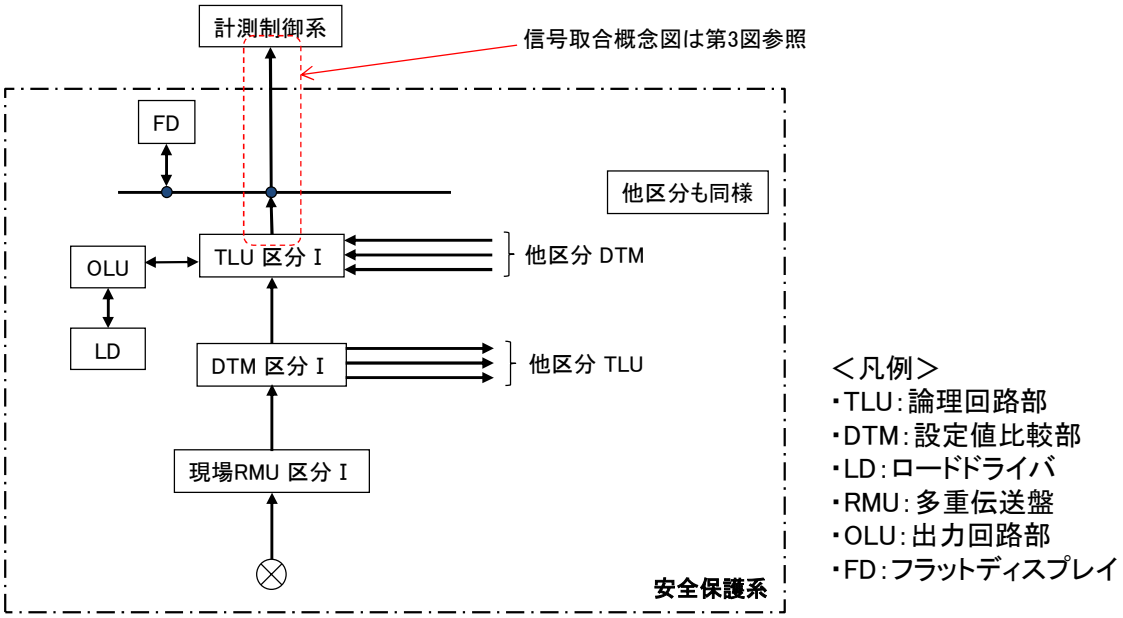
別紙 5 ディジタル型安全保護回路のシステムへ接続可能なアクセスについて

ディジタル型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盤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。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 図の通りであり，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，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。

また，安全保護系盤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，保守ツール使用時は安全保護系盤制御装置の保守ツール接続コネクタ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）

第 3 図　安全保護回路と計測制御系との信号取合概念図

：枠囲みの内容は商業機密に属しますので公開できません。

別紙 6 ディジタル型安全保護回路について，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

制御装置用デバイス（ソフトウェア含む）は，供給者独自のハードウェア及びソフトウェアを使用し，システム設計通りの機能を実現するため，必要なシステムソフトウェアを組み込む形態となっており，不要デバイスの具備を排除した構造としている。ハードウェア的には，信号取合のインターフェイス部に空きポートが存在するが，実動作している回路に影響を及ぼすことが無いようにソフトウェア的に無効化している。

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，ディ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，「安全保護系へのディジタル計算機の適用に関する規程」（JEAC4620）及び「ディジタル安全保護系の検証及び妥当性確認に関する指針」（JEAG4609）に基づき，供給者による検証及び妥当性確認の各段階において，確実に実施されていることを確認している。

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，柏崎刈羽原子力発電所 6 号炉及び 7 号炉の安全保護系の設計面へ反映すべき事項を下記の通り確認した。

（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

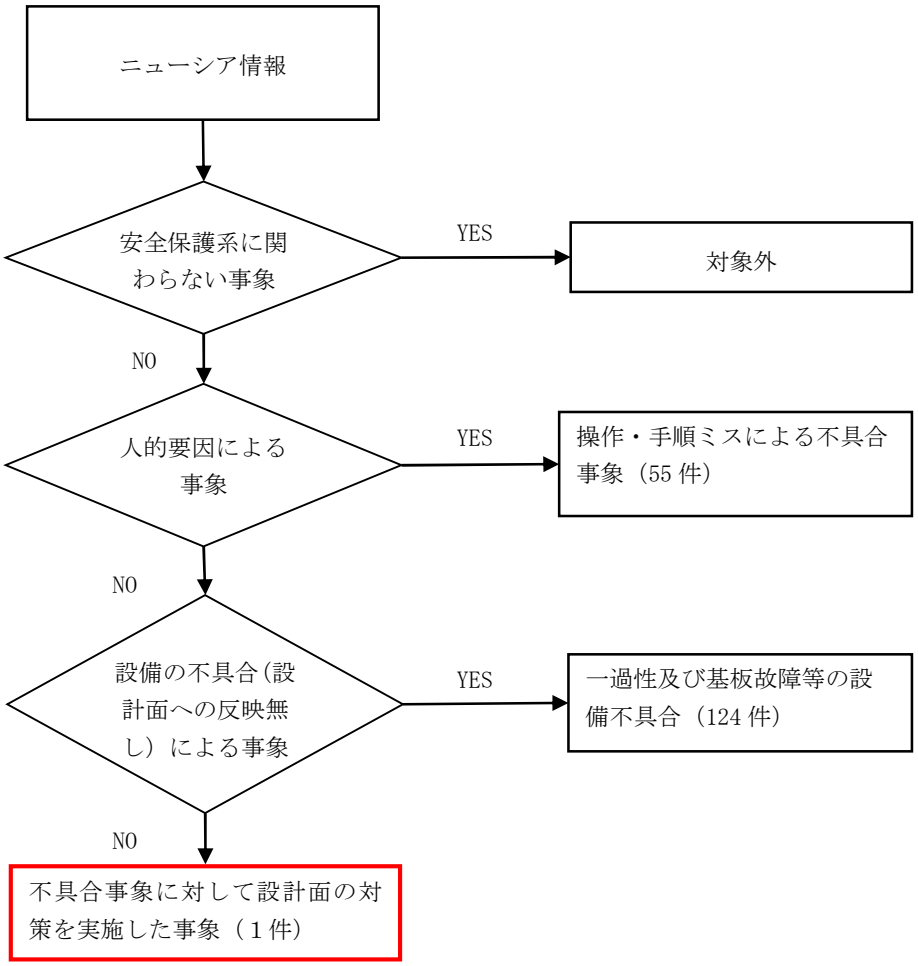
② キーワード検索（安全保護系，原子炉緊急停止系，工学的安全施設作動回路，雷，ノイズ，スクラム等）により抽出

（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，もしくは，反映不要であることを確認した。



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

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。

第２表　抽出された過去の不具合事象

件名	柏崎刈羽原子力発電所６号機　「主蒸気管放射能高」信号誤動作によるスクラムについて
会社名・プラント	東京電力株式会社　柏崎刈羽原子力発電所６号機
発生日	2012 年 08 月 22 日
事象概要	平成２４年８月２２日２０時１２分頃，定期検査中の６号機において，「主蒸気管放射能高」信号の誤動作によりスクラム信号が発生し，原子炉スクラム（ゼロスクラム）が発生した。 なお，６号機は冷温停止状態であり，制御棒は全挿入状態であった。 ＜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ーヘッダー圧力低」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	雷によるノイズ
対策	(1) アナログ式モニタからディ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。

以上