資料２

補足説明資料６

安全保護系の設計方針に関する補足説明

1. 概要

本資料では、デジタル安全保護系の設計方針について、説明する。

2. 更新前後における機能比較

安全保護装置のシステム構成について、更新前後の機能比較を行う。原子炉保護設備のシステム構成及び機能を第 1 図及び第 1 表に、工学的安全施設作動設備のシステム構成及び機能を第 2 図及び第 2 表にそれぞれ示す。

更新前では、原子炉トリップ信号又は工学的安全施設作動信号の発信に係るパラメータは、安全保護系計器ラック（以下「計器ラック」という。）に入力され、設定値比較される。この結果は、計器ラックの出力信号として、すべての安全保護系ロジック盤（以下「ロジック盤」という。）に信号分配され、2 out of 4（以下「2/4」という。）等の論理回路にて論理演算が行われる。

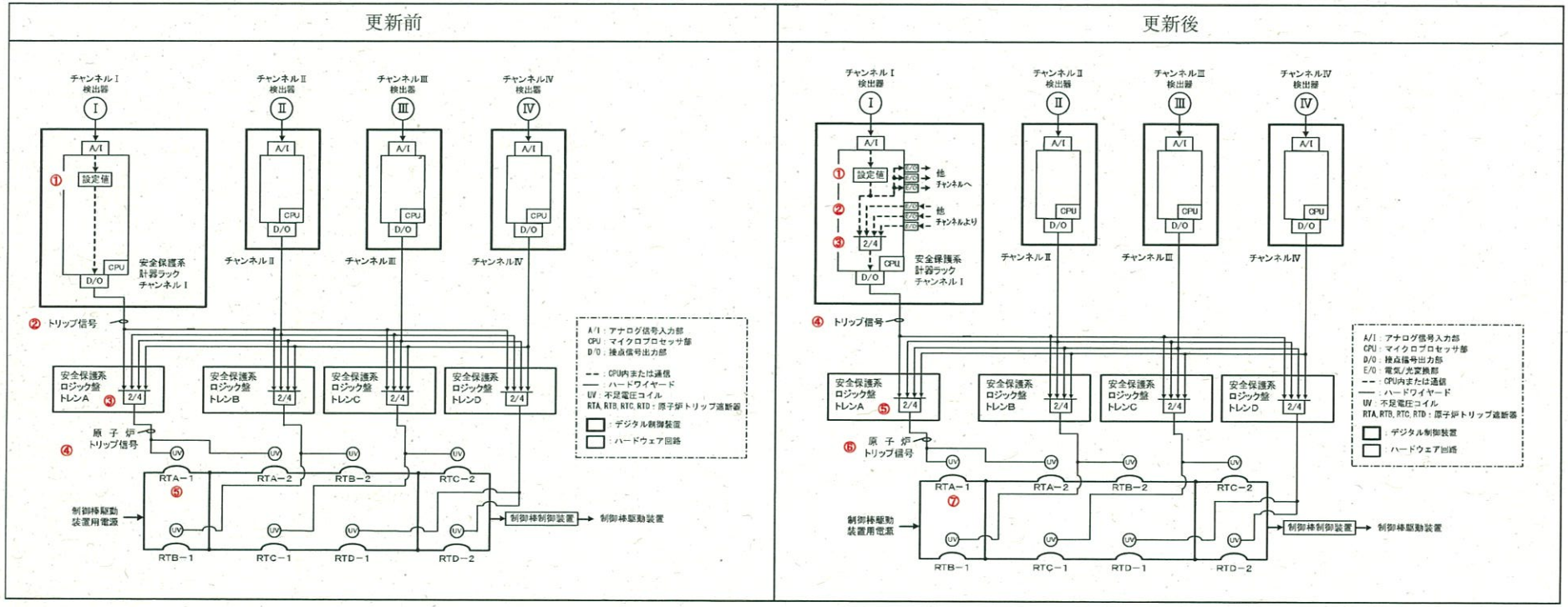
更新後では、上記の論理回路は、デジタル制御装置である計器ラックに機能分配（原子炉トリップ信号）または機能移設（工学的安全施設作動信号）され、ソフトウェアで実現される。新たに構築するロジック盤については、計器ラックからの出力信号に対する 2/4 の論理回路を設ける。この論理回路は、4 チャンネルある計器ラックのうち 2 チャンネル以上から、原子炉トリップ信号又は工学的安全施設作動信号が発信されているかを判断する機能を有する。ロジック盤を設けることによって更新後も既設同等の運用性を維持し、ロジック盤を設けずに更新した場合に比べて運用性の向上を図ることができる。

また、工学的安全施設作動信号について、更新前では、安全防護系シーケンス盤において、ロジック盤の 2 トレンの出力信号に対する 2/2 の論理回路を設け、論理演算が成立した場合に、1 トレンの工学的安全施設作動信号が発信する。（例えば、ロジック盤のトレン A と C の 2/2 回路で、トレン A の工学的安全施設作動信号が発信する。）

更新後では、上記の 2/2 の論理回路は、機能上、ロジック盤の 2/4 の論理回路に置き換わるため、ロジック盤の 1 トレンから工学的安全施設作動信号が発信によって、安全防護系シーケンス盤の 1 トレンから工学的安全施設作動信号が発信する設計とする。（例えば、ロジック盤のトレン A のみで、トレン A の工学的安全施設作動信号が発信する。）

なお、安全防護系シーケンス盤の 2/2 の論理回路は、機能上は不要になるものの、ケーブル損傷時の誤動作防止対策として、ロジック盤から同一信号を多重化して入力する。

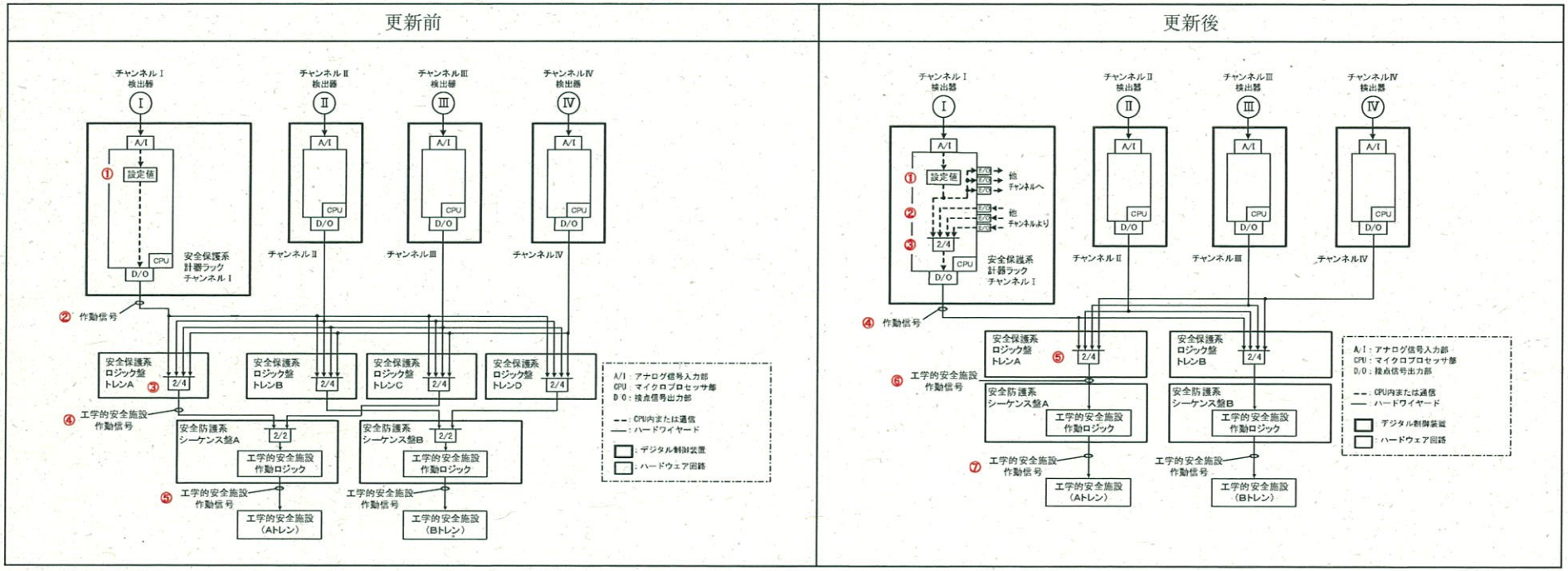
第１図　原子炉保護設備のシステム構成



第１表　原子炉保護設備の機能

	更新前	更新後
安全保護系計器ラックⅠ～Ⅳ（４チャンネル）	①プロセス信号を受け、作動設定値との比較演算を行う。 ②作動設定値の比較演算の結果、作動設定値に達したチャンネルは、安全保護系ロジック盤にトリップ信号を発信する。	①プロセス信号を受け、作動設定値との比較演算を行う。 ②作動設定値の比較演算の結果、作動設定値に達したチャンネルは、４チャンネルすべてにトリップ信号を発信する。 ③チャンネルからのトリップ信号を受け、論理演算（2/4 等）を行う。 ④論理演算の結果、作動条件が成立した場合には、安全保護系ロジック盤にトリップ信号を発信する。
安全保護系ロジック盤A～D（４トレン）	③安全保護系計器ラックからのトリップ信号を集約し、論理演算（2/4 等）を行う。 ④論理演算の結果、作動条件が成立した場合に、原子炉トリップ遮断器に原子炉トリップ信号を発信する。	⑤安全保護系計器ラックからトリップ信号を集約し、論理演算（2/4）を行う。 ⑥論理演算の結果、作動条件が成立した場合には、原子炉トリップ遮断器に原子炉トリップ信号を発信する。
原子炉トリップ遮断器（４トレン）	⑤原子炉トリップ信号を受け、原子炉トリップ遮断器を開放する。	⑦原子炉トリップ信号を受け、原子炉トリップ遮断器を開放する。

第２図　工学的安全施設作動設備のシステム構成



第２表　工学的安全施設作動設備の機能

	更新前	更新後
安全保護系計器ラックⅠ～Ⅳ（４チャンネル）	①プロセス信号を受け、作動設定値との比較演算を行う。 ②作動設定値の比較演算の結果、作動設定値に達したチャンネルは、安全保護系ロジック盤に作動信号を発信する。	①プロセス信号を受け、作動設定値との比較演算を行う。 ②作動設定値の比較演算の結果、作動設定値に達したチャンネルは、４チャンネルすべてに作動信号を発信する。 ③チャンネルからの作動信号を受け、論理演算（2/4 等）を行う。 ④論理演算の結果、作動条件が成立した場合には、安全保護系ロジック盤に作動信号を発信する。
安全保護系ロジック盤 A～D（４トレン）	③安全保護系計器ラックからの作動信号を集約し、論理演算（2/4 等）を行う。 ④論理演算の結果、作動条件が成立した場合に、安全防護系シーケンス盤に工学的安全施設作動信号を発信する。	⑤安全保護系計器ラックから作動信号を集約し、論理演算（2/4）を行う。 ⑥論理演算の結果、作動条件が成立した場合には、安全防護系シーケンス盤に工学的安全施設作動信号を発信する。
安全防護系シーケンス盤 A, B（２トレン）	⑤作動条件が成立した場合には、工学的安全施設の作動ロジックに従い、工学的安全施設作動信号を発信する。	⑦工学的安全施設の作動ロジックに従い、工学的安全施設作動信号を発信する。

3. 安全保護系ロジック盤の機能

3.1 原子炉トリップ信号及び工学的安全施設作動信号の発信について

3.1.1 通常時

（1）原子炉トリップ信号の発信（通常時）

すべての安全保護装置が健全な状態（通常時）において、ロジック盤が原子炉トリップ信号の発信を阻害しないことを示す。パラメータが設定値に達した場合の原子炉トリップ信号発信時の状態を第3図に示す。

例えば、チャンネルⅠの検出器信号は、ハードワイヤードで計器ラックのチャンネルⅠに入力され、ソフトウェアに取り込まれた後、設定値比較が行われる。設定値比較回路の出力信号は、下流の論理回路に入力されるとともに、通信で他チャンネルの計器ラックに出力される。同様に、他チャンネルの検出器信号が通信で入力されるため、計器ラックには、すべてのチャンネルの検出器信号が入力される。

ロジック盤を設ける場合の図(a)では、計器ラックの論理回路の出力信号は、すべてのロジック盤に信号分配されるため、ロジック盤には、すべての計器ラックの出力信号が入力される。４つの検出器のうち、２つ以上が原子炉トリップの設定値に達した場合、すべての計器ラックから原子炉トリップ信号が発信され、すべての原子炉トリップ遮断器が動作（開放）して、原子炉トリップに至る。

ロジック盤を設けない場合の図(b)では、計器ラックの論理回路の出力信号は、それぞれ対応する原子炉トリップ遮断器へ発信される。４つの検出器のうち、２つ以上が原子炉トリップの設定値に達した場合、計器ラックからのトリップ信号で、すべてのロジック盤から原子炉トリップ信号が発信され、すべての原子炉トリップ遮断器が動作（開放）して、原子炉トリップに至る。

このため、ロジック盤は、安全保護機能を阻害しない。

（2）工学的安全施設作動信号の発信（通常時）

すべての安全保護装置が健全な状態（通常時）において、ロジック盤が工学的安全施設作動信号の発信を阻害しないことを示す。パラメータが設定値に達した場合の工学的安全施設作動信号発信時の状態を第4図に示す。

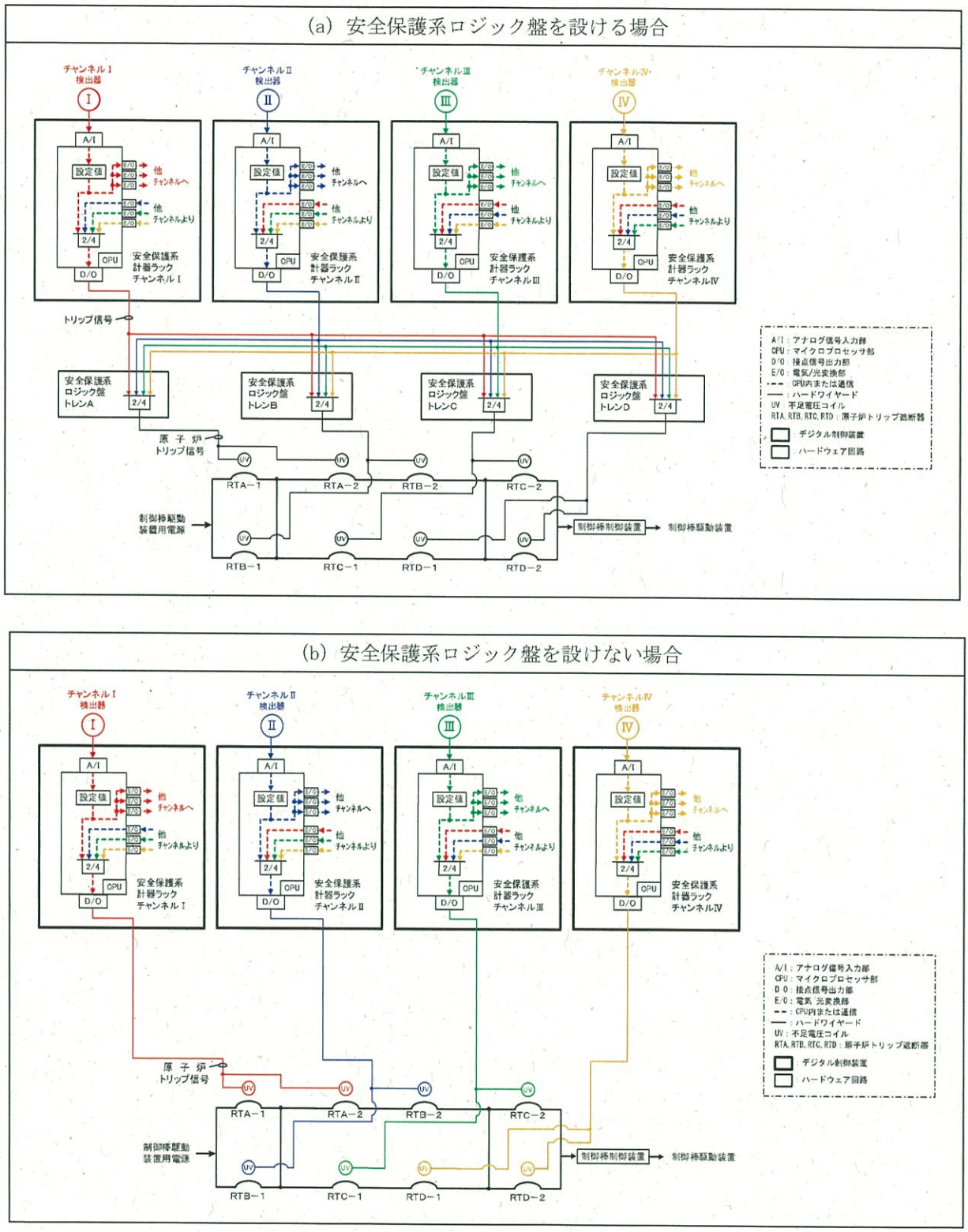
例えば、チャンネルⅠの検出器信号は、ハードワイヤードで計器ラックのチャンネルⅠに入力され、ソフトウェアに取り込まれた後、設定値比較が行われる。設定比較回路の出力信号は、下流の論理回路に入力されるとともに、通信で他チャンネルの計器ラックに出力される。同様に、他チャンネルの検出器信号が通信で入力されるため、計器ラックには、すべてのチャンネルの検出器信号が入力される。

ロジック盤を設ける場合の図(a)では、計器ラックの論理回路の出力信号は、トレンA及びBのロジック盤に信号分配されるため、トレンA及びBのロジック盤には、すべての計器ラックの出力信号が入力される。４つの検出器のうち、２つ以上が工

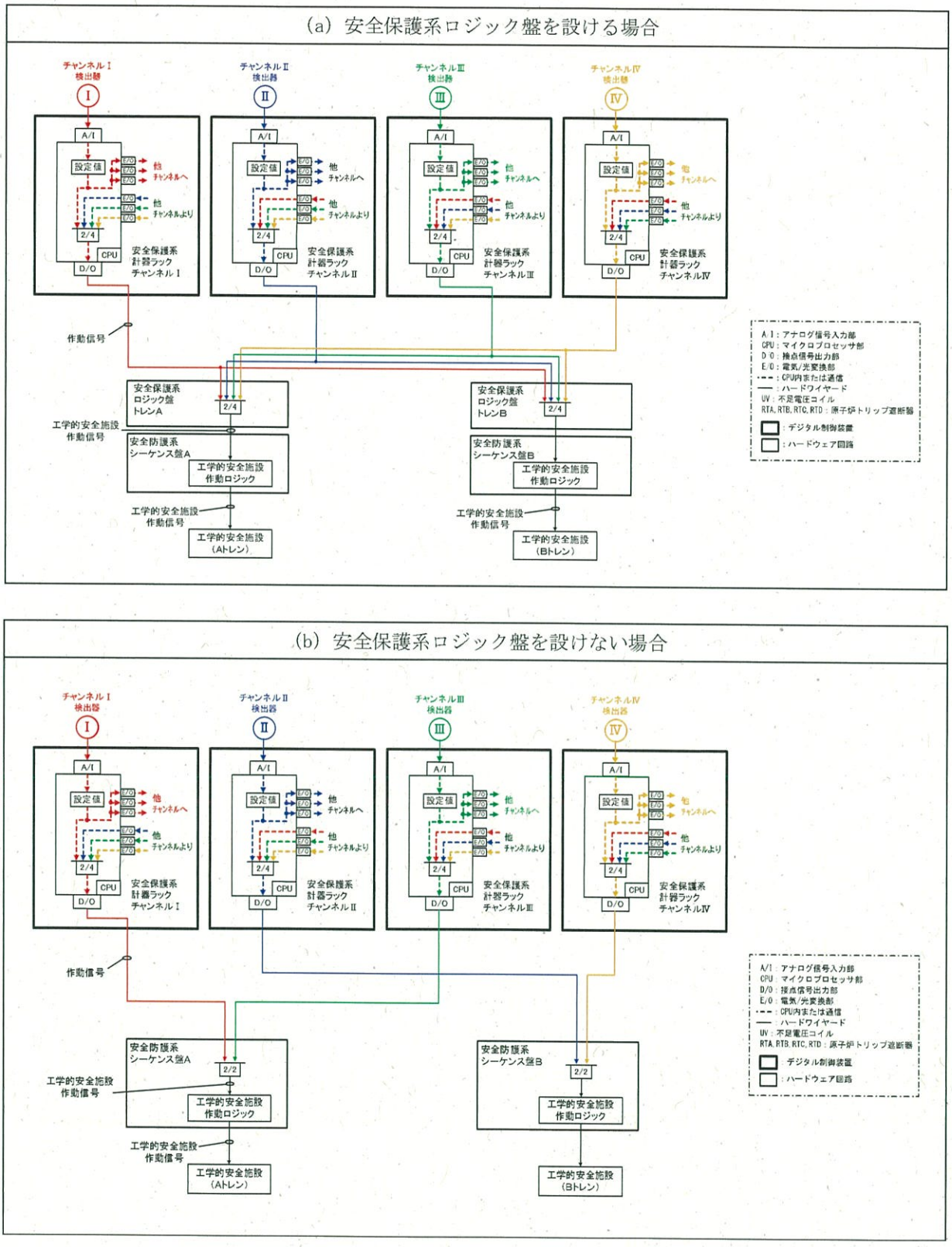
学的安全施設作動の設定値に達した場合、すべての計器ラックから工学的安全施設作動信号が発信され、トレンA及びBの安全防護系シーケンス盤で工学的安全施設が作動する。

ロジック盤を設けない場合の図(b)では、計器ラックの論理回路の出力信号は、チャンネルⅠ及びⅢはトレンAの安全防護系シーケンス盤に、またチャンネルⅡ及びⅣはトレンBの安全防護系シーケンス盤に入力されることになる。4つの検出器のうち、2つ以上が工学的安全施設作動の設定値に達した場合、計器ラックからの作動信号で、すべてのロジック盤から工学的安全施設作動信号が発信され、トレンA及びBの安全防護系シーケンス盤で工学的安全施設が作動する。

このため、ロジック盤は、安全保護機能を阻害しない。



第３図　原子炉トリップ信号の発信（通常時）



第４図　工学的安全施設作動信号の発信（通常時）

3.1.2 故障時

（1）原子炉トリップ信号の発信（故障時）

安全保護装置の不動作故障を想定した場合においても、ロジック盤が原子炉トリップ信号の発信を阻害しないことを示す。

例として、計器ラック又はロジック盤が単一故障に加えて追加故障を想定した場合に、パラメータが原子炉トリップ信号の設定値に達した場合の原子炉トリップ信号発信時の状態を第5図に示す。

2チャンネルの計器ラックの不動作故障を想定した場合の図(a)では、健全なチャンネルⅠ及びⅢの計器ラックにおいて、チャンネルⅠ及びⅢの検出器信号が入力されることから、2/4の論理回路が成立して、トリップ信号を発信する。

ロジック盤では、健全なチャンネルⅠ及びⅢの計器ラックから信号分配された2チャンネルの信号によって、すべてのロジック盤の2/4の論理回路が成立して、原子炉トリップ信号が発信する。

また、2トレンのロジック盤の不動作故障を想定した場合の図(b)では、健全なトレンB及びDのロジック盤において、2/4の論理回路が成立して、原子炉トリップ信号が発信する。

このため、ロジック盤は、安全保護機能を阻害しない。

（2）工学的安全施設作動信号の発信（故障時）

安全保護装置の不動作故障を想定した場合においても、ロジック盤が工学的安全施設作動信号の発信を阻害しないことを示す。

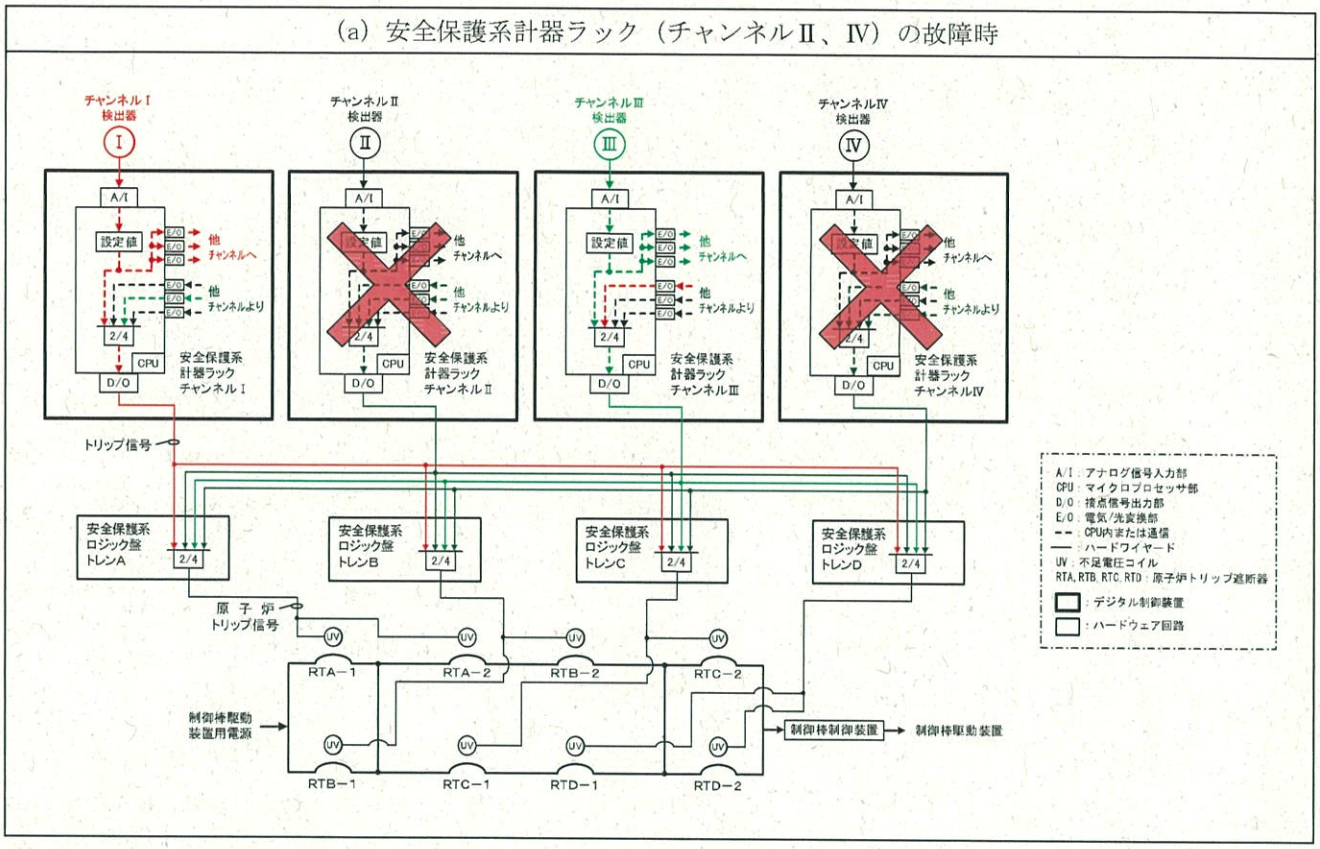
例として、計器ラックが単一故障に加えて追加故障を想定した場合又はロジック盤が単一故障した場合に、パラメータが工学的安全施設作動信号の設定値に達した場合の工学的安全施設作動信号発信時の状態を第6図に示す。

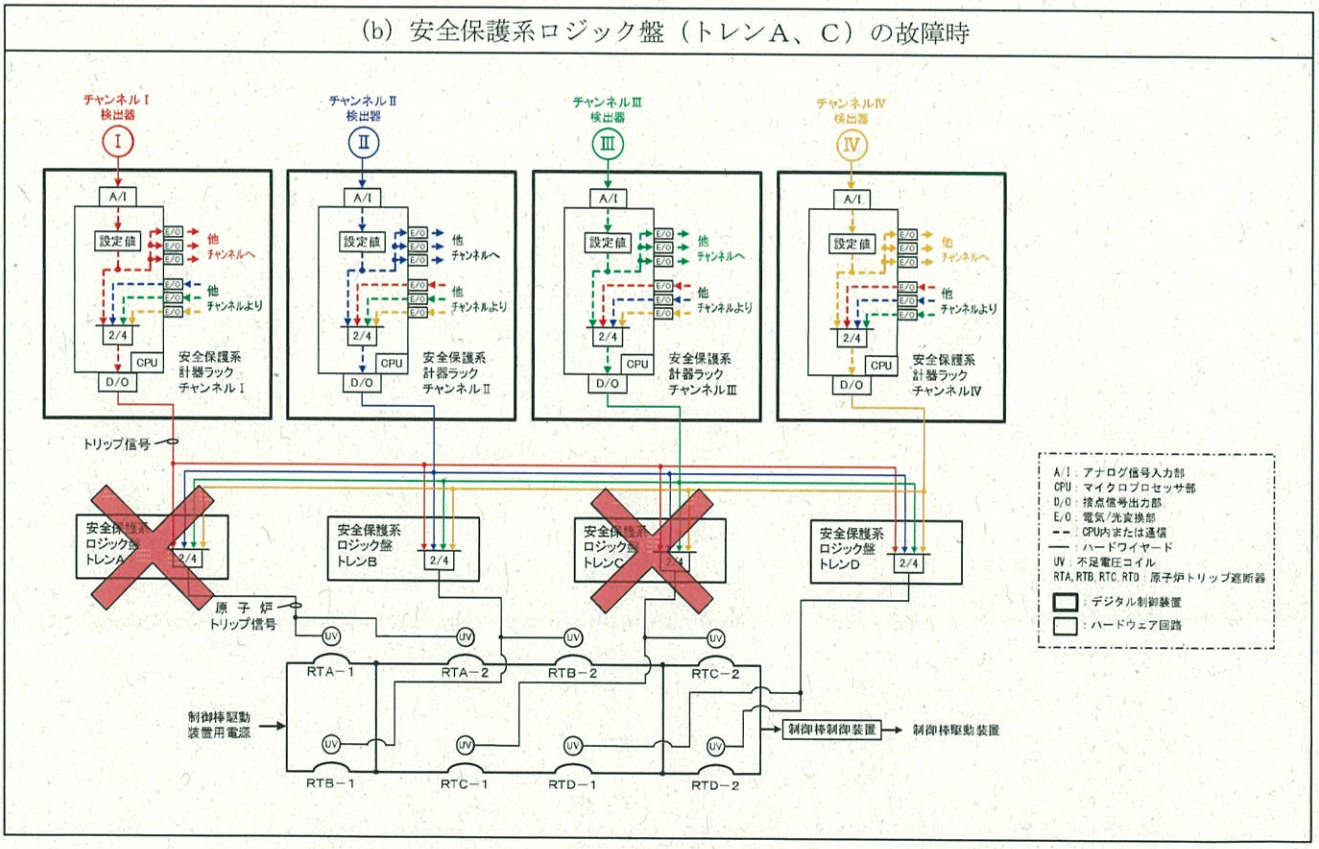
2チャンネルの計器ラックの不動作故障を想定した場合の図(a)では、健全なチャンネルⅠ及びⅢの計器ラックにおいて、チャンネルⅠ及びⅢの検出器信号が入力されることから、2/4の論理回路が成立して、作動信号を発信する。

ロジック盤では、健全なチャンネルⅠ及びⅢの計器ラックから信号分配された2チャンネルの信号によって、ロジック盤の2/4の論理回路が成立して、工学的安全施設作動信号が発信される。

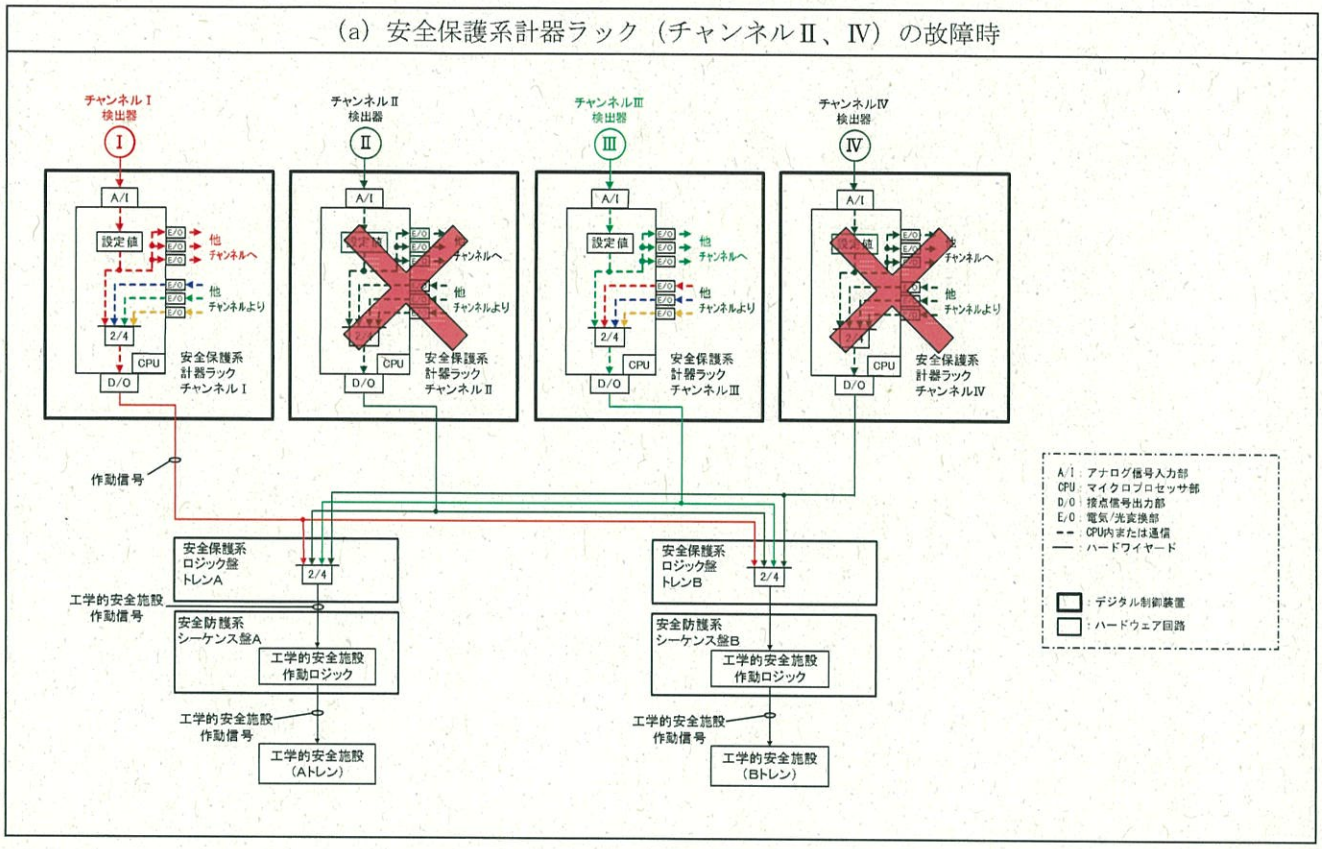
1トレンのロジック盤の不動作故障を想定した場合の図(b)では、健全なトレンBのロジック盤において、2/4の論理回路が成立して、工学的安全施設作動信号が発信される。

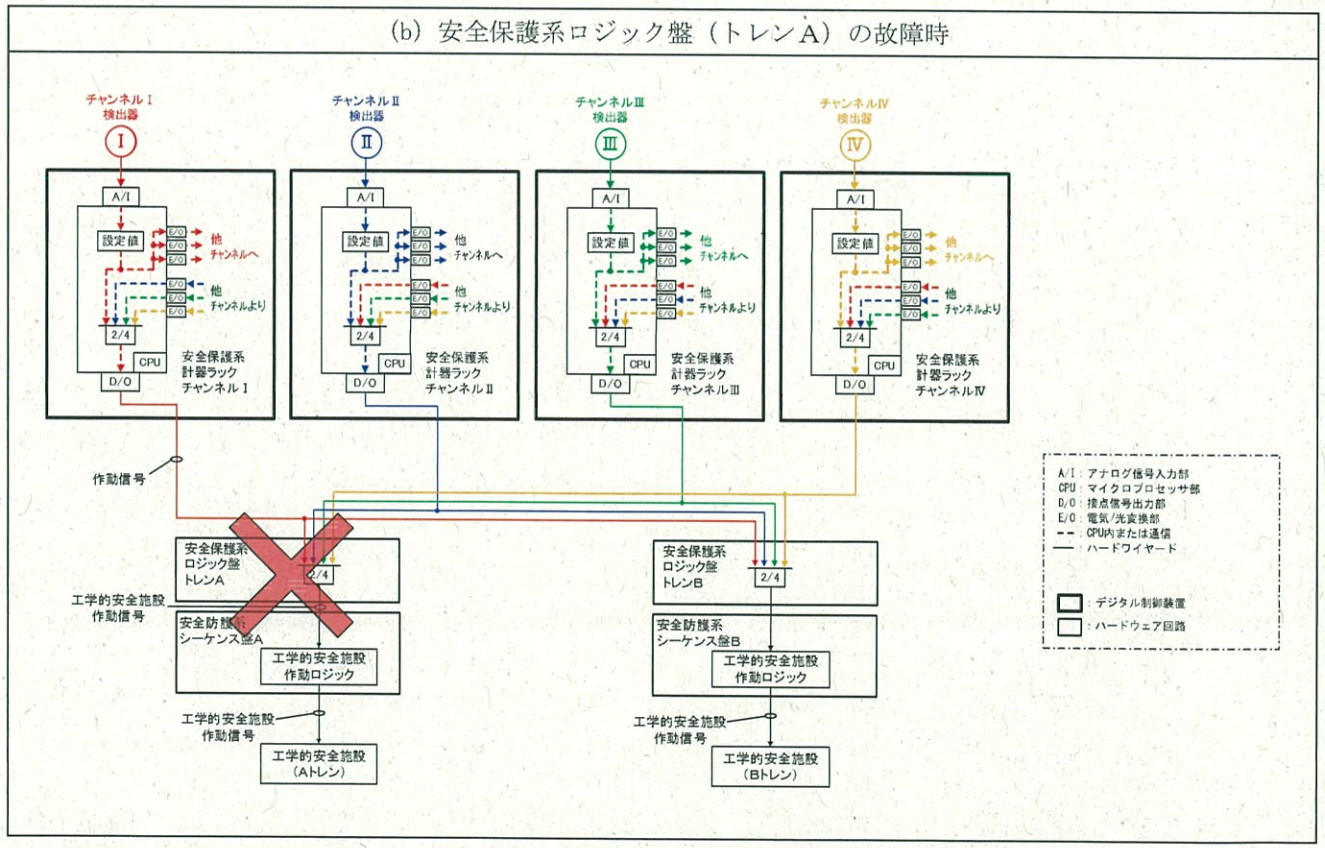
このため、ロジック盤は、安全保護機能を阻害しない。





第5図　原子炉トリップ信号の発信（故障時）





第６図　工学的安全施設作動信号の発信（故障時）

3.2 運用性の向上

3.2.1 原子炉保護設備

計器ラックの誤動作故障時において、更新後にロジック盤を設けることによって更新後にロジック盤を設けない場合に比べて、原子炉保護設備の運用性向上を図った構成とする。(更新前に対しては、同等の運用性を維持する)

計器ラックの誤動作故障時の動作状況およびバイパス後の時の状況について、更新前を第7図に、更新後ロジック盤を設ける場合を第8図に、更新後ロジック盤を設けない場合を第9図に示す。

(1) 更新前

更新前における、計器ラックの誤動作故障時及び故障チャンネルのバイパス時のプラント状態を第7図に示す。

計器ラックは、図(a)のマイクロプロセッサ部等の故障に伴う誤動作時に、故障した計器ラックからトリップ信号が発信され、すべてのロジック盤の論理回路の状態が1/3となる。

その後、故障した計器ラックを、図(b)の除外(バイパス)状態にすることによって、すべてのロジック盤の論理回路の状態は2/3の状態になり、2チャンネルのトリップ信号によって、原子炉トリップ信号を発信する状態に復帰する。

(2) 安全保護系ロジック盤を設ける場合

更新後にロジック盤を設ける場合における、計器ラックの誤動作故障時及び故障チャンネルのバイパス時のプラント状態を第8図に示す。

計器ラックは、図(a)のマイクロプロセッサ部等の故障に伴う誤動作時に、故障した計器ラックからトリップ信号が発信され、すべてのロジック盤の論理回路の状態が1/3となる。

その後、故障した計器ラックを、図(b)の除外(バイパス)状態にすることによって、すべてのロジック盤の論理回路の状態は2/3の状態になり、2チャンネルのトリップ信号によって、原子炉トリップ信号を発信する状態に復帰する。

(3) 安全保護系ロジック盤を設けない場合

更新後にロジック盤を設けない場合における、計器ラックの誤動作故障時及び故障チャンネルのバイパス時のプラント状態を第9図に示す。

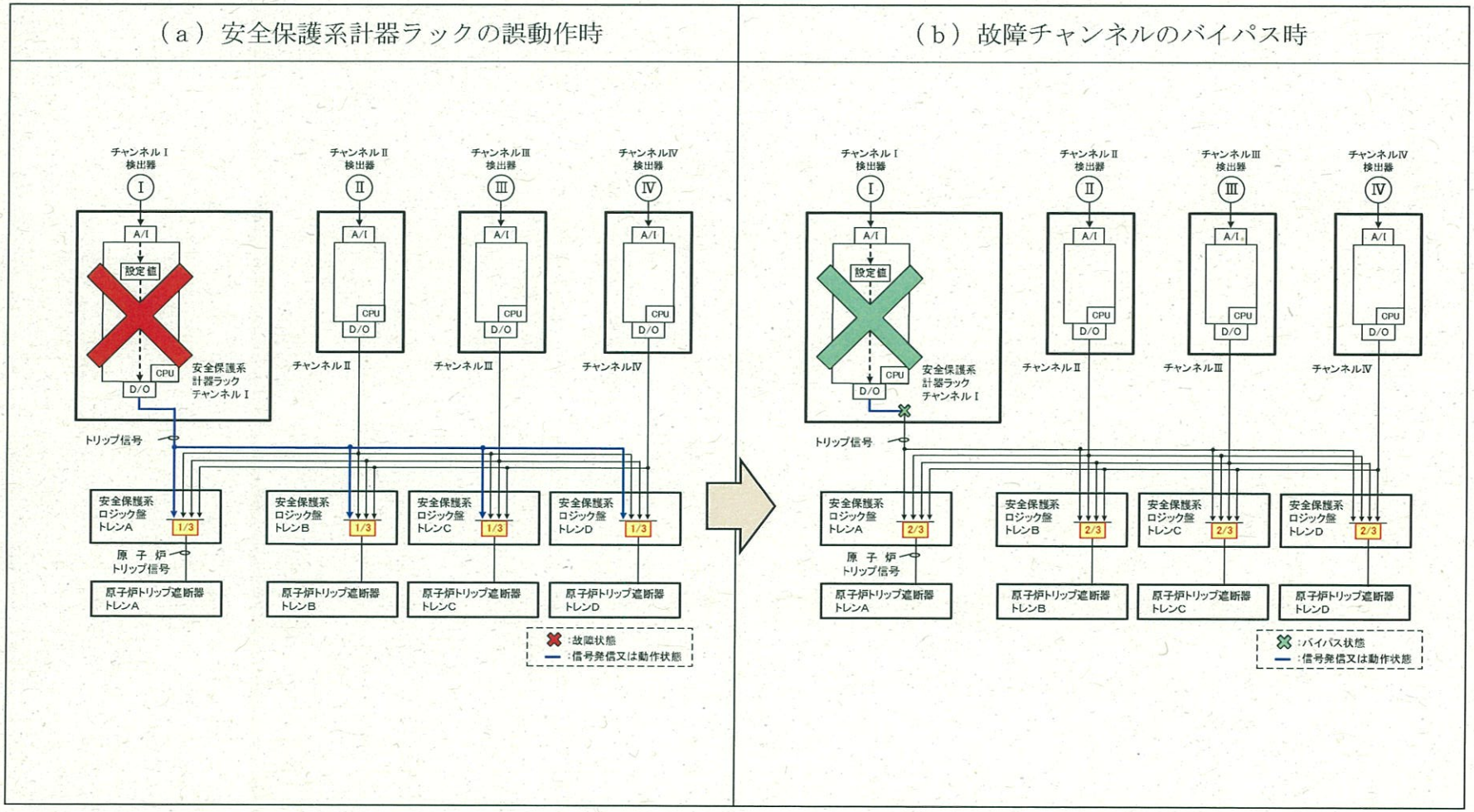
計器ラックは、図(a)のマイクロプロセッサ部等の故障に伴う誤動作時に、故障した計器ラックからトリップ信号が発信され、故障した計器ラックに対応する原子力トリップ遮断器が動作(開放)し、残り1/3で原子力トリップする状態となる。

その後、故障した計器ラックを、図(b)の除外(バイパス)状態にする場合、保安規定に、「原子炉保護系論理回路」の所要数を4系統※と定めていることから、

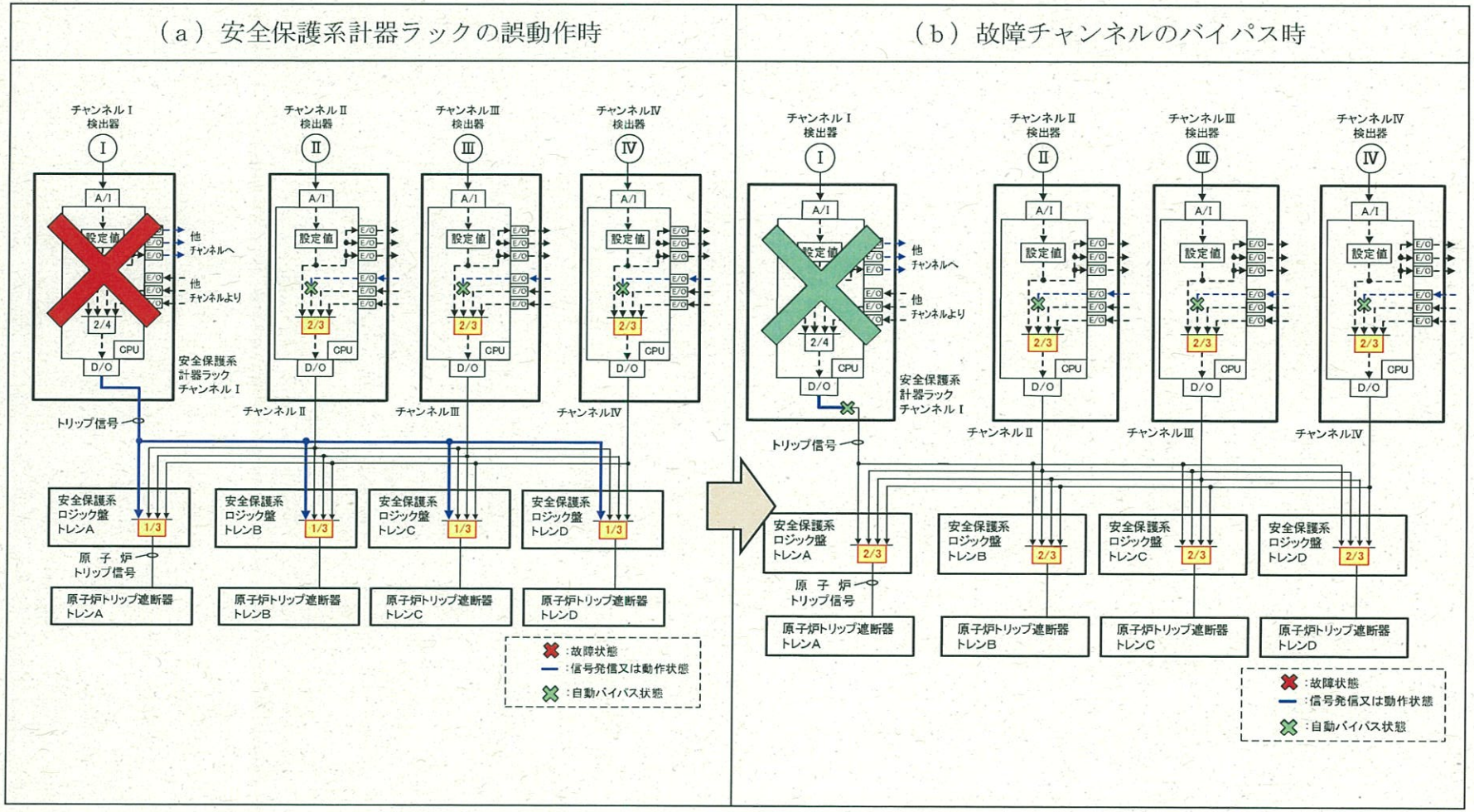
動作（開放）した原子炉トリップ遮断器を不動作（投入）に復帰させることは許容されない。

このため、故障した計器ラックの修理が完了するまでの間、残り 1/3 で原子力トリップする状態が継続し、他チャンネルの計器ラック又は他トレンの原子力トリップ遮断器の故障によって、誤トリップする。

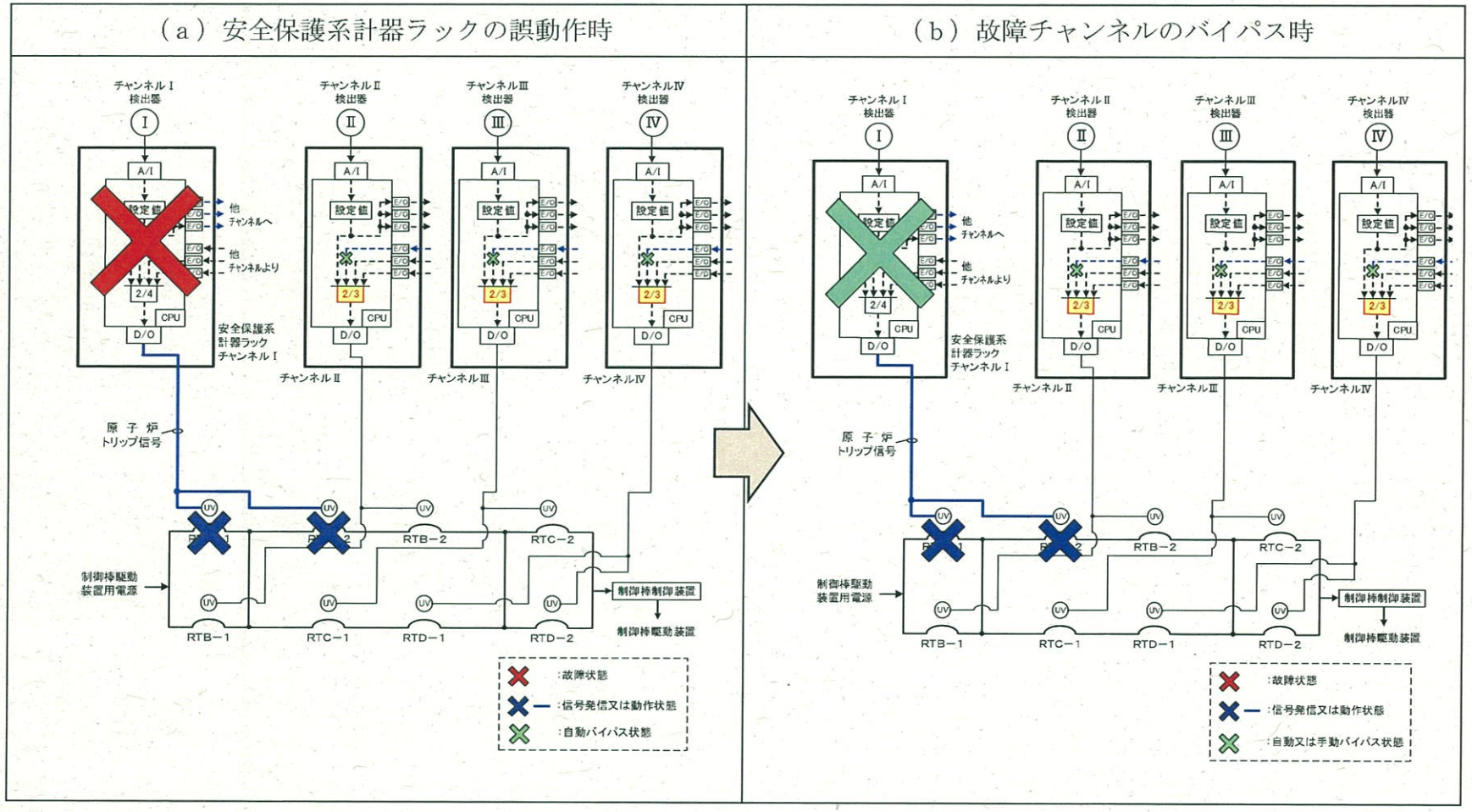
※保安規定における動作可能の考え方として、「動作信号を出力させている状態、または誤動作により動作信号を出力している状態は、動作可能とみなす。」とされている。



第７図　更新前（原子炉保護設備）



第８図　更新後、安全保護系ロジック盤を設ける場合（原子炉保護設備）



第９図　更新後、安全保護系ロジック盤を設けない場合（原子炉保護設備）

3.2.2　工学的安全施設作動設備

更新後にロジック盤を設けることによって、更新後にロジック盤を設けない場合に比べて工学的安全施設作動設備の運用性向上を図った構成とする。

3.2.2.1 不動作故障時

不動作故障時の状態について更新後にロジック盤を設ける場合と設けない場合について第10図に示す。

(1) 安全保護系ロジック盤を設ける場合

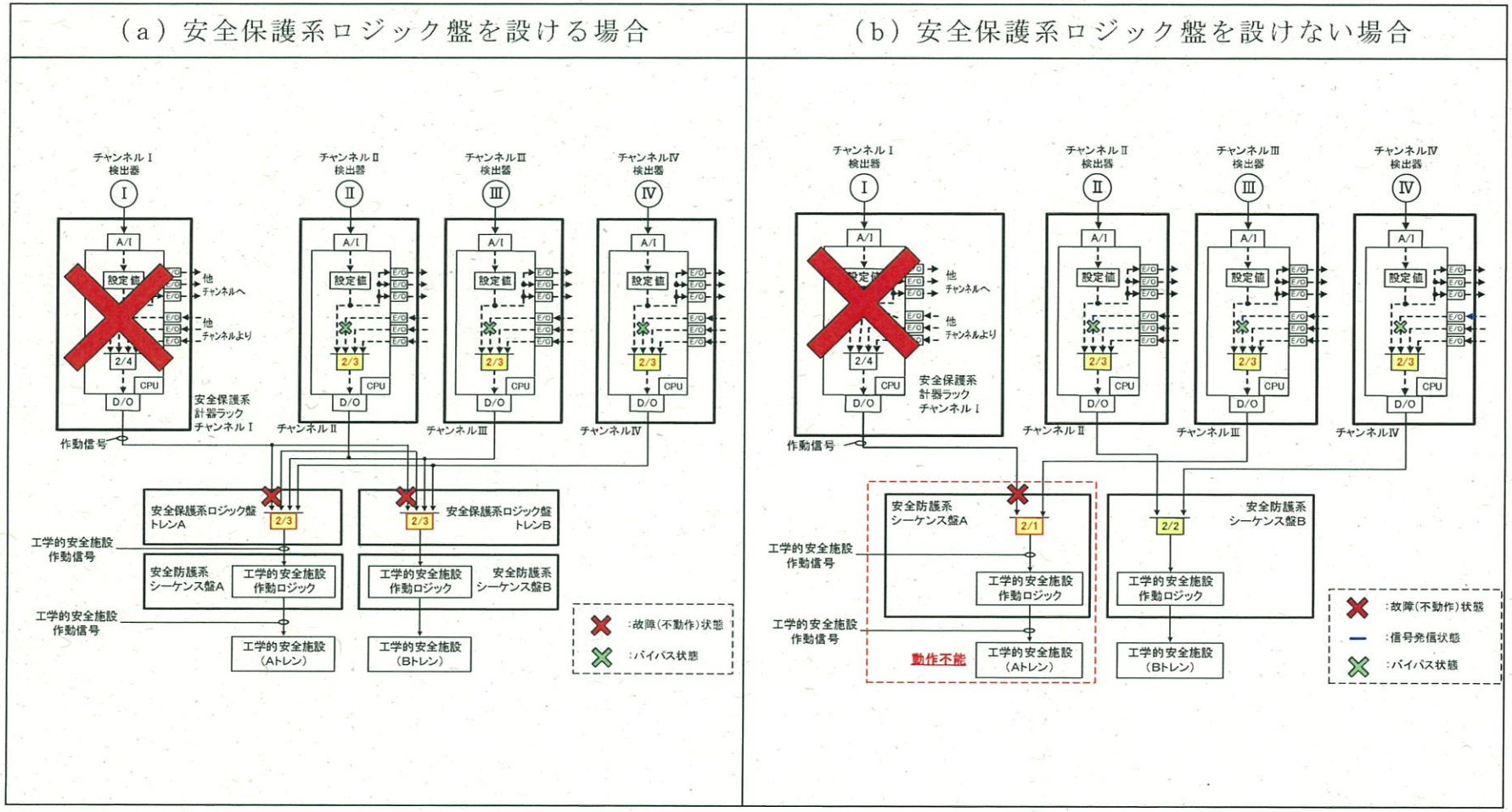
更新後にロジック盤を設ける場合における、計器ラックの不動作故障時のプラント状態を図(a)に示す。

トレンA及びBのロジック盤の論理回路の状態は2/3状態になり、残りの健全な計器ラックからの2チャンネル以上の作動信号によって、工学的安全施設作動信号を発信する。

(2) 安全保護系ロジック盤を設けない場合

更新後にロジック盤を設ける場合における、計器ラックの不動作故障時のプラント状態を図(b)に示す。

トレンA及びBの安全防護系シーケンス盤の論理回路の状態は、不動作故障した計器ラックから入力を受けるトレンでは、論理回路が成立しなくなり、当該トレンの工学的安全施設作動信号は発信しない。（例えば、チャンネルⅠの計器ラックが不動作故障した場合、トレンAの安全防護系シーケンス盤は工学的安全施設作動信号を発信できない。）



第 10 図　工学的安全施設作動設備に係る運用性の比較

3.2.2.2 誤動作故障時

(1) 安全保護系ロジック盤を設ける場合

更新後にロジック盤を設ける場合における、計器ラックの誤動作時及び故障チャンネルのバイパス時のプラント状態を第11図に示す。

計器ラックは、図(a)のマイクロプロセッサ部等の故障に、故障した計器ラックから工学的安全施設作動信号が発信され、トレンA及びBのロジック盤の論理回路の状態が1/3となる。

その後、故障した計器ラックを、図(b)の除外（バイパス）状態にすることによって、残りの健全な計器ラック及びトレンA及びBのロジック盤の論理回路の状態は2/3の状態になり、2チャンネルの作動信号によって、工学的安全施設作動信号を発信する状態に復帰する。

(2) 安全保護系ロジック盤を設けない場合

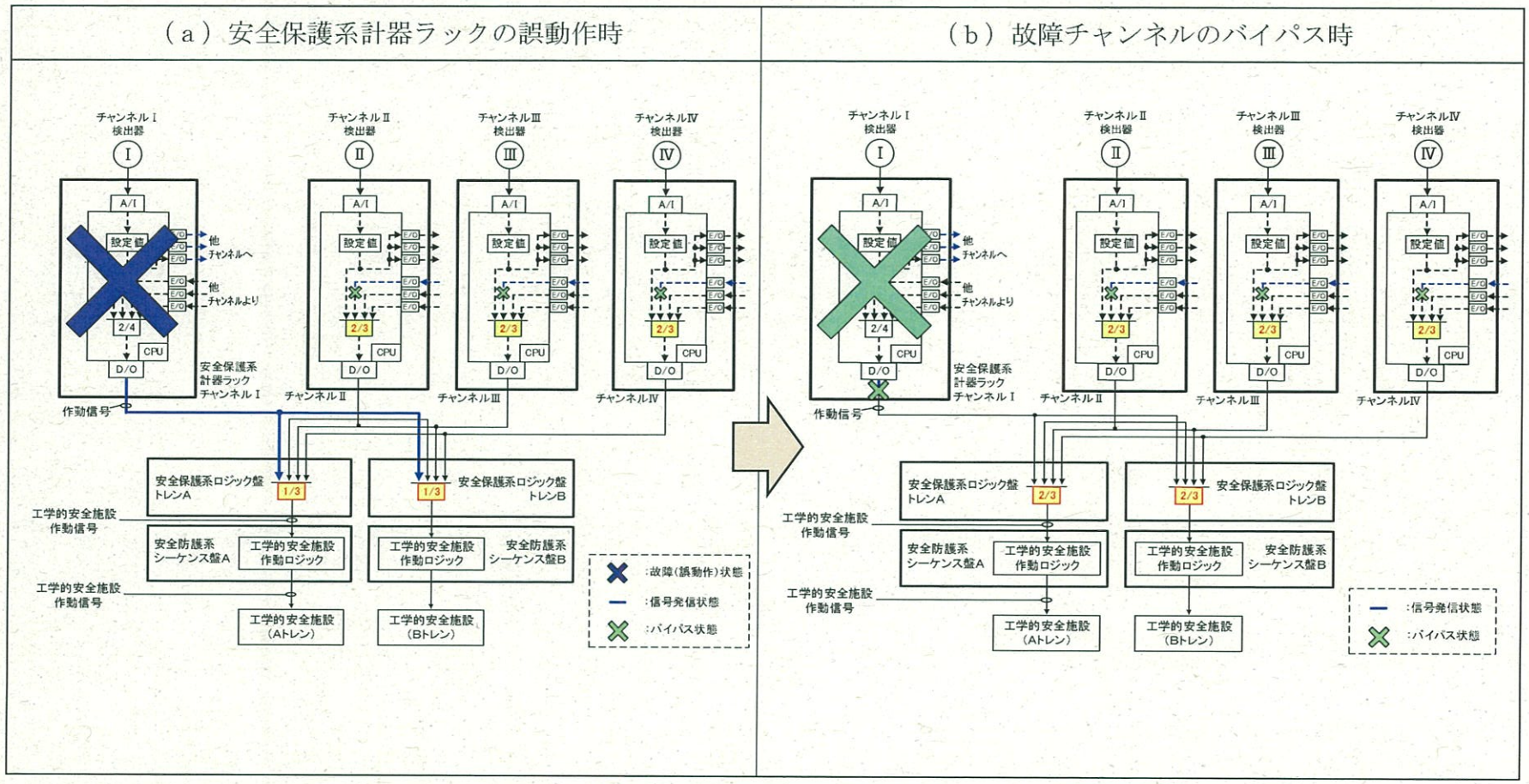
更新後にロジック盤を設けない場合における、計器ラックの誤動作時及び故障チャンネルのバイパス時のプラント状態を第12図に示す。

計器ラックは、マイクロプロセッサ部等の故障に伴う誤動作時に、故障した計器ラックから作動信号が発信され、故障した計器ラックに対応するトレンの安全防護系シーケンス盤は残り1チャンネルで誤作動する状態になる。

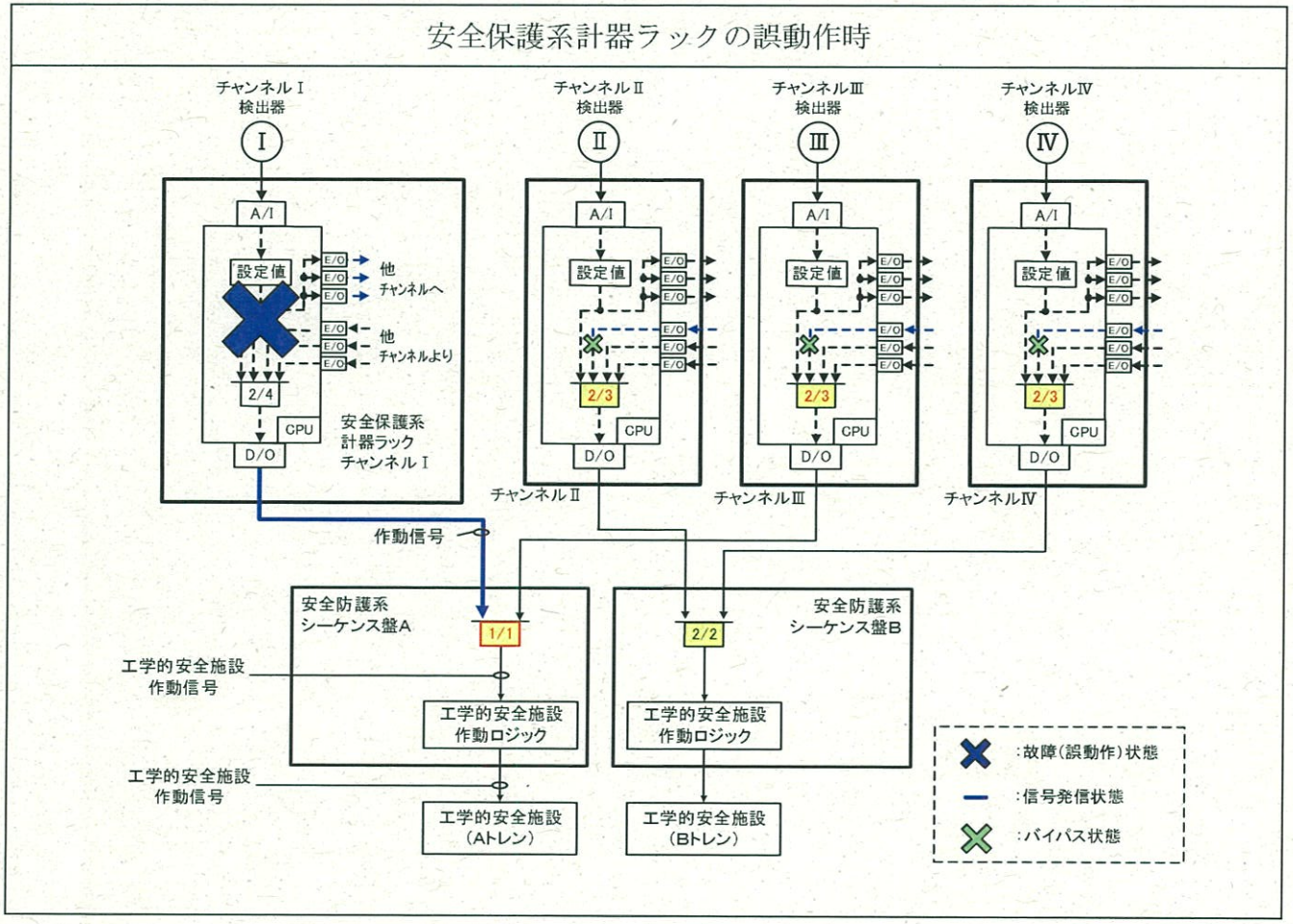
保安規定に、「非常用炉心冷却系作動論理回路」等の所要数を2系統※と定めていることから、故障した計器ラックから発信している作動信号を除外（バイパス）することは許容されない。

このため、故障した計器ラックの修理が完了するまでの間、残り1チャンネルで工学的安全施設作動信号が作動する状態が継続し、他チャンネルの計器ラックの故障によって、誤作動する。

※保安規定における動作可能の考え方として、「動作信号を出力させている状態、または誤動作により動作信号を出力している状態は、動作可能とみなす。」とされている。



第 11 図　更新後、安全保護系ロジック盤を設ける場合（工学的安全施設作動設備）



第 12 図　更新後、安全保護系ロジック盤を設けない場合（工学的安全施設作動設備）

4. 定期点検（サーベイランス）時における運用性向上

原子炉保護設備に係る定期点検（サーベイランス）時において、更新後は更新前に比べて工学的安全施設作動設備の運用性が向上する。

更新前及び更新後の設備構成における定期点検（サーベイランス）時の状態を第13図に示す。

(1) 更新前における定期点検（サーベイランス）時の状態

更新前では、原子炉保護設備に係る定期点検（サーベイランス）の実施時、図(a)に示す状態になる。

原子炉保護設備に係る定期点検（サーベイランス）では、原子炉保護設備で原子炉トリップ信号が発信されることを確認する必要があるが、原子炉トリップ信号の発信によって、原子炉トリップ遮断器が実動作（開放）することを防ぐために、ロジック盤からの出力信号をバイパスする。

この際、更新前では、原子炉トリップ信号に加えて、工学的安全施設作動信号もバイパスされる設備構成となっている。

安全防護系シーケンス盤は、工学的安全施設作動信号の 2/2 で工学的安全施設を作動させる回路となっているため、出力信号をバイパスしたロジック盤に対応するトレンの安全防護系シーケンス盤は、作動することができない。

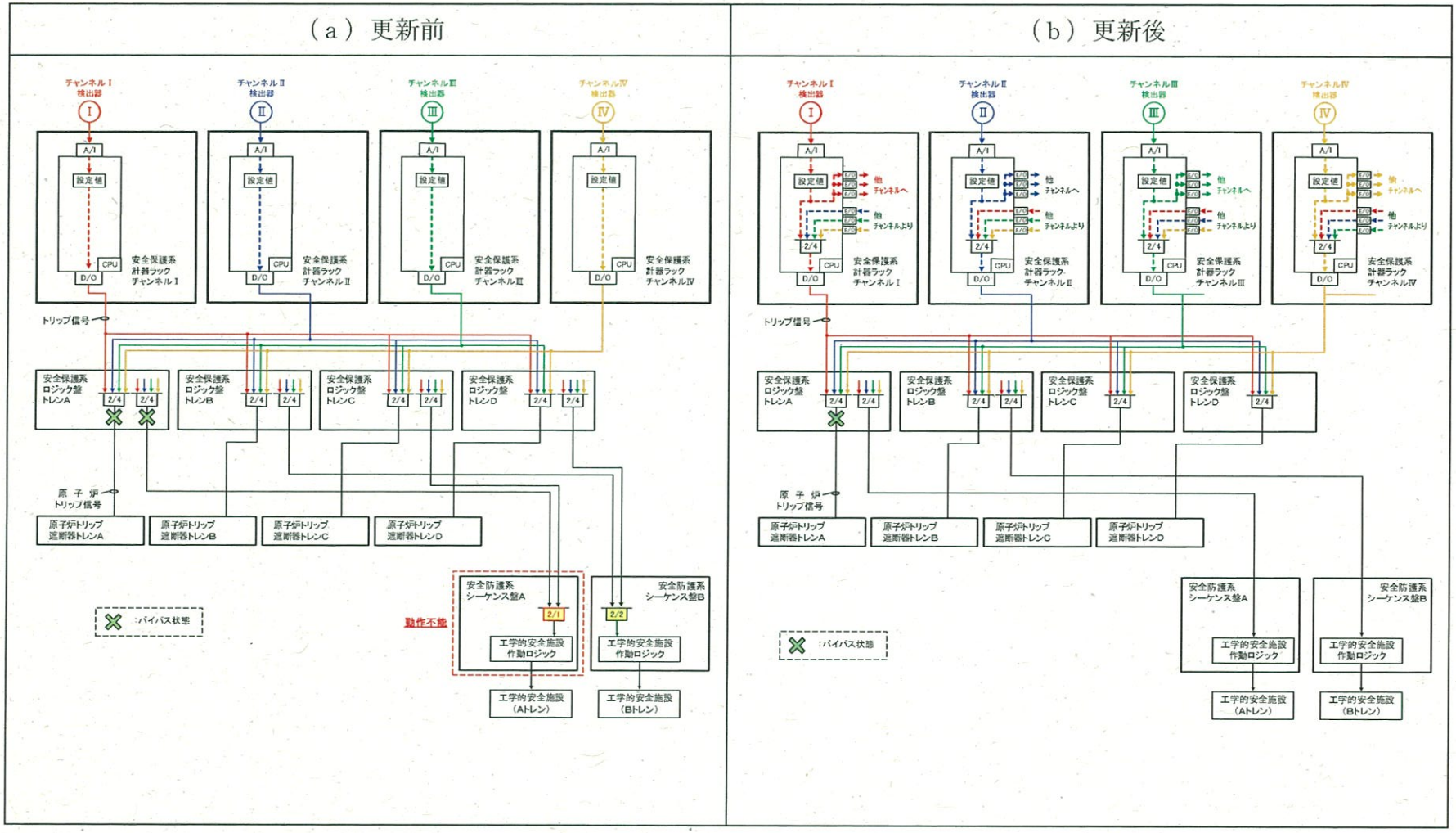
この理由から、保安規定には、非常用炉心冷却系作動論理回路等の工学的安全施設作動信号に係る機能の所要数について、「原子炉保護系論理回路の機能検査時においては、残り１系統が動作可能であることを条件に、２時間に限り、１系統をバイパスすることができる。この場合、バイパスした系統を動作不能とはみなさない。」と定めているが、この間、動作可能な工学的安全施設作動信号は１トレンになる。

(2) 更新後の設備構成における定期点検（サーベイランス）時の状態

更新後の設備構成では、原子炉保護設備に係る定期点検（サーベイランス）時は、図(b)に示す状態になる。

取替え後のロジック盤では、原子炉保護設備に係る定期点検（サーベイランス）時におけるロジック盤のバイパス時に、原子炉トリップ信号の出力信号のみがバイパスされ、工学的安全施設作動信号の出力信号をバイパスしない設計に変更する。

このため、原子炉保護設備に係る定期点検（サーベイランス）時においても、非常用炉心冷却系作動論理回路等の工学的安全施設作動信号に係る機能について、所要数を満足することができ、運用性の向上が図れる。



第 13 図　原子炉保護設備に係る定期点検（サーベイランス）時の状態

5. まとめ

○更新後におけるロジック盤は、原子炉トリップ信号及び工学的安全施設作動信号の発信を阻害せず、安全保護機能に悪影響を与えない。

○更新後においてロジック盤を設けた場合とロジック盤を設けない場合を比較すると、ロジック盤を設けることによって下記の運用性向上が図れる。

（1）原子炉保護設備

✓ 計器ラックの誤動作故障時に、2チャンネル以上の検出器からの信号発信で原子炉トリップする通常状態に復帰することができる。（更新前と同等の運用性）

（2）工学的安全施設作動設備

✓ 計器ラックの不動作故障時に、2トレンの工学的安全施設が作動できる通常状態を維持できる。

✓ 計器ラックの誤動作故障時に、2チャンネル以上の検出器からの信号発信で、2トレンの工学的安全施設が作動できる通常状態に復帰することができる。

○更新前は、原子炉保護系論理回路の定期点検（サーベイランス）時に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、更新後は2トレンが動作できる状態を維持でき、運用性が向上する。