デジタル安全保護系への変更工事の設計思想（1／5）

1. 設計の流れ

まず、決定論にて故障を想定し、安全保護系の機能（ロジック盤設置、フェイル動作）を設計する。このとき、技術基準規則第35条第4号（フェイル動作）に適合するようにフェイル動作を設計する。

安全保護系の機能の設計後、システム全体の信頼性を「確率論」にて評価し、技術基準規則の解釈第35条第4項（デジタル安全保護系適用）の適合性を確認している。

2. 安全保護系の機能設計

○原子炉保護設備

（1）論理演算機能の移設

今回、ロジック盤の電子部品の製造中止等に伴いロジック盤を取替えるにあたって、ロジック盤が担っている、パラメータに対する論理演算機能（①）について、既設のデジタル制御装置である計器ラックのソフトウェアにて実現する。

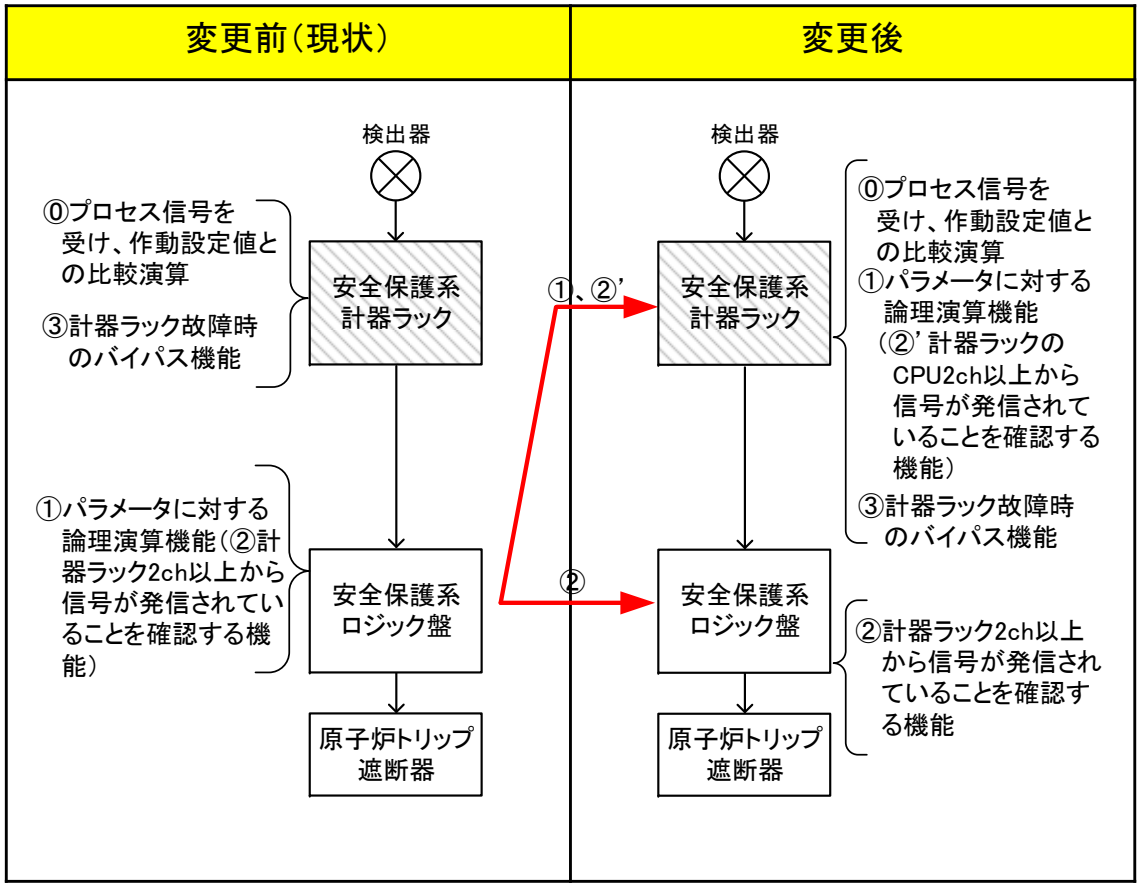
（2）設計における考慮事項

既設の計器ラックのCPUが1重化であるため、変更後において計器ラックの1重故障時の対応を考慮する。

ロジック盤を設置し、4chある計器ラックのうち2ch以上からの信号が発信されているかを判断する機能（②）をロジック盤に持たせることで、計器ラック1chの誤動作時においても原子炉トリップ遮断器が不要に動作することはない。（※）また、②の機能をロジック盤に持たせることで、計器ラック1chの不動作時においても残りの健全な3チャンネルによって、原子炉トリップ遮断器を動作させることができる。

計器ラック1chの誤動作時、警報発信後、運転員または保修員が計器ラックの保守パネルに設置されている操作スイッチにて当該計器ラックを系統から除外（バイパス）することにより、残り1chの計器ラックの動作で原子炉トリップ遮断器が実動作し、原子炉トリップする状態から、残り2chの計器ラックの動作で原子炉トリップ遮断器が実動作する状態に復帰できる。（機能（③））（故障計器ラックの系統からの除外については5項参照のこと。）

※計器ラック誤動作時、フェイルセーフ設計により原子炉トリップ信号を発信するものの、当該信号以外の3チャンネルからの信号が発信していないことをもって当該信号が誤動作であることを正常なロジック盤が判定し、原子炉トリップ遮断器への信号発信を阻止することにより、原子炉トリップ遮断器の不要な動作を回避する設計としている。ロジック盤を設置することによる信頼性への影響については、4項のとおり信頼性評価として実施している。



デジタル安全保護系への変更工事の設計思想（2／5）

○工学的安全施設作動設備

（1）論理演算機能の移設

原子炉保護設備同様に、ロジック盤が担っている、パラメータに対する論理演算機能（①）について、既設のデジタル制御装置である計器ラックのソフトウェアにて実現する。

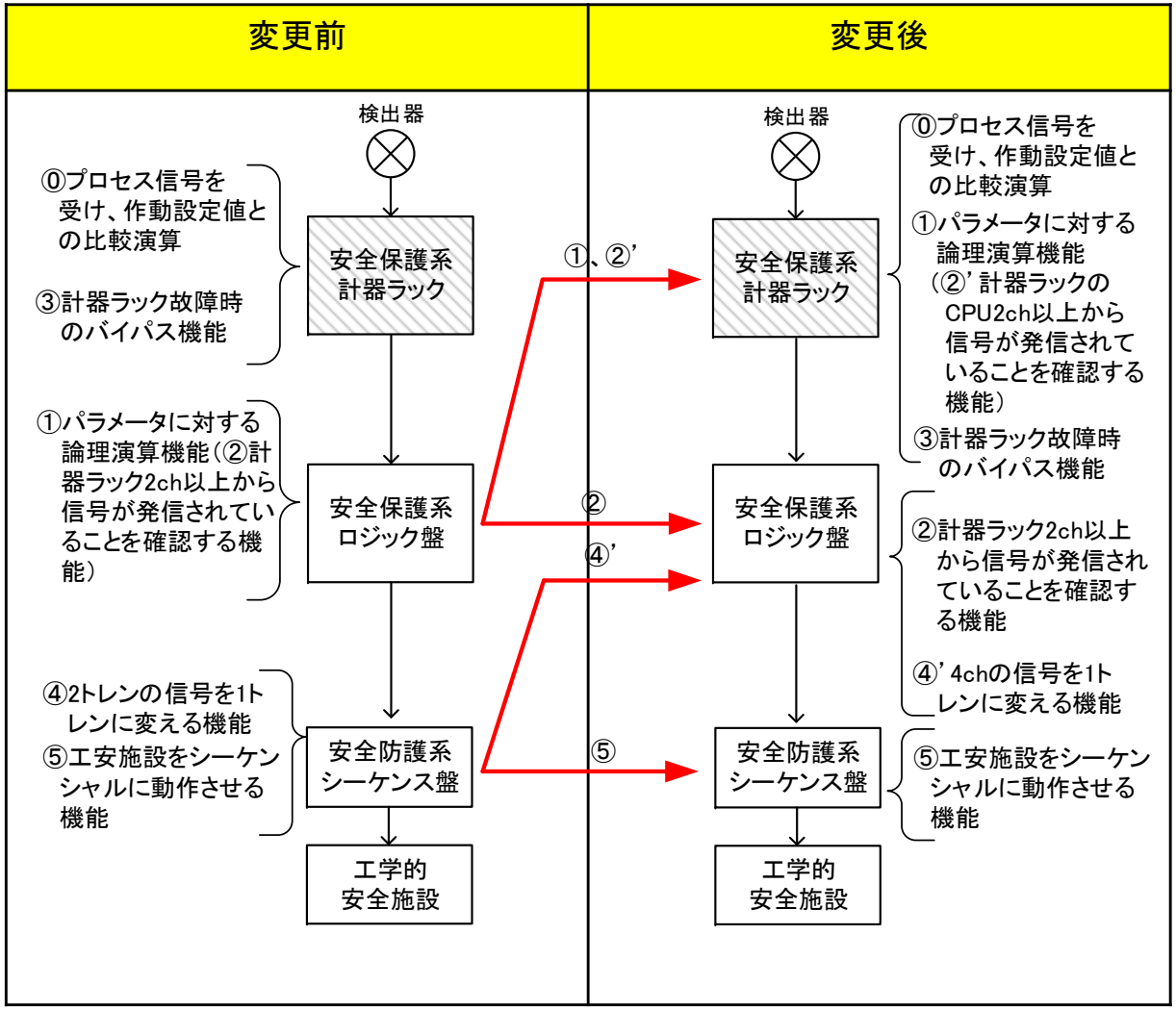
（2）設計における考慮事項

既設の計器ラックのCPUが1重化であるため、変更後において計器ラックの1重故障時の対応を考慮する。

ロジック盤を設置し、4chある計器ラックのうち2ch以上からの信号が発信されているかを判断する機能（②）を持たせることで、計器ラック1chの誤動作時においても、当該信号以外の3チャンネルからの信号が発信していないことをもって当該信号が誤動作であることを正常なロジック盤が判定し工学的安全施設への信号を阻止し、工学的安全施設の不要な動作を回避する設計としている。また、②および④’の機能をロジック盤に持たせることで、計器ラック1chの不動作時においても残りの健全な3チャンネルによって、工学的安全施設2トレンを動作させることができる。

変更前は、計器ラック1chの不動作時、4chある計器ラックのうち2ch以上からの信号が発信されているかを判断する機能（②）を持つロジック盤があることで工学的安全施設2トレンが動作可能であるが、変更後に仮にロジック盤を設置せず、既設同様にシーケンス盤で2/2の論理演算を行う設計とした場合、計器ラック1chの不動作時において工学的安全施設1トレンが動作不可となる。一方、変更後は2/4ロジックを持つロジック盤を設置する設計とすることから、ロジック盤が4chの信号を1トレンに変える機能（④’）を持つことにより、計器ラック1chの不動作時においても工学的安全施設2トレンが動作可能となる。

計器ラック1chの誤動作時、警報発信後、運転員または保修員が当該計器ラックを系統から除外（バイパス）することにより、残り1chの計器ラックの動作で工学的安全施設が実動作する状態から、残り2chの計器ラックの動作で工学的安全施設が実動作する状態に復帰できる。（機能（③））（故障計器ラックの系統からの除外については5項参照のこと。）



デジタル安全保護系への変更工事の設計思想（3／5）

（3）トレン構成

変更前のロジック盤が有する論理演算機能（①、②）については、4つのロジック盤で構成し、論理演算の結果、シーケンス盤に信号を発信している。シーケンス盤が有する論理演算機能（④）については、工学的安全施設作動設備が2トレン設備であること、また工学的安全作動設備全体の信頼性を評価した結果、2/2で必要十分であったことから2/2のロジックとしている。

変更後、ロジック盤の論理演算機能（①、②）が計器ラックに機能移設（①、②’）されることによって、ロジック盤を設置せず、2つの計器ラックから発信された信号をシーケンス盤で2/2の論理演算を行うことでも成立するが、計器ラック1chの不動作故障を考慮した場合、工学的安全施設1トレンが動作不可となる。一方、2/4ロジックを持つロジック盤を設置する設計としていることから、変更前と同様に計器ラック1chの不動作故障時においても工学的安全施設2トレンの動作が可能となる。2/4ロジックを持つロジック盤が計器ラックからの4ch信号を1トレンに集約する機能（④’）を有しているため、変更前にシーケンス盤が有している2/2の論理演算機能（④）は不要となる。このため、ロジック盤とシーケンス盤が1対1となるトレン構成となる。

（4）ロジック盤の出力リレーの設計

・駆動源の喪失（フェイル動作）

技術基準規則第35条第4号において、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（フェイルセーフ）か、又は当該状態を維持する（フェイルアズイズ）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が要求されている。

工学的安全施設に関しては誤作動により、プラントに外乱等（例：プラント運転中の誤SI作動）を与え、安全上支障を及ぼす可能性があることから、工学的安全施設作動設備全体としてフェイルアズイズ設計とし、単一のフェイル動作によって工学的安全施設が誤動作しない範囲の一部についてはフェイルセーフの設計としている。これは工事前後で変更はない。具体的に、単一のフェイル動作によって工学的安全施設が誤動作しない計器ラック（検出器含む）については一部をフェイルセーフの設計とし、最終段の論理演算機能を持つロジック盤についてはフェイルアズイズの設計とし、システム全体としてフェイルアズイズの設計としている。

最終段の論理演算機能（④）については、駆動源の喪失に対してフェイルセーフの設計とした場合、当該制御盤の駆動源喪失時に工学的安全施設が実際に誤動作することからフェイルアズイズの設計としている。

このフェイルアズイズ設計としている当該論理演算機能は、既設ではシーケンス盤が担っているが、変更後ではロジック盤が担う(④’)ことから、ロジック盤の出力リレーの駆動源喪失に対してはフェイルアズイズの設計とするため、出力リレーをb接からa接に変更する。これにより、既設同様に最終段の論理演算機能の駆動源の喪失に対してフェイルアズイズを実現している。最終段の論理演算機能を担う盤の駆動源の喪失を想定した場合において、1トレンが動作不能となるが、工学的安全施設作動設備は2トレン構成であり、残りの健全な1トレンにて安全保護系の機能は確保される。これは工事前後で変更はない。

※駆動源の喪失、系統の遮断その他の不利な状況として、電力もしくは計装用空気の喪失またはマイクロプロセッサ部の安全保護機能を喪失するような故障が考えられるが、ロジック盤はCPUを持たない電気盤であるため、駆動源の喪失（電力の喪失）のみが対象となる。

・単一の故障

出力リレーの不動作故障時、工学的安全施設作動設備の1トレンが動作不能となるが、残りの健全な1トレンにて安全保護系の機能は確保される。これは工事前後で変更はない。

（3）のとおり、変更後は、2/4ロジックをロジック盤に持たせ、2つのロジック盤で実現することから、ロジック盤とシーケンス盤が1対1となるトレン構成となる。このため、ロジック盤の出力リレーを1重化とした場合、出力リレー単体の誤動作故障（例：ノイズによるチャタリング等）により、シーケンス盤に誤信号が出力され、工学的安全施設が実際に誤動作し、外乱となる。これを回避するため、出力リレーを2重化（アンド回路）とする設計としている。

デジタル安全保護系への変更工事の設計思想（4／5）

3. 電源の設計

安全保護系に限らず、停電時の影響が大きい制御盤については、保守性※も踏まえ2重化する設計としている。

※電源を2重化することによって、電源側点検時に、当該制御盤を停止することなく点検することが可能。

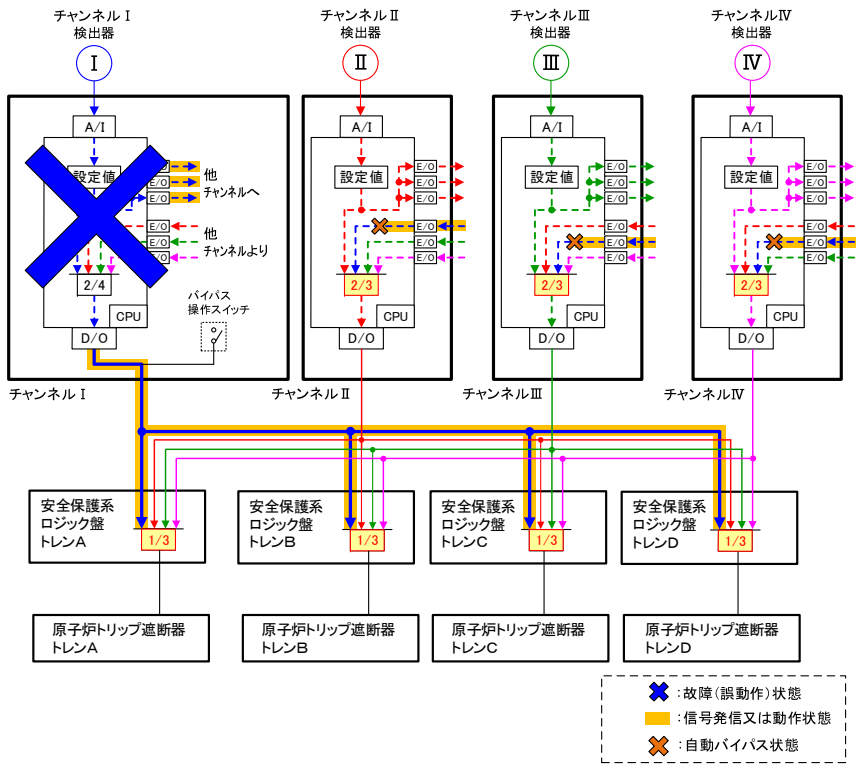
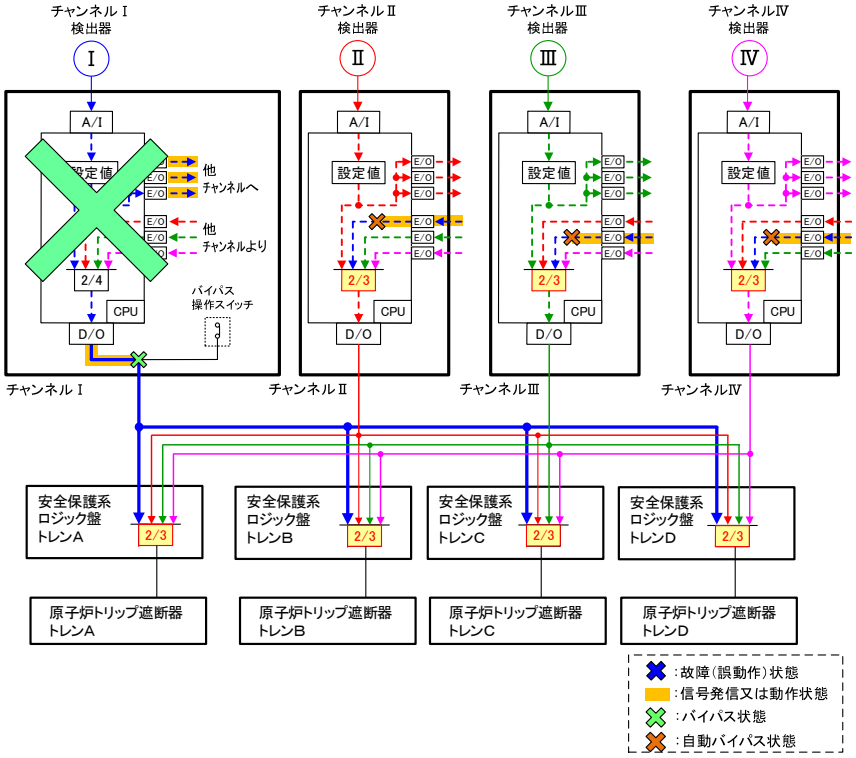
4. 原子炉保護設備の信頼性評価

1項～3項にて設計した原子炉保護設備に対してシステム全体の信頼性を評価した結果、既設同等であり、技術基準規則の解釈第35条第4項（6）を満足することを確認している。

デジタル安全保護系への変更工事の設計思想（5／5）

5. 故障計器ラックの系統からの除外について

警報発信後、運転員または保修員が計器ラックの保守パネルに設置されているバイパス操作スイッチにて、誤動作計器ラックからロジック盤へのDO出力をハードワイヤードにて強制的に励磁（格納容器スプレイ作動については非励磁）することで、残り1chの計器ラックの動作で原子炉トリップ遮断器が実動作し、原子炉トリップする状態から残り2chの計器ラックの動作で原子炉トリップ遮断器が動作する状態に復帰する。（なお、下図は、原子炉保護設備に係る説明であるが、工学的安全施設作動設備においてもロジック盤がトレンA、Bとなるだけで挙動に差異はない。）

故障時（誤動作）	バイパス時
	
原子炉トリップ信号の信号状態： 1／3	原子炉トリップ信号の信号状態： 2／3
計器ラックのマイクロプロセッサ等の故障に伴う誤動作時に、故障したチャンネルから信号が発信され、すべてのロジック盤の論理回路の状態が1/3となる。	故障した計器ラックを系統から除外（バイパス）することによって、すべてのロジック盤の論理回路の状態は2/3になり、2チャンネルの信号によって、原子炉トリップ遮断器が動作する状態に復帰する。