伊方発電所保安規定審査資料	
資料番号	TS(76)-04(r4)

原子炉保護系論理回路の機能確認時の運用について

令和３年８月

四国電力株式会社

目　　次

１．伊方３号炉ロジック盤取替工事の設計及び工事計画認可申請内容

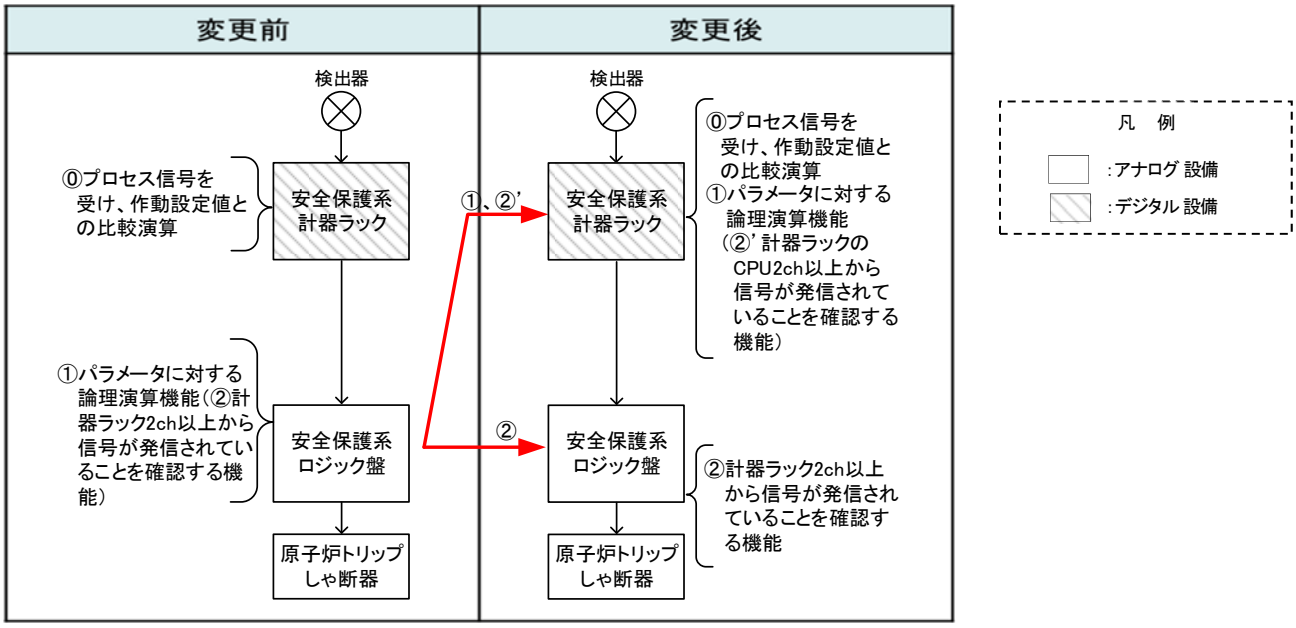
設備の保守性向上の観点からロジック盤を取替えることとし、取替に伴い、令和２年９月１０日に設計及び工事計画認可申請(以下「設工認申請」という。)を行い、令和３年５月２７日に認可された。

＜申請内容＞

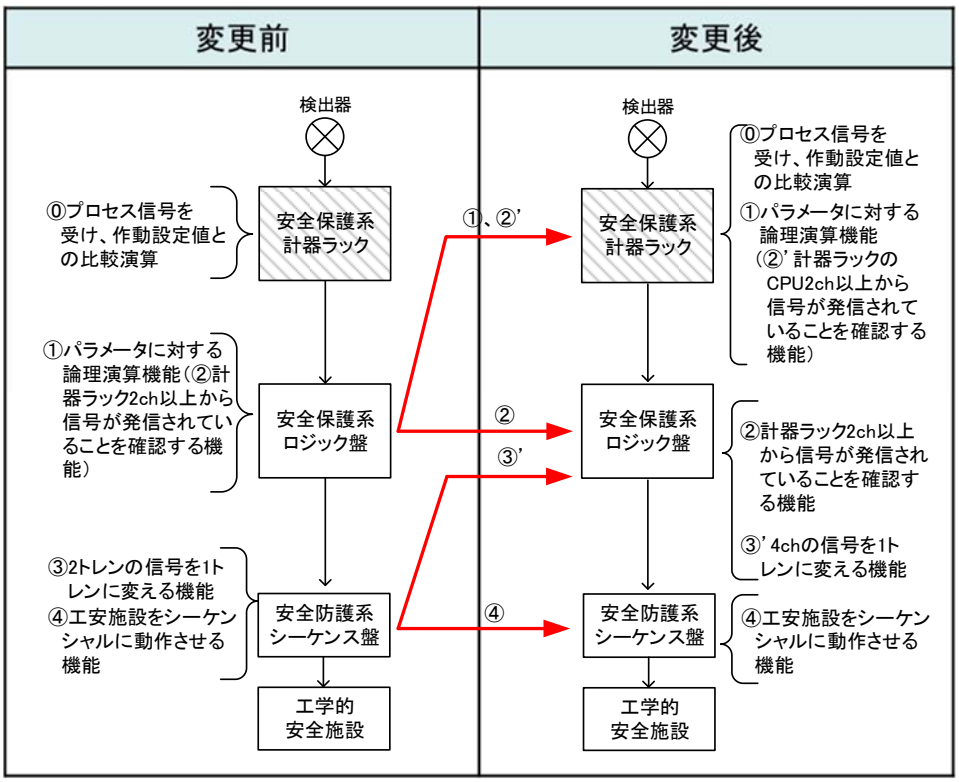
✓ ロジック盤が担っているパラメータに対する論理演算機能（以下、「論理演算機能」という。）について、既設のデジタル制御装置である安全保護系計器ラックのソフトウェアにて実現する。

✓ 安全保護系計器ラックの故障が生じた場合においても安全保護系の機能を確保するためにリレー回路（以下、「保障回路」という）を備えたロジック盤を設ける。

ａ．原子炉停止系



ｂ．工学的安全施設作動系



２．ロジック盤取替に伴う工事内容

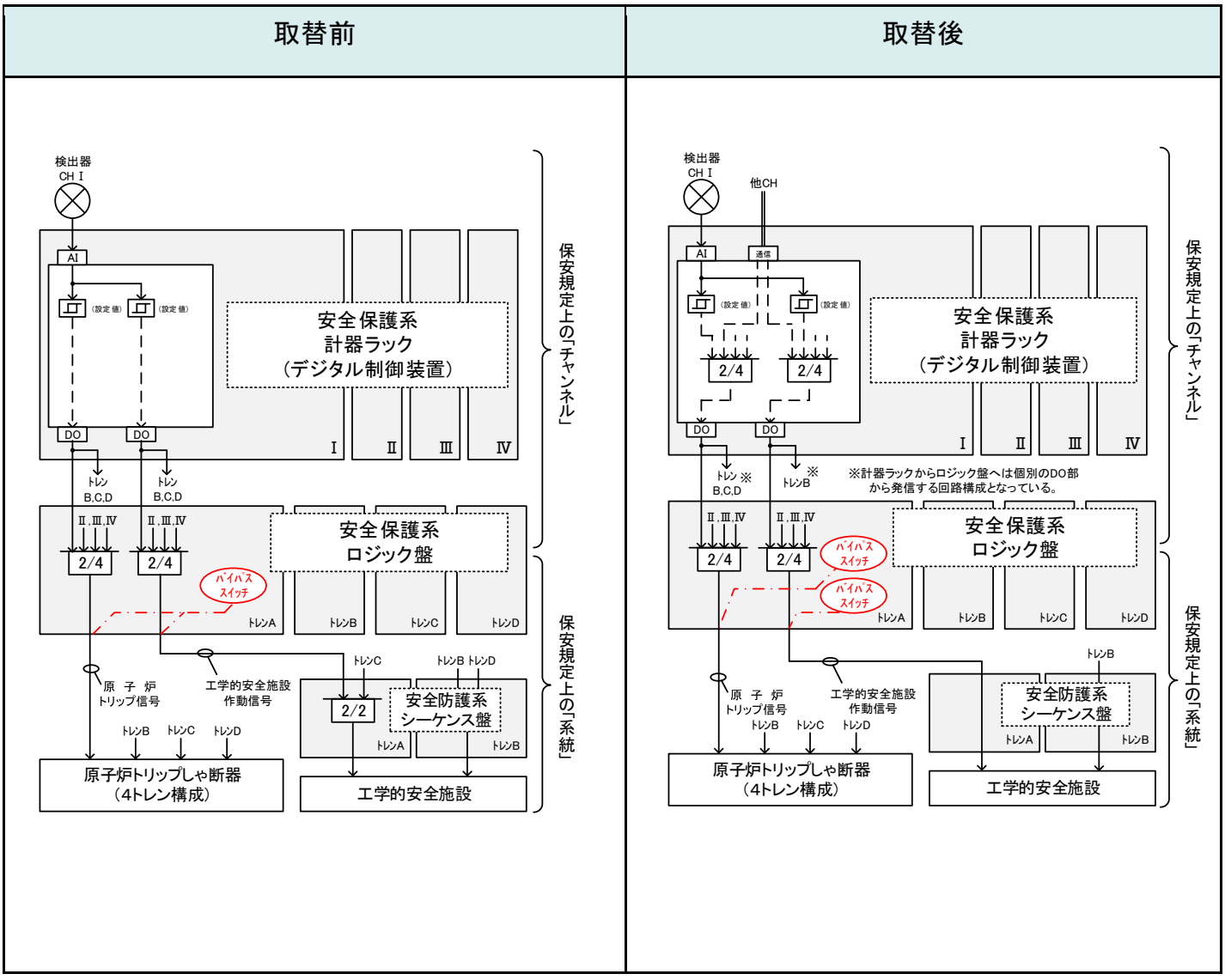
１．項の設工認申請の工事内容に合わせて、ロジック盤内のバイパス回路の設備構成を以下の通り変更する。

ロジック盤には、原子炉保護系論理回路の機能確認時に原子炉トリップ信号(テスト信号)の発信によって原子炉トリップしゃ断器が実動作することを防ぐため、原子炉トリップしゃ断器への原子炉トリップ信号を除外とするバイパススイッチを設置している。

ロジック盤取替前は、原子炉トリップ信号と工学的安全施設作動信号のバイパス回路が共通であったため、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一括でバイパスされる設備構成となっていた。

ロジック盤取替後は、原子炉トリップ信号と工学的安全施設作動信号それぞれにバイパス回路を個別に設けることで、原子炉トリップ信号と工学的安全施設作動信号の各出力信号を個別にバイパスできる設備構成とする。

なお、これまで一括でバイパスされる設備構成は、もともとのメーカの標準設計であった。



３．保安規定変更における考え方

（１）現状の記載

運転中に原子炉トリップ信号を発信させるために必要なパラメータに対する論理演算機能の健全性を確認するため、原子炉保護系論理回路の機能を確認※する(別紙－１)。その際、原子炉トリップ信号(テスト信号)の発信によって原子炉トリップしゃ断器が実動作することを防ぐため、試験対象のロジック盤の１系統をバイパスする必要があった。

このバイパスによって、原子炉トリップ信号以外に、工学的安全施設作動信号も発信することが不可能となることから、バイパスされたロジック盤から工学的安全施設作動信号を受け取る構成となっている安全防護系シーケンス盤については、工学的安全施設の補機等を起動させる論理回路（ＡＮＤ回路）が成立しなくなり、１系統の機能を満足しないことになる。

このため、工学的安全施設等作動計装の作動論理回路の所要数について、残り１系統が動作可能であることを条件として点検を行うよう、「原子炉保護系論理回路の機能確認時においては、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。」の注釈を付記している。

※保安規定における原子炉保護系論理回路の機能確認には、「定期事業者検査時の機能確認」と「１カ月に１回の機能確認」があり、信号をバイパスさせるのは「１カ月に１回の機能確認（以下、「定期点検」という。)」のみである。

（２）変更理由

ロジック盤取替に伴い、定期点検時に原子炉保護系論理回路と工学的安全施設等作動計装を一括でバイパスされる設備構成から、個別にバイパスできる設備構成に変更することにより、定期点検時に工学的安全施設等作動計装の２系統が動作できる状態を維持できることから、設備と運用の整合を図る。(別紙－２)

（３）変更箇所

第３３条(計測および制御設備) 第３項の表３３－３工学的安全施設等作動計装について、「原子炉保護系論理回路の機能確認時においては、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。」の注釈を削除する。

削除する注釈は、下記の論理回路に関する箇所であり、別紙－３に「非常用炉心冷却系作動論理回路」を例にとって変更前後を示す。

・非常用炉心冷却系作動論理回路
・原子炉格納容器スプレイ系作動論理回路
・格納容器隔離Ａ作動論理回路
・格納容器隔離Ｂ作動論理回路
・格納容器隔離Ａと 6.6kV 非常用母線電圧低の一致による隔離作動論理回路
・格納容器換気系隔離作動論理回路
・主蒸気ライン隔離作動論理回路
・主給水隔離作動論理回路

原子炉保護系論理回路の定期点検の内容について

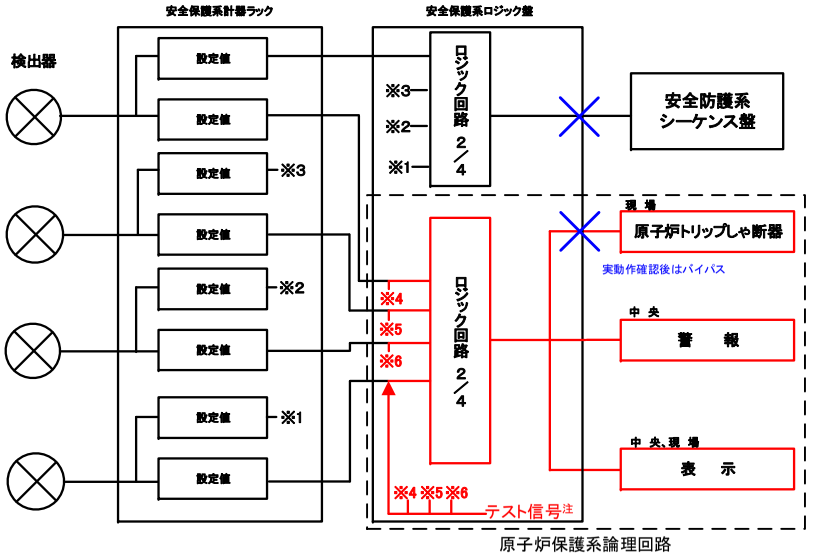
目的

原子炉保護系論理回路の機能を確認するため、以下の動作確認により健全性を確認する。（１回／１カ月）

- ✓ 原子炉トリップしゃ断器の実動作
- ✓ 警報、表示の発信

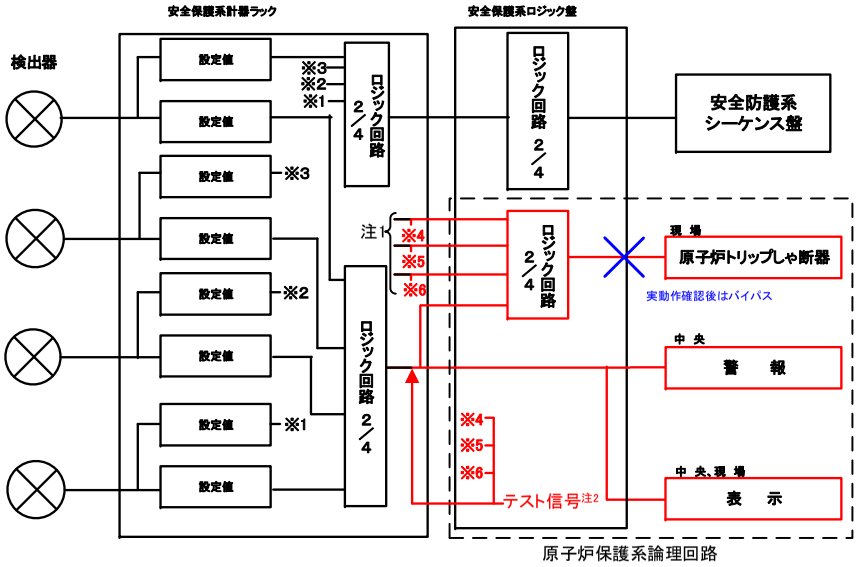
点検内容

- ✓ 取替前の定期点検は、論理演算機能の上段へテスト信号を模擬入力し、ロジック回路と原子炉トリップしゃ断器が動作することを確認する。
- ✓ 論理演算機能の上段へ入力するテスト信号は、２１種類ある。
- ✓ 原子炉トリップしゃ断器の健全性を確認するため、代表１種類のテスト信号により原子炉トリップしゃ断器を実動作させる。
- ✓ 原子炉トリップしゃ断器の実動作を確認後は、残り２０種類のテスト信号による原子炉保護系論理回路の健全性を警報、表示により確認する。この際、原子炉トリップしゃ断器の健全性は既に確認していることから、原子炉トリップ信号の発信によって原子炉トリップしゃ断器が実動作することを防ぐため、原子炉トリップしゃ断器への原子炉トリップ信号をバイパスし、テスト信号(残り２０種類)によるロジック回路の健全性を確認する。
- ✓ 取替後の定期点検において、変更となる内容は、審査資料 TS(76)-05-05 にて示す。



注:定期点検では、4つの入力箇所に対して、順次2つのテスト信号を模擬入力する。

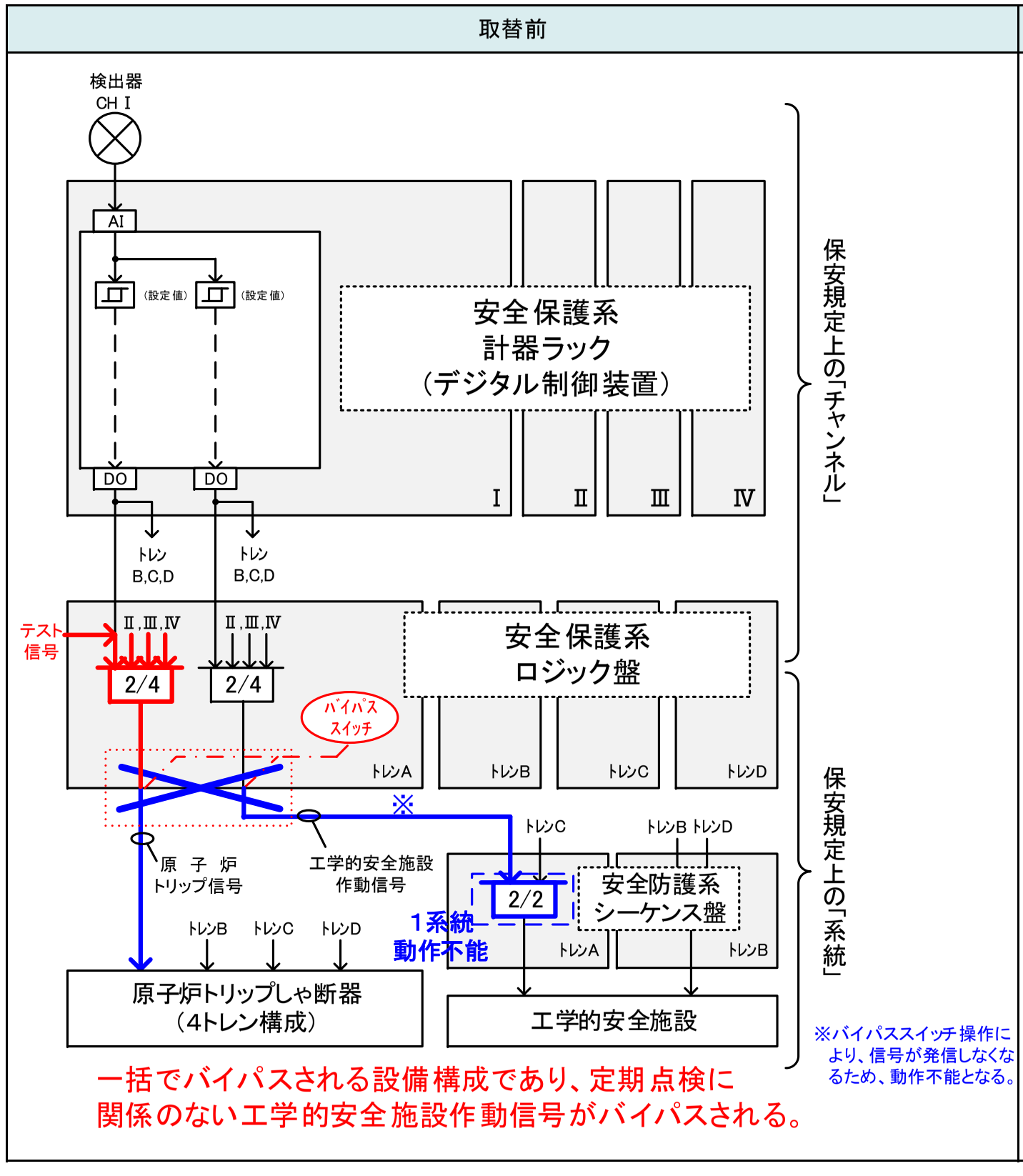
図１.取替後の回路イメージ

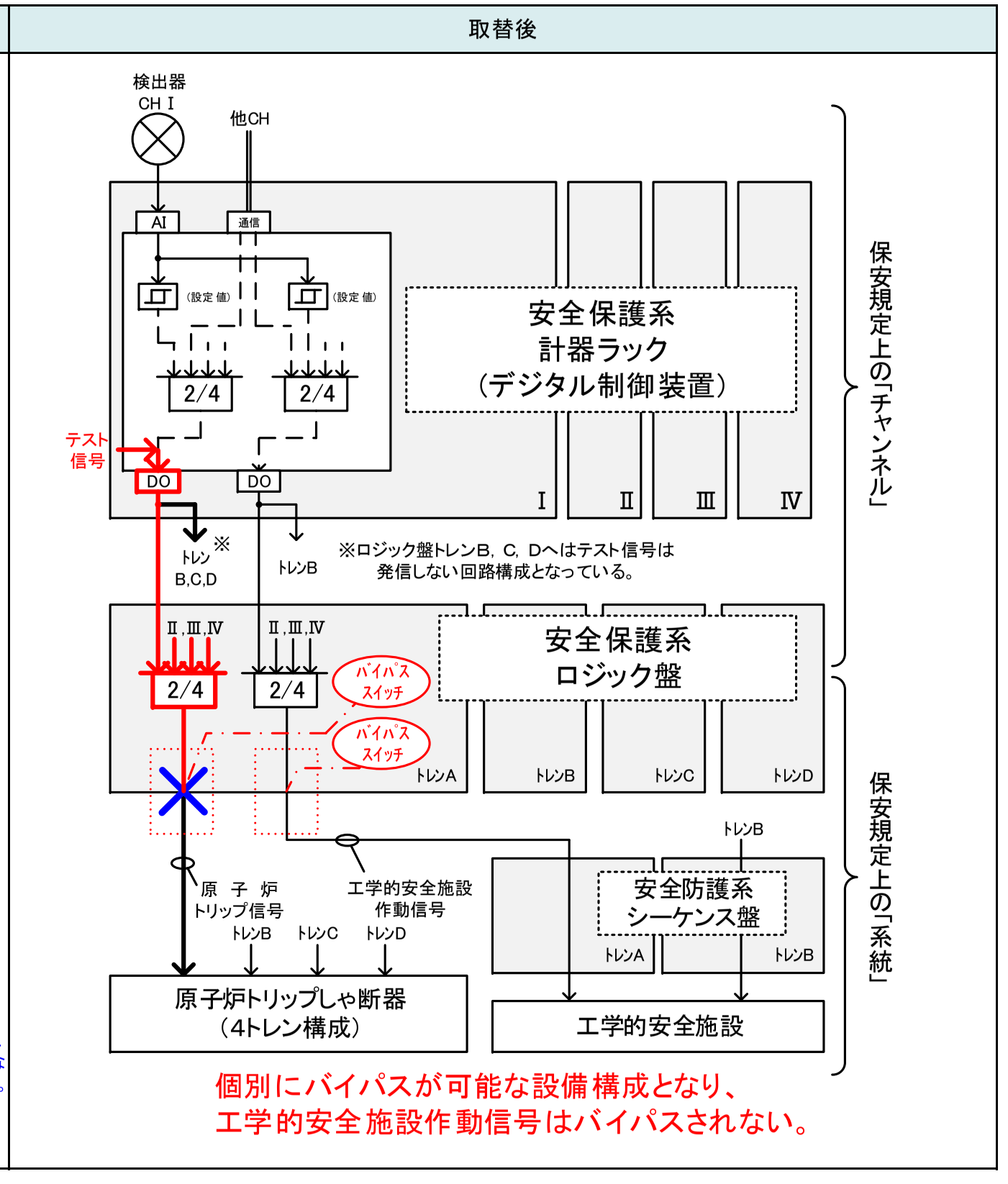


注1:安全保護系計器ラックの他3チャンネルからの信号がある。
注2:定期点検では、4つの入力箇所に対して、順次2つのテスト信号を模擬入力する。

図２.取替後の回路イメージ

- ✓ 原子炉保護系論理回路の定期点検時において、ロジック盤取替前は原子炉トリップ信号をバイパスしたことにより、工学的安全施設作動信号も一括でバイパスされるため、定期点検時においては、工学的安全施設等作動計装の２系統のうち１系統が動作不能となることから、残り１系統が動作可能であることを条件に、２時間に限り定期点検のための１系統動作不能が許容されていた。
- ✓ ロジック盤取替後は原子炉トリップ信号と工学的安全施設作動信号の各出力信号を個別にバイパスでき、工学的安全施設作動信号の論理回路がバイパスされないため、定期点検時においても工学的安全施設等作動計装の２系統が動作できる状態を維持できる。





変　　更　　前

表33－３　工学的安全施設等作動計装

機　　能	設定値	適用モード	所要チャンネル・系統数	所要チャンネル条件
１．非常用炉心冷却系作動				
ａ．非常用炉心冷却系作動論理回路	－	モード１，２，３および４	２系統※24	A. １系統が動作不能である場合 B. 条件Ａの措置を完了時間内に達成できない場合
ｂ．手動起動	－	モード１，２，３および４	２	A. １チャンネルが動作不能である場合 B. 条件Ａの措置を完了時間内に達成できない場合
ｃ．格納容器圧力高（高１）	0.034MPa[gage]以下	モード１，２および３	４※25	A. １チャンネル（バイパスしたチャンネルを除く）が動作不能である場合 B. 条件Ａの措置を完了時間内に達成できない場合
ｄ．原子炉圧力異常低	11.36MPa[gage]以上	モード１および２（P-6以上）	４※25	A. １チャンネル（バイパスしたチャンネルを除く）が動作不能である場合 B. 条件Ａの措置を完了時間内に達成できない場合

※24：原子炉保護系論理回路の機能確認時においては，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。
※25：残り３チャンネルが動作可能であることを条件に，１チャンネルをバイパスすることができる。この場合，バイパスしたチャンネルを動作不能とはみなさない。
※26：残り３チャンネルが動作可能であることを条件に，１チャンネルをバイパスする措置を行うことができる。

変　　更　　後

表33－３　工学的安全施設等作動計装

機　　能	設定値	適用モード	所要チャンネル・系統数	所要チャンネル条件
１．非常用炉心冷却系作動				
ａ．非常用炉心冷却系作動論理回路	－	モード１，２，３および４	２系統	削除 A. １系統が動作不能である場合 B. 条件Ａの措置を完了時間内に達成できない場合
ｂ．手動起動	－	モード１，２，３および４	２	A. １チャンネルが動作不能である場合 B. 条件Ａの措置を完了時間内に達成できない場合
ｃ．格納容器圧力高（高１）	0.034MPa[gage]以下	モード１，２および３	４※24	A. １チャンネル（バイパスしたチャンネルを除く）が動作不能である場合 B. 条件Ａの措置を完了時間内に達成できない場合
ｄ．原子炉圧力異常低	11.36MPa[gage]以上	モード１および２（P-6以上）	４※24	A. １チャンネル（バイパスしたチャンネルを除く）が動作不能である場合 B. 条件Ａの措置を完了時間内に達成できない場合

削除

※24：残り３チャンネルが動作可能であることを条件に，１チャンネルをバイパスすることができる。この場合，バイパスしたチャンネルを動作不能とはみなさない。
※25：残り３チャンネルが動作可能であることを条件に，１チャンネルをバイパスする措置を行うことができる。

伊方発電所保安規定審査資料	
資料番号	TS(76)-05-04(r2)

ロジック盤取替工事による
保安規定表８４－１６への影響について

令和３年８月

四国電力株式会社

目　　次

１．保安規定第８４条表８４－１６の規定について

重大事故等発生時において、炉心損傷防止対策及び格納容器破損防止対策を実施するために、発電用原子炉施設の状態を把握するため、当該重大事故等発生時に監視することが必要なパラメータを「主要パラメータ」、主要パラメータを計測することが困難となった場合において、主要パラメータを推定するために必要なパラメータを「代替パラメータ」として、保安規定第８４条表８４－１６に規定している。

保安規定第８４条表８４－１６に規定している計測設備の一部は、設計基準事故対処設備（以下、「ＤＢ設備」という。）と重大事故等対処設備（以下、「ＳＡ設備」という。）を兼用している。検出器においては、主要パラメータ「加圧器水位」を例にとると、ＤＢ設備（保安規定第３３条表３３－２）における保安規定の所要チャンネル数は４チャンネルを、ＳＡ設備（保安規定第８４条表８４－１６）における保安規定の所要チャンネル数は１チャンネルを規定している。

○保安規定（抜粋）

表８４－１６　計装設備

８４－１６－１　計測設備（例：主要パラメータ「加圧器水位」）

分類	機能		所要チャンネル数	適用モード	所要チャンネル数を満足できない場合の措置		
	主要パラメータ	代替パラメータ			条件	措置	完了時間
原子炉容器内の水位	加圧器水位	①原子炉容器水位 ②１次冷却材圧力 および １次冷却材高温側温度（広域）	１	モード１，２，３，４，５および６	A. 主要パラメータを計測する計器すべてが動作不能である場合	A.1 当直長は，代替パラメータが動作可能であることを確認する。 および A.2 計装計画課長は，当該計器が故障状態であることが運転員に明確に分かるような措置を講じる。 および A.3 計装計画課長は，当該計器を動作可能な状態にする。	速やかに 速やかに 30 日
					B. 代替パラメータを計測する計器すべてが動作不能である場合	B.1 当直長は，主要パラメータが動作可能であることを確認する。 および B.2 計装計画課長は，当該計器が故障状態であることが運転員に明確に分かるような措置を講じる。 および B.3 計装計画課長は，当該計器を動作可能な状態にする。	速やかに 速やかに 30 日
					C. １つの機能を確認するすべての計器が動作不能である場合	C.1 計装計画課長は，当該機能の主要パラメータまたは代替パラメータを１手段以上動作可能な状態にする。	72 時間
					D. モード１，２，３および４において条件Ａ，ＢまたはＣの措置を完了時間内に達成できない場合	D.1 当直長は，モード３にする。 および D.2 当直長は，モード５にする。	12 時間 56 時間

２．ロジック盤取替工事による保安規定第８４条表８４－１６への影響について

主要パラメータ「加圧器水位」を例にとり、ロジック盤取替前後におけるＳＡ設備および工事の範囲を確認し、保安規定への変更有無を検討した。

２．１　ＳＡ設備の範囲

・検出器～【計器ラック】～A/Ｉ～ＣＰＵ～【計器ラック】～指示計

※【　】内は経由場所を示す。

２．２　ロジック盤取替工事の範囲

ロジック盤取替工事の範囲は安全保護系計器ラック内のＣＰＵ設定値より下流の部分になり、ＳＡ時に用いる指示計による指示機能（以下、「指示機能」という。）はロジック盤取替工事の範囲に含まれないことから、ロジック盤取替工事において指示機能の変更はない。

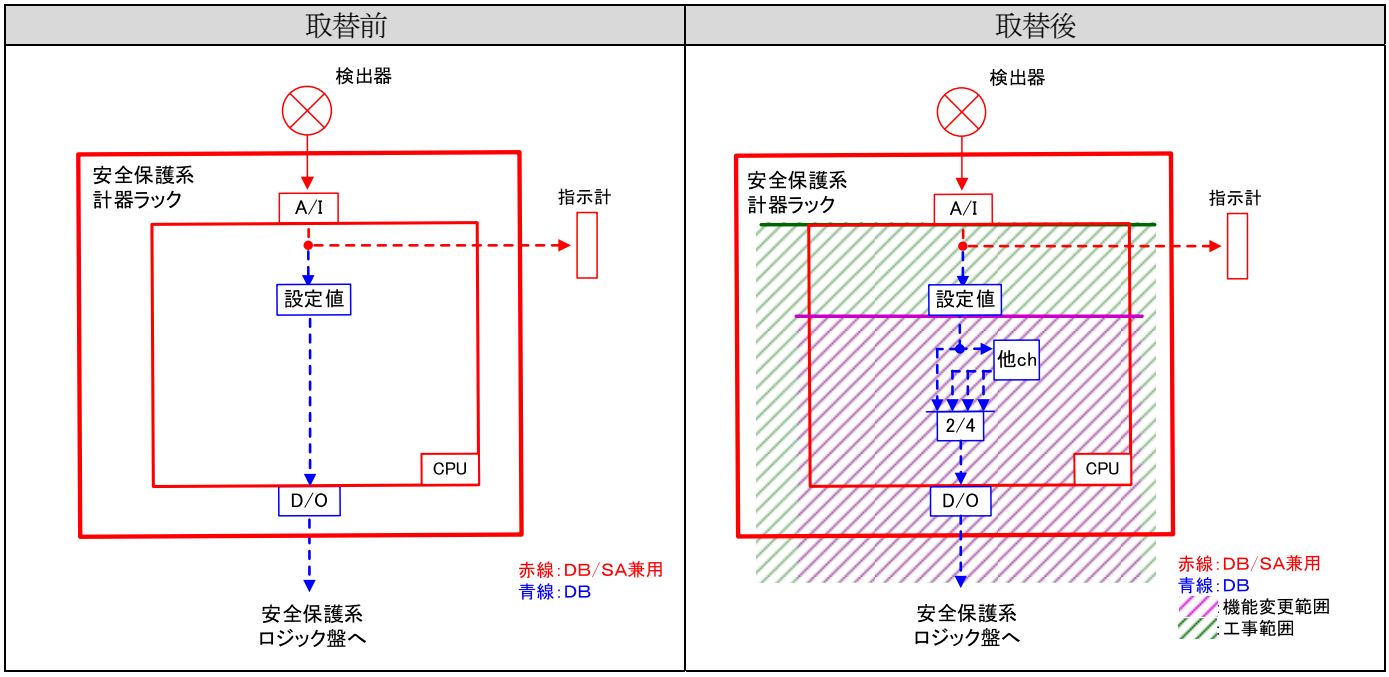


図１．ロジック盤取替前後におけるＳＡ設備および工事の範囲

２．３　ＳＡ時に用いる指示計に用いる指示機能が変更ないことの検証および妥当性確認

JEAG4609-2008「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」、JEAC4620-2008「ディジタル安全保護系の検証及び妥当性確認に関する規程」に以下の記載がある。

○JEAG4609-2008「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」

４．検証及び妥当性確認

ディジタル安全保護系に装荷するソフトウェアは、検証及び妥当性確認を実施して、安全保護上要求される機能が正しく実現されていることが確認されるべきである。

４．１　検証及び妥当性確認の目的

（１）検証及び妥当性確認は、JEAC4620-2008 のディジタル安全保護系システム要求事項が設計・製作・試験・変更の各プロセスにおいて正しく実現されていることを保証するための活動である。

○JEAC4620-2008「安全保護系へのディジタル計算機の適用に関する規程」

４．ディジタル安全保護系に対する要求事項

ディジタル安全保護系は、動作に失敗する確率及び誤動作する頻度を考慮し、その安全保護機能に相応した高い信頼性を有すること。

計器ラックにはディジタル計算機※1を適用しており、ＣＰＵはディジタル計算機の一部である。ロジック盤取替工事においては、ディジタル安全保護系※2のソフトウェアの変更があることから、検証および妥当性確認（Ｖ＆Ｖ：Verification and Validation）（以下、「Ｖ＆Ｖ」という。）を行っている。

※１：ディジタル計算機
内蔵されたプログラムによって制御され、人手の介入なしにディジタルデータの算術演算や論理演算などの計算を行う装置。

※２：ディジタル安全保護系
ディジタル計算機を適用した安全保護系。

（Ｖ＆Ｖの確認結果）
Ｖ＆Ｖにおいて、システム変更の影響範囲を明確にしたうえで、変更のない範囲については、新旧照合を行うことにより、変更が加えられていないことを確認している。

以上より、「２．２」に示す、ロジック盤取替工事において指示機能に変更がないことは妥当であると確認された。

２．４　ロジック盤取替工事範囲対象内の機器故障時の保安規定への影響

保安規定第８４条表８４－１６には、運転上の制限（以下、「ＬＣＯ」という。）を定めており、ＬＣＯを満足していない場合に要求される措置（以下、「要求される措置」という。）を規定している。

ロジック盤取替工事の工事範囲において機器の故障が発生した際のＳＡ設備への影響は、ＣＰＵ内の論理回路等に不具合が発生した場合、ＣＰＵ故障となり、ＣＰＵからの信号が発信不能となるため、図２に示すとおり、ＳＡ設備（指示計）が動作不能となる。その場合、保安規定に定めた要求される措置を実施することになり、主要パラメータ「加圧器水位」を例にとると、所要チャンネル数１チャンネルを満足できない場合は、「１．保安規定（抜粋）」に示すとおりの要求される措置を実施することとなる。

「２．２」、「２．３」に示すとおり、ロジック盤取替前後において指示機能に変更はないことから、ロジック盤取替工事における工事範囲対象内の機器故障時においても、保安規定に定める事項に影響はない。

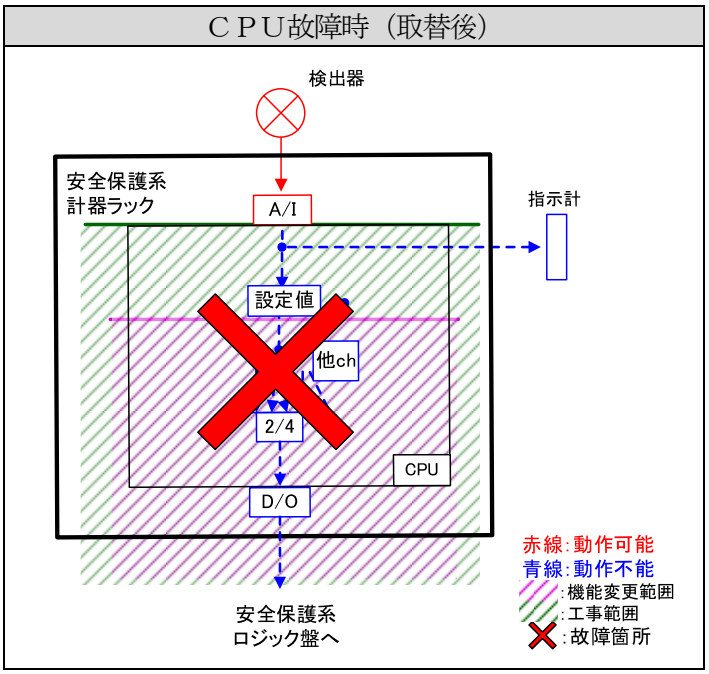


図２．ＣＰＵ故障時の影響範囲

以　上

伊方発電所保安規定審査資料	
資料番号	TS(76)-05-05(r2)

ロジック盤取替工事による
保安規定の確認事項の整理

令和３年８月

四国電力株式会社

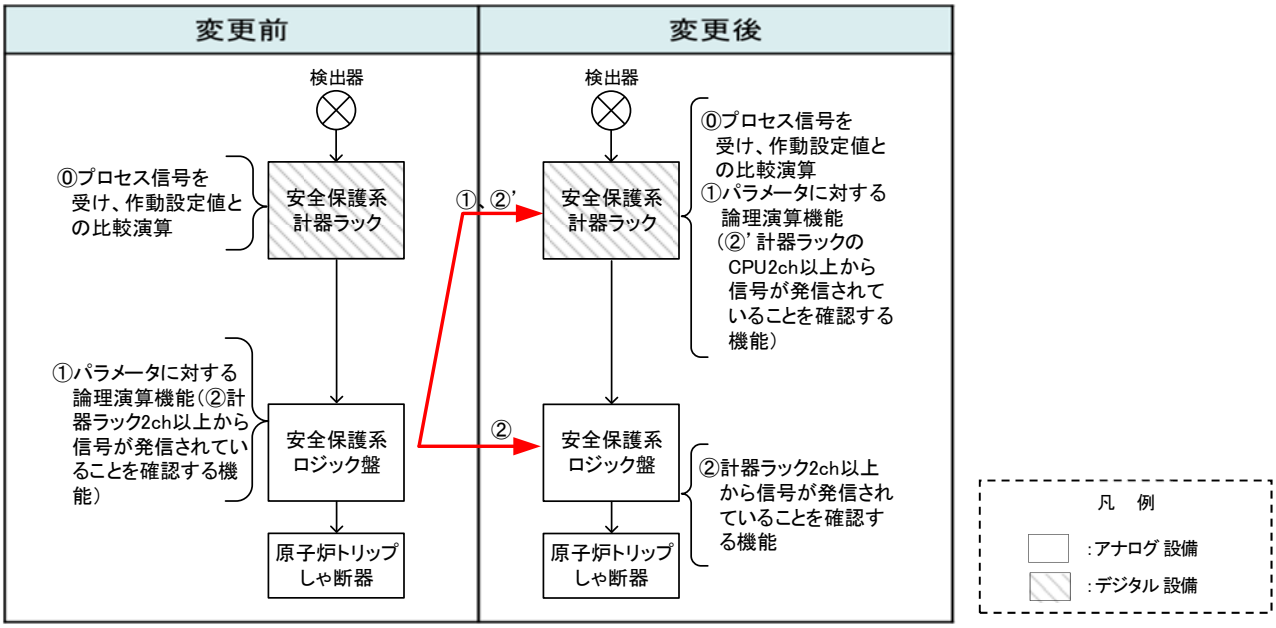
目　　次

１．設工認申請における計器ラックの論理演算機能とロジック盤の保障回路について

設計及び工事計画認可申請（以下、「設工認申請」という。）において、安全保護系ロジック盤（以下、「ロジック盤」という。）が担っているパラメータに対する論理演算機能（以下、「論理演算機能」という。）は、デジタル制御装置である安全保護系計器ラック（以下、「計器ラック」という。）のソフトウェアに移設することとともに、ロジック盤を計器ラックのマイクロプロセッサ故障等による原子炉トリップしゃ断器の誤作動等を防ぐためのリレー回路（以下、「保障回路」という。）を設置している。

上記の設備変更による、保安規定第３３条(計測および制御設備)表３３－２原子炉保護系計装について１カ月に１回の確認事項への影響について整理する。

ａ．原子炉停止系



《保安規定　抜粋》

表３３－２　原子炉保護系計装

表33－２　原子炉保護系計装

機　能	設定値	適用モード	所要チャンネル・系統数	所要チャンネル・系統数を満足できない場合の措置※2			確認事項		
				条　件	要求される措置	完了時間	項　目	頻　度	担　当
１．原子炉保護系論理回路※3	－	モード１および２	４系統	A. １系統が動作不能である場合	A. 1 計装計画課長は，当該系統を動作可能な状態にする。ただし，残りの系統が正常な状態であることを確認※4のうえ，作業のため当該系統のバイパスを行うことができる。	６時間	機能の確認を行う。	定期事業者検査時	計装計画課長
							機能の確認を行う。残りの系統が動作可能な状態においては，機能確認のためのバイパスを２時間に限り行うことができる。	１ヶ月に１回（交互に２系統ずつ）	計装計画課長
				B. 原子炉トリップしゃ断器１系統が動作不能である場合	B. 1 電気計画課長は，当該系統を動作可能な状態にする。	１時間			
				C. 条件ＡまたはＢの措置を完了時間内に達成できない場合	C. 1 当直長は，モード３にする。	12時間			
		原子炉トリップしゃ断器が閉じ，制御棒の引抜きが行える場合のモード３，４および５	４系統	A. １系統が動作不能である場合	A. 1 計装計画課長は，当該系統を動作可能な状態にする。ただし，残りの系統が正常な状態であることを確認のうえ，作業のため当該系統のバイパスを行うことができる。	48時間			
				B. 原子炉トリップしゃ断器１系統が動作不能である場合	B. 1 電気計画課長は，当該系統を動作可能な状態にする。	48時間			
				C. 条件ＡまたはＢの措置を完了時間内に達成できない場合	C. 1 当直長は，原子炉トリップしゃ断器を開く。	１時間			

※２：特に定める場合を除き，チャンネル・系統毎に個別の条件が適用される。（以下，本条において同じ。）
※３：モード１および２における原子炉トリップしゃ断器は，重大事故等対処設備を兼ねる。
※４：「正常な状態であることを確認」とは，定期事業者検査時の記録確認および運転中に作業を実施した場合はその復旧状態の確認を行うことをいう。（以下，本条において同じ。）

２．原子炉保護系計装の健全性の確認方法の整理

２．１　保安規定上の健全性の確認方法について

保安規定第８６条（運転上の制限の確認）では、運転上の制限を満足していることの確認について以下のとおり記載されている。

（運転上の制限の確認）
第 86 条 各課長は，運転上の制限を満足していることを第３節第 19 条から第 85 条の２の第２項（以下，各条において「この規定第２項」という。）で定める事項により確認する。なお，この確認は，確認する機能が必要となる事故時等の条件で必要な性能が発揮できるかどうかを確認（以下「実条件性能確認」という。）するために十分な方法（事故時等の条件を模擬できない場合等においては，実条件性能確認に相当する方法であることを検証した代替の方法を含む。）により行う。

保安規定では、「必要な性能が発揮できるかどうかを確認するために十分な方法を定期事業者検査時またはプラント運転時の定期的な頻度で行うこと」として規定している。

保安規定第３３条(計測および制御設備)表３３－２原子炉保護系計装に必要な性能とは、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にある第２４条（安全保護回路）の機能が健全に作動することである。

２．２　取替前後の確認範囲について

取替前後の確認範囲について以下に示す。取替前は図中の確認範囲①であったが、取替後はロジック盤が有していた論理演算機能がデジタル制御装置である計器ラックのソフトウェアで実現されたため、図の確認範囲②となる。

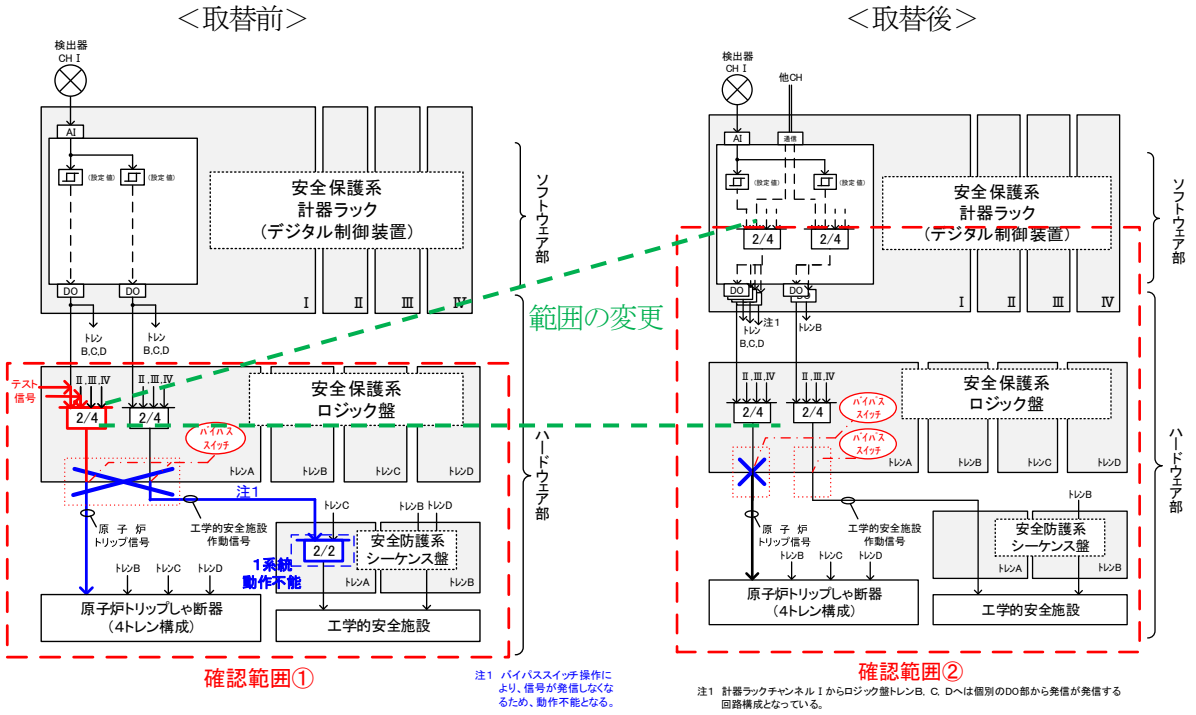


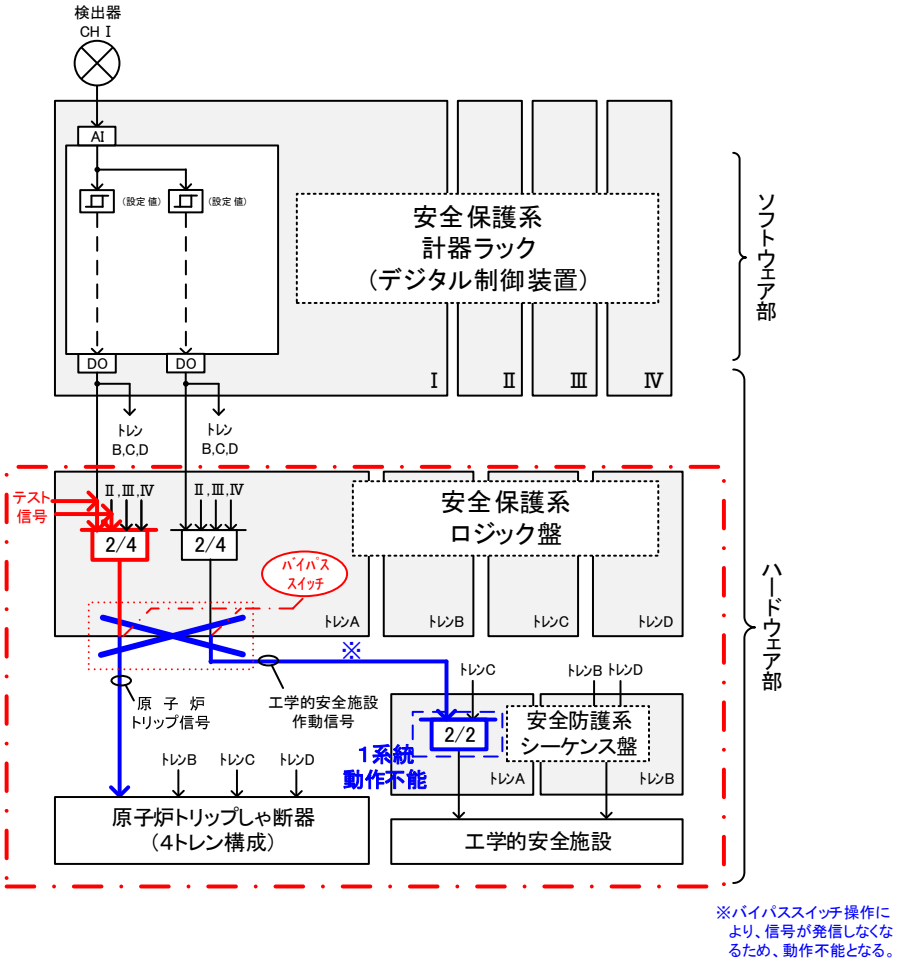
図　取替前後の確認範囲について

２．３　取替前後の確認方法について

取替前後の確認方法について以下に整理する。

２．３．１　取替前の確認方法

ロジック盤の論理演算機能はアナログ制御装置のハードウェアにて構成されており、ハードウェアのため実動作により機能確認を実施する必要があった。そのため、ロジック盤の論理演算機能の上流からテスト信号を模擬入力し、ロジック盤の論理演算機能が動作することを下流にある原子炉トリップしゃ断器の実動作や警報等の発信により１カ月に１回の頻度で確認し、論理演算機能が問題ないことを確認していた。



２．３．２　取替後の論理演算機能の上流から信号入力する場合の確認方法（その１）

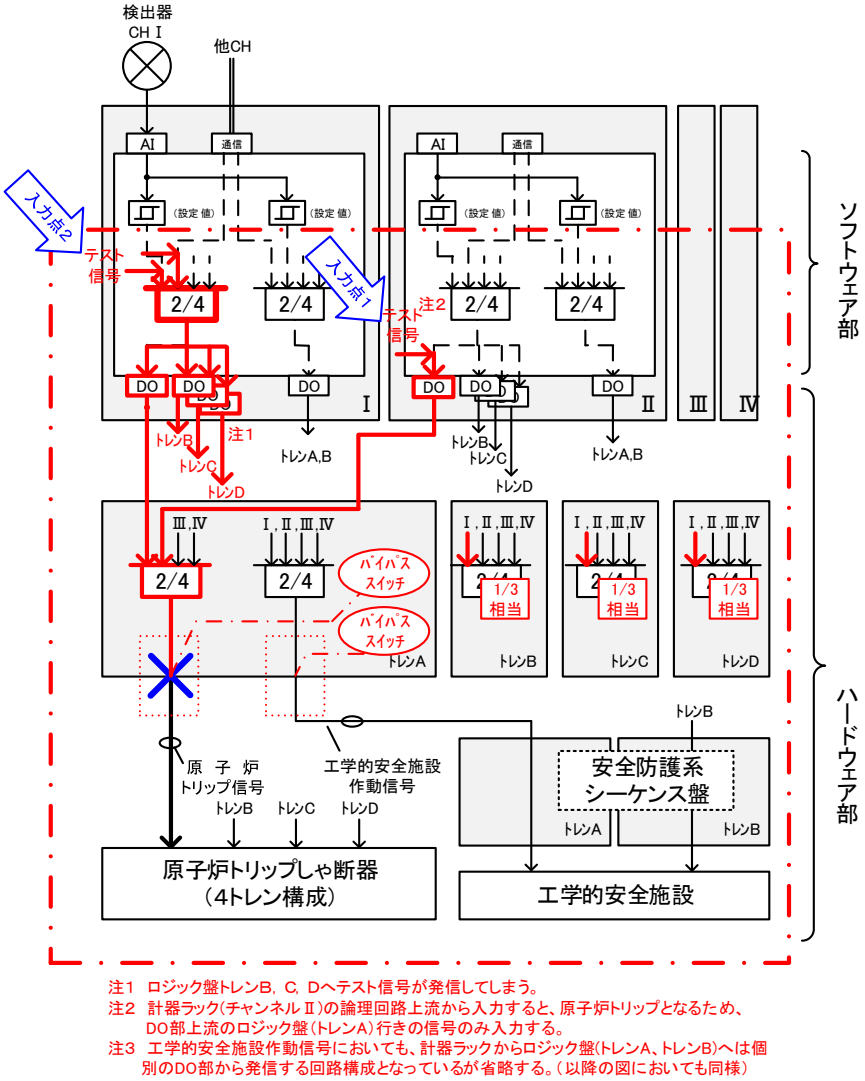
論理演算機能の上流から信号入力する場合の確認方法について、整理する。

論理演算機能の上流から信号を入力し、取替前の「原子炉保護系論理回路」に相当する確認範囲について１つの試験として実施する場合の方法を以下に示す。

入力点１：ロジック盤(トレンA)の保障回路を動作させるために、計器ラック（チャンネルⅡ）からテスト信号を入力する。
この際、ロジック盤トレンB，C，Dへテスト信号を発信しないよう、DO部上流のロジック盤トレンA行きのテスト信号を入力して、試験対象のロジック盤（トレンA）の保障回路へ信号を発信させる。

入力点２：計器ラック(チャンネルⅠ)の論理演算機能の上流から信号を入力する。この際、計器ラック(チャンネルⅠ)のDO部からロジック盤トレンB，C，Dへテスト信号が発信してしまうこととなるため、すべてのロジック盤にある保障回路の2/4の状態が、1/3相当※となる。このため、誤動作により他の１チャンネルの計器ラックからの原子炉トリップ信号が発信した場合、ロジック盤にある保障回路が動作し、原子炉トリップする。

※　1/3相当とは、2/4ロジックの内、一つの信号が動作した状態のことである。



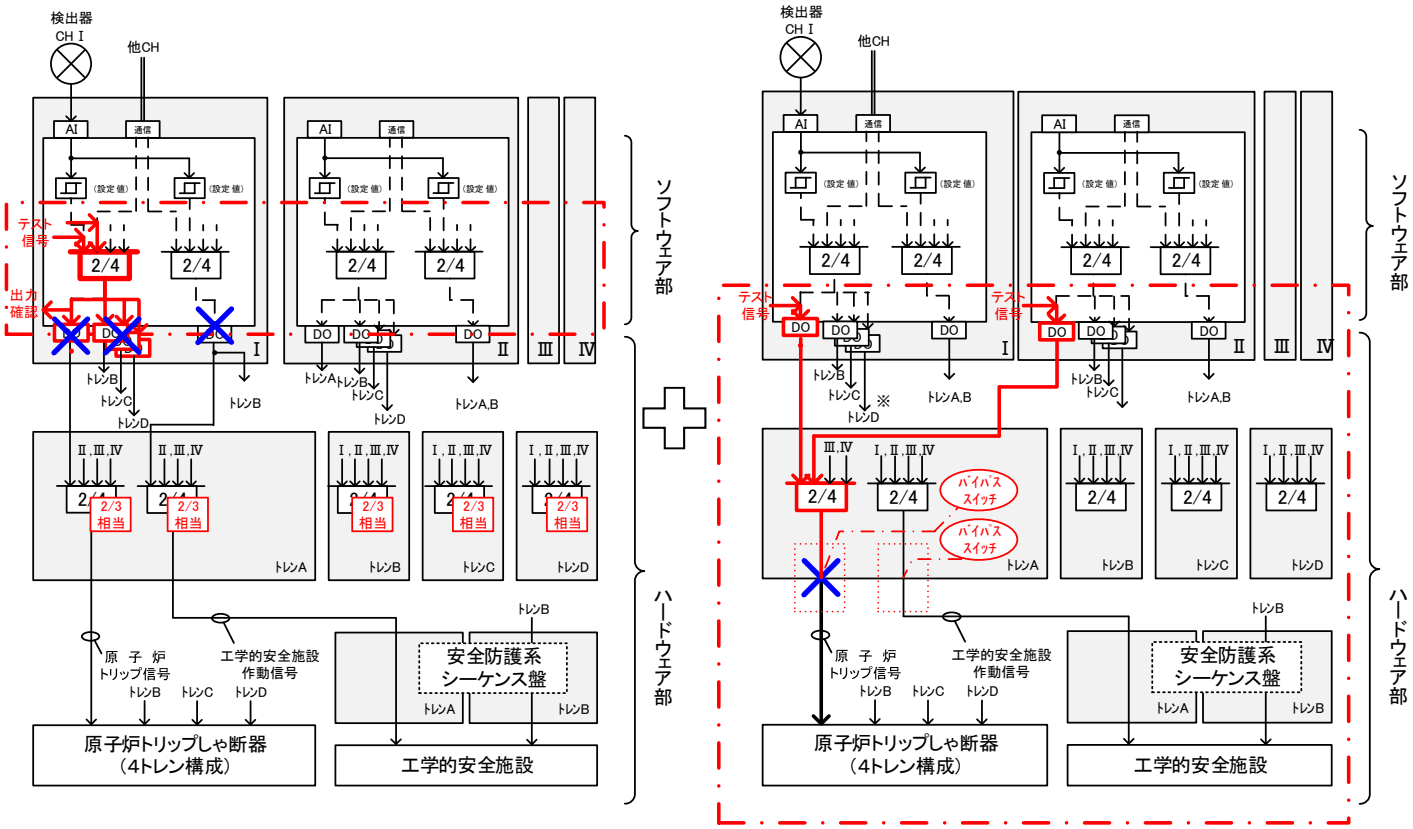
注1　ロジック盤トレンB，C，Dへテスト信号が発信してしまう。
注2　計器ラック(チャンネルⅡ)の論理回路上流から入力すると、原子炉トリップとなるため、DO部上流のロジック盤(トレンA)行きの信号のみ入力する。
注3　工学的安全施設作動信号においても、計器ラックからロジック盤(トレンA、トレンB)へは個別のDO部から発信する回路構成となっているが省略する。(以降の図においても同様)

本手順により試験を実施する場合、不要な原子炉トリップを招く恐れがある。このため、別の方法にて機能の健全性の確認を実施する。

２．３．３　論理演算機能の上流からにより信号入力する場合の確認方法（その２）

論理演算機能の上流から信号入力する場合の確認方法として、不要な原子炉トリップを招く恐れを低くするため、ソフトウェア部とハードウェア部に分けて試験を実施する方法がある。ソフトウェア部の確認を試験方法A、ハードウェア部の確認を試験方法Bとして、それぞれ試験を実施し、これらの組み合わせにより原子炉保護系の機能の健全性を確認する。

＜試験方法A＞　　＜試験方法B＞



・ソフトウェア部（図の試験方法A）

他チャンネルへの信号発信を防止するため、試験対象の計器ラック(図中のチャンネルⅠの計器ラック)を除外（バイパス）状態にすることによって、すべてのロジック盤にある保障回路の2/4の状態が、2/3相当となる。このため、誤動作により他の１チャンネルの計器ラックからの原子炉トリップ信号が発信しても、ロジック盤にある保障回路は動作せず、不要な原子炉トリップを防止できる。

この条件のもと、論理演算機能上流からテスト信号を模擬入力し、論理演算機能が動作することを下流（ソフトウェア内部のDO部入口前）で確認する。

※2/3相当とは、2/4ロジックの内、一つの信号が使用不能となった状態のことである。

・ハードウェア部（図の試験方法B）

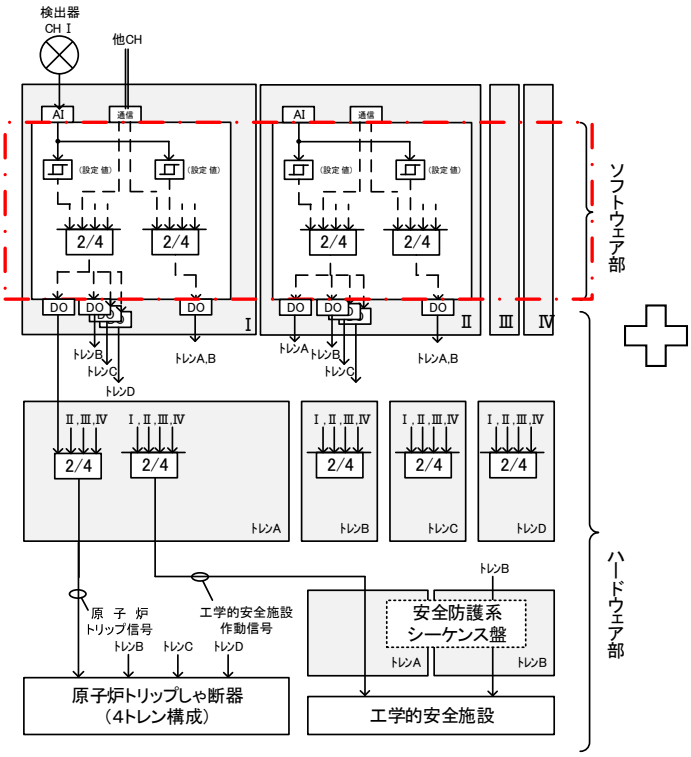
計器ラックの論理演算機能の下流からテスト信号を模擬入力し、ロジック盤の保障回路が動作することを下流にある原子炉トリップしゃ断器の実動作や警報等の発信により確認し、ロジック盤の保障回路が問題ないことを確認する。

２．３．４　ソフトウェアの特性を用いた健全性の確認方法

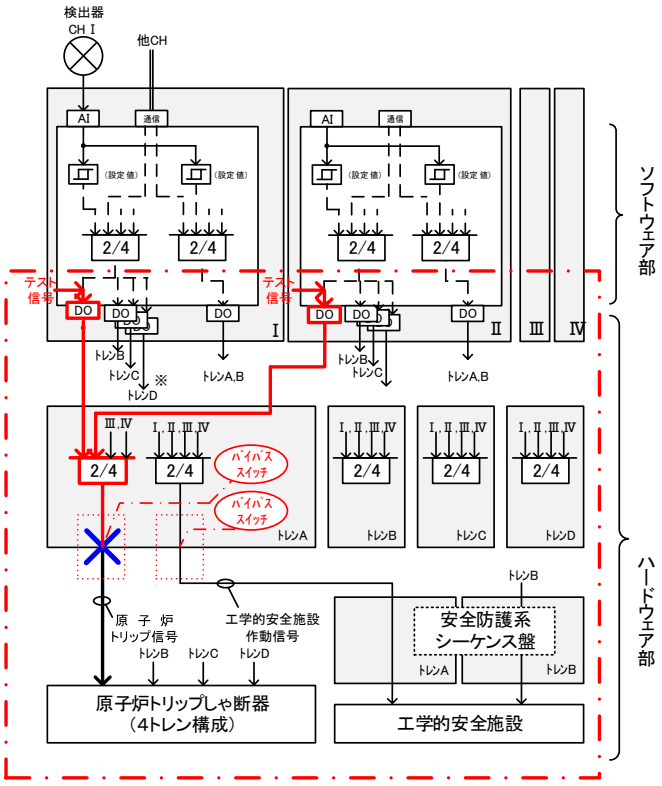
ソフトウェア部については、「原子力事業者等における使用前事業者検査、定期事業者検査、保安のための措置等に係る運用ガイド」（最終改正令和３年４月２８日）（以下、「ガイド」という。）において、以下に示す健全性の確認方法が認められている。（具体的な運用については、別紙－１に示す。）

このため、ソフトウェアの特性を用いた健全性の確認方法を試験方法A’とする。なお、試験方法Bは２．３．３項の方法と同様である。

＜試験方法A’＞



＜試験方法B＞



図中のソフトウェア部とは、「マイクロプロセッサ等※1」とマイクロプロセッサ等によって処理される「ソフトウェア」の総称である。

・ソフトウェア部（図の試験方法A’）

論理演算機能はデジタル制御装置のマイクロプロセッサ等によって処理されるソフトウェアにより実現される。

論理演算機能の健全性を確認するためには、マイクロプロセッサ等とソフトウェアの両方の健全性を確認する必要がある。

ソフトウェアは、経年的に変化するものではないため、「日本電気協会「安全保護系へのディジタル計算機の適用に関する規程」（ＪＥＡＣ４６２０－２００８）」の要求事項に準じた文書体系を整備、維持し、ソフトウェア構成管理が適切になされていることの確認を行うことで論理演算機能が問題ないことを確認する。

マイクロプロセッサ等は、経年的に劣化するものであることから、自己診断機能によって、常時確認すること※2でマイクロプロセッサ等の健全性を確認し、論理演算機能が問題ないことを確認する。

なお、マイクロプロセッサ等については、自己診断機能にて健全性を常時確認されているものの、更なる健全性の確認として、物理的な損傷がないことを１カ月に１回の頻度で確認する。

・ハードウェア部（図の試験方法Ｂ）

ハードウェアで構成されていることから、計器ラックの論理演算機能の下流からテスト信号を模擬入力し、ロジック盤の保障回路が動作することを下流にある原子炉トリップしゃ断器の実動作や警報等の発信により確認し、ロジック盤の保障回路が問題ないことを確認する。

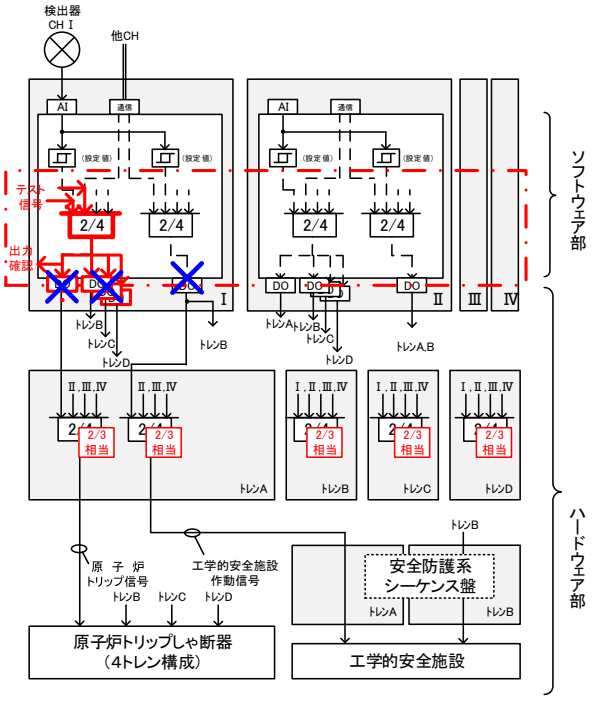
※１　マイクロプロセッサ等とは、外部からのハードワイヤード（配線）の信号を入力するアナログ信号入力部、外部へハードワイヤードの信号を出力する接点信号出力部、外部の制御装置と１対１の通信出力あるいは通信入力を行う電気/光変換通信部、外部の制御装置と１対複数の通信出力を行うネットワーク通信部、およびこれらの部位から入出力される信号の処理や論理演算処理などを行うマイクロプロセッサ、入出力信号のデータなどを一時的に格納するメモリ(RAM)、論理演算などの不変のソフトウェアを格納するメモリ(ROM)などを有するマイクロプロセッサ部などで構成される設備をいう。

※２　ソフトウェアは３０ｍｓｅｃの周期で「入力処理」→「演算処理」→「自己診断処理」→「出力処理」の処理を行っていることから、自己診断機能としては３０ｍｓｅｃの周期毎に確認している。

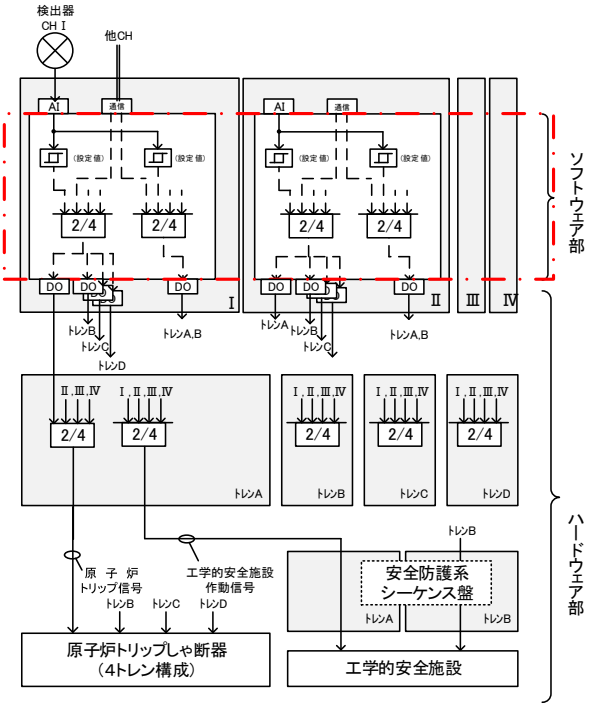
２．３．５　論理演算機能の確認方法の比較

ソフトウェアで実現された論理演算機能の健全性の確認方法について、試験方法Ａと試験方法Ａ’について比較する。

＜試験方法Ａ＞



＜試験方法Ａ’＞



試験方法		メリット	デメリット
Ａ	論理演算機能の上流から信号入力する方法	－	・計器ラックを１チャンネル除外（バイパス）する必要があるため、ロジック盤の保障回路が２/３相当となり、原子炉保護系の機能の信頼性が低下する（アンアベイラビリティ※がＡ’に比べて増加） ・試験方法Ａ’は模擬入力作業がないが、試験方法Ａは模擬入力作業が必要となるため、作業によるヒューマンエラーのリスクが増加する。
Ａ’	ソフトウェアの特性を用いた確認方法	・計器ラックを１チャンネル除外（バイパス）しなくてよいため、ロジック盤の保障回路が２/４を維持でき、原子炉保護系の機能の信頼性が維持できる（アンアベイラビリティは変わらない。） ・試験方法Ａ’は模擬入力作業がないため、作業によるヒューマンエラーのリスクは増加しない。	－

※　アンアベイラビリティとは、原子炉トリップ動作が失敗する確率である。

以上より、試験方法Ａと試験方法Ａ’ともに健全性は確認できる。その一方、試験方法Ａについては、試験中に原子炉保護系の機能の信頼性が低下することから、試験方法Ａ’により論理演算機能の健全性を確認することとする。

３．原子炉保護系計装の確認事項の整理

３．１　保安規定上の確認事項の目的

保安規定第１１条第２項において、各条文の第２項に運転上の制限を満足していることを確認するために行う事項を規定している。

（構成および定義）
第 11 条　本編において，原子炉の運転モード（以下「モード」という。）は，表 11 のとおりとする。
２　第３節（第 86 条から第 89 条を除く。）における条文の基本的な構成は次のとおりとする。
(1)　第１項：運転上の制限
(2)　第２項：運転上の制限を満足していることを確認するために行う事項
(3)　第３項：運転上の制限を満足していないと判断した場合※1に要求される措置

保安規定第３３条（計測および制御設備）では、運転上の制限を満足していることを確認するために表３３－２から表３３－８で定める確認事項を実施することを規定している。また、第３３条の運転上の制限は、表３３－１のとおり「表３３－２から表３３－８に定める所要チャンネル数、系統数および機能がそれぞれの適用モードにおいて動作可能であること」を規定している。

（計測および制御設備）
第 33 条　次の計測および制御設備は，表 33－１で定める事項を運転上の制限とする。
(1)　原子炉保護系計装
(2)　工学的安全施設等作動計装
(3)　事故時監視計装
(4)　非常用ディーゼル発電機起動計装
(5)　中央制御室換気系隔離計装
(6)　中央制御室外原子炉停止装置
(7)　燃料落下および燃料取扱建屋空気浄化系計装
２　計測および制御設備が前項で定める運転上の制限を満足していることを確認するため，次号を実施する。
(1)　安全技術課長，当直長，電気計画課長および計装計画課長は，表 33－２から表 33－８で定める確認事項を実施する。また，安全技術課長，電気計画課長および計装計画課長は，その結果を発電課長または当直長に通知する。
３　当直長，電気計画課長および計装計画課長は，計測および制御設備が第１項で定める運転上の制限を満足していないと判断した場合，表 33－２から表 33－８の措置を講じるとともに，必要に応じ，関係各課長へ通知する。通知をうけた関係各課長は，同表に定める措置を講じる。

表 33－１

項　　目	運転上の制限
第１項で定める計測および制御設備	表33－２から表33－８に定める所要チャンネル数，系統数および機能がそれぞれの適用モードにおいて動作可能※1であること

※１：本条における動作可能とは，当該計測および制御設備に期待されている機能が達成されている場合をいう。また，本条における動作不能とは，特に定めのある場合を除き，点検・修理のために当該チャンネルもしくは論理回路をバイパスする場合，または不動作の場合をいう。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。

保安規定第３３条表３３－２　１.原子炉保護系論理回路において、運転上の制限を満足していることの確認事項は、原子炉保護系論理回路４系統および機能が動作可能であることを定期事業者検査時および１カ月に１回の機能の確認で行うことを規定している。

表33－２　原子炉保護系計装

機　能	設定値	適用モード	所要チャンネル・系統数	所要チャンネル・系統数を満足できない場合の措置※2			確認事項		担　当
				条　件	要求される措置	完了時間	項　目	頻　度	
1．原子炉保護系論理回路※3	－	モード１および２	４系統	A. １系統が動作不能である場合	A. 1 計装計画課長は，当該系統を動作可能な状態にする。ただし，残りの系統が正常な状態であることを確認※4のうえ，作業のため当該系統のバイパスを行うことができる。	６時間	機能の確認を行う。	定期事業者検査時	計装計画課長
							機能の確認を行う。残りの系統が動作可能な状態においては，機能確認のためのバイパスを２時間に限り行うことができる。	１ヶ月に１回（交互に２系統ずつ）	計装計画課長
				B. 原子炉トリップしゃ断器１系統が動作不能である場合	B. 1 電気計画課長は，当該系統を動作可能な状態にする。	１時間			
				C. 条件ＡまたはＢの措置を完了時間内に達成できない場合	C. 1 当直長は，モード３にする。	12時間			
		原子炉トリップしゃ断器が閉じ，制御棒の引抜きが行える場合のモード３，４および５	４系統	A. １系統が動作不能である場合	A. 1 計装計画課長は，当該系統を動作可能な状態にする。ただし，残りの系統が正常な状態であることを確認のうえ，作業のため当該系統のバイパスを行うことができる。	48時間			
				B. 原子炉トリップしゃ断器１系統が動作不能である場合	B. 1 電気計画課長は，当該系統を動作可能な状態にする。	48時間			
				C. 条件ＡまたはＢの措置を完了時間内に達成できない場合	C. 1 当直長は，原子炉トリップしゃ断器を開く。	１時間			

※２：特に定める場合を除き，チャンネル・系統毎に個別の条件が適用される。（以下，本条において同じ。）
※３：モード１および２における原子炉トリップしゃ断器は，重大事故等対処設備を兼ねる。
※４：「正常な状態であることを確認」とは，定期事業者検査時の記録確認および運転中に作業を実施した場合はその復旧状態の確認を行うことをいう。（以下，本条において同じ。）

３．２　取替後の確認事項の確認方法

保安規定における「原子炉保護系論理回路」の確認事項は、運転上の制限（原子炉保護系論理回路４系統および機能が動作可能であること）を満足していることを確認することである。

取替前の「原子炉保護系論理回路」に相当する確認範囲については、取替後はソフトウェア部とハードウェア部となるため、それぞれの方法により機能が動作可能であることを確認する。確認イメージを参考－１に示す。

取替後の「原子炉保護系論理回路」であるハードウェア部は、定期事業者検査および１カ月に１回の実動作により確認することで、運転上の制限を満足していることを確認する。

なお、取替後のソフトウェア部(マイクロプロセッサ等を含む)は「原子炉保護系論理回路」には該当しないが、機能が動作可能であることを自己診断機能により常時確認できるため、検出器毎のチャンネルにて確認することで、運転上の制限を満足していることを確認する。
また、マイクロプロセッサ等については、自己診断機能にて健全性を常時確認されているものの、経年的な劣化に関しては、１カ月に１回のハードウェア部の確認時にあわせて物理的な損傷がないことを確認する。

定期事業者検査時は、保全として計器ラックの点検作業を行っていることから、機能に影響を与えるソフトウェアに変更がないことをソフトウェアのバージョン確認および照合試験を実施することで確認する。

４．確認事項の頻度の整理

発電用原子炉施設の各設備については、設備に応じた常時の運転監視、発電用原子炉施設の巡視および日常の保守点検（外観点検、バッテリー点検等）等の管理に加え、特に運転上の制限となる設備については、保安規定の確認事項として、定期的に運転上の制限を満足しているかの確認（以下、「サーベイランス」という。）を行っている。

「保安規定変更に係る基本方針」（改訂６）（以下、「基本方針」という。）を踏まえ、ロジック盤取替前後での原子炉保護系計装に対するサーベイランスについて整理する。

４．１　ロジック盤取替前までの頻度の考え方

保安規定に記載すべきサーベイランス頻度の考え方について、基本方針には、「サーベランスの実施は、ＬＣＯを満足しているかの確認であり、サーベランスの頻度を増やしても設備の健全性が向上することはないことから、サーベランス頻度と設備の健全性は、必ずしも直接的に関連するものではない」と記載されている（基本方針にはサーベランスと記載されているが、保安規定審査基準改正に伴い「サーベランス」は「サーベイランス」に変更されている）。

基本方針の記載内容を踏まえ、以下の２点より、これまでのサーベイランス頻度を１カ月に１回として決定していた。

・米国標準技術仕様書は１カ月に１回として実施することを推奨していた。
・他社プラントも含めて、我が国での運転経験に基づき、１カ月に１回の頻度で十分な実績があった。

４．２　ロジック盤取替後の頻度の設定

ロジック盤取替後は、ソフトウェア部とハードウェア部があるため、それぞれの頻度について整理する。

➢　ソフトウェア部

ソフトウェアはマイクロプロセッサ等によって処理されるため、ソフトウェアとマイクロプロセッサ等の両方の健全性を確認する頻度が必要となる。

・ソフトウェアは、経年的に変化するものではないため、ソフトウェアに変更がないことを、中央制御室へ不要な警報の発信がないことをもって常時監視している。
・マイクロプロセッサ等は、自己診断機能にて健全性を常時確認されているものの、更なる健全性の確認として物理的な損傷がないことを１カ月に１回の頻度で実施するものであり、これまでの実績も踏まえて、１カ月に１回の頻度で実施することによりプラントの安全性は維持できると考える。

➢　ハードウェア部

以下の２点を踏まえて、サーベイランス頻度として妥当と考える。

・米国標準技術仕様書の１カ月に１回から変わるものでない。
・他社プラントも含めて、我が国での運転経験に基づき、１カ月に１回の十分な実績があった。（例えば、伊方発電所１、２号機についても同様の頻度で実施）

５．まとめ

ロジック盤取替前後において、設備構成がハードウェア部とソフトウェア部に変わることで、確認事項の範囲および方法は変更となるものの、原子炉保護系論理回路４系統および機能が動作可能であることの確認は、取替前と同様に取替後も確認している。

取替前	取替後
１カ月に１回の機能確認 ・実動作による機能確認	１カ月に１回の機能確認 ➢　ハードウェア部 ・実動作による機能確認 ➢　ソフトウェア部 ・マイクロプロセッサ等の物理的な損傷がないことを確認 常時 ➢　ソフトウェア部 ・ソフトウェア変更は、不要な警報発信の有無にて確認 ・マイクロプロセッサ等の健全性は、自己診断により健全であることを確認
定期事業者検査時 ・実動作による機能確認	定期事業者検査時 ➢　ハードウェア部 ・実動作による機能確認 および ➢　ソフトウェア部 ・マイクロプロセッサ等の物理的な損傷がないことを確認 ・点検作業によるソフトウェアの変更を考慮して、ソフトウェアの健全性確認としてバージョン確認および照合試験にて確認 常時 ➢　ソフトウェア部 ・ソフトウェア変更は、不要な警報発信の有無にて確認 ・マイクロプロセッサ等の健全性は、自己診断により健全であることを確認

以上

ソフトウェアで実現された論理演算機能の健全性の確認について

計器ラックのソフトウェアで実現された論理演算機能の健全性を確認するには、ソフトウェアとマイクロプロセッサ等の両方の健全性を確認する必要があるため、その確認方法について以下に整理する。

１．ソフトウェアの健全性について

「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の解釈」（以下「解釈」という。）第３５条（安全保護装置）の４の要求に基づく、ＪＥＡＣ４６２０－２００８の４．１８品質管理にソフトウェアの健全性を確保することが規定されている。

> JEAC4620 4.18 品質管理
> 安全保護系に用いられるデジタル計算機は、以下の手法によりソフトウェアの健全性を確保すること。（解説－13）
> ・ソフトウェアライフサイクル及び構成管理手法を含めた、品質保証活動
> ・検証及び妥当性確認活動

上記のとおり、ソフトウェアの健全性を確保するための、品質保証活動等の内容を以下に示す。
（詳細な活動内容については、添付資料－１参照）

(a) ソフトウェアライフサイクル

デジタル安全保護系に使用するソフトウェアについては、設計、製作、試験、装荷、運転、変更、廃止の各段階における品質の管理手法を定め、その管理手法に基づき実施するとともに、その結果を文書化する。

(b) ソフトウェア構成管理

デジタル安全保護系のソフトウェアに対して、構成管理手法を予め定め、実施するとともに、構成管理計画として文書化する。また、ソフトウェアを構成する管理対象項目は、ソフトウェア構成管理計画に基づき文書化する。

安全保護系計器ラックに使用するソフトウェアは、演算処理回路が可視化されたシンボル化言語を使用し、設備単位あるいは演算処理のブロック単位で設計、製作、変更、保管等の管理を行う。

(c) 検証及び妥当性確認

デジタル安全保護系に使用するソフトウェアについては、設計、製作、試験、変更の各過程で「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」（ＪＥＡＧ４６０９－２００８）に基づく検証及び妥当性確認を実施し、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が保証されたソフトウェアを使用する。

ソフトウェアが変更されれば、変更範囲について上記(a)～(c)を適宜実施することから、デジタル安全保護系のソフトウェアの健全性は確保できる。

このため、論理演算機能上段からテスト信号を入力し、論理演算機能の健全性が確認された時点からソフトウェア構成管理を実施し、ソフトウェアに変更がないことを管理することで、論理演算機能の健全性は確保できている。

また、ソフトウェアを変更する場合は、中央制御室へ警報が発信されるため、発信がないことをもってソフトウェアに変更がないことを管理し、論理演算機能の健全性が確保できていることを確認する。

上記方法は、機能及び作動の状況を確認するための十分な方法として「原子力事業者等における使用前事業者検査、定期事業者検査、保安のための措置等に係る運用ガイド」（最終改正令和３年４月２８日）（以下、「ガイド」という。）において認められている。以下、ガイドを抜粋する。

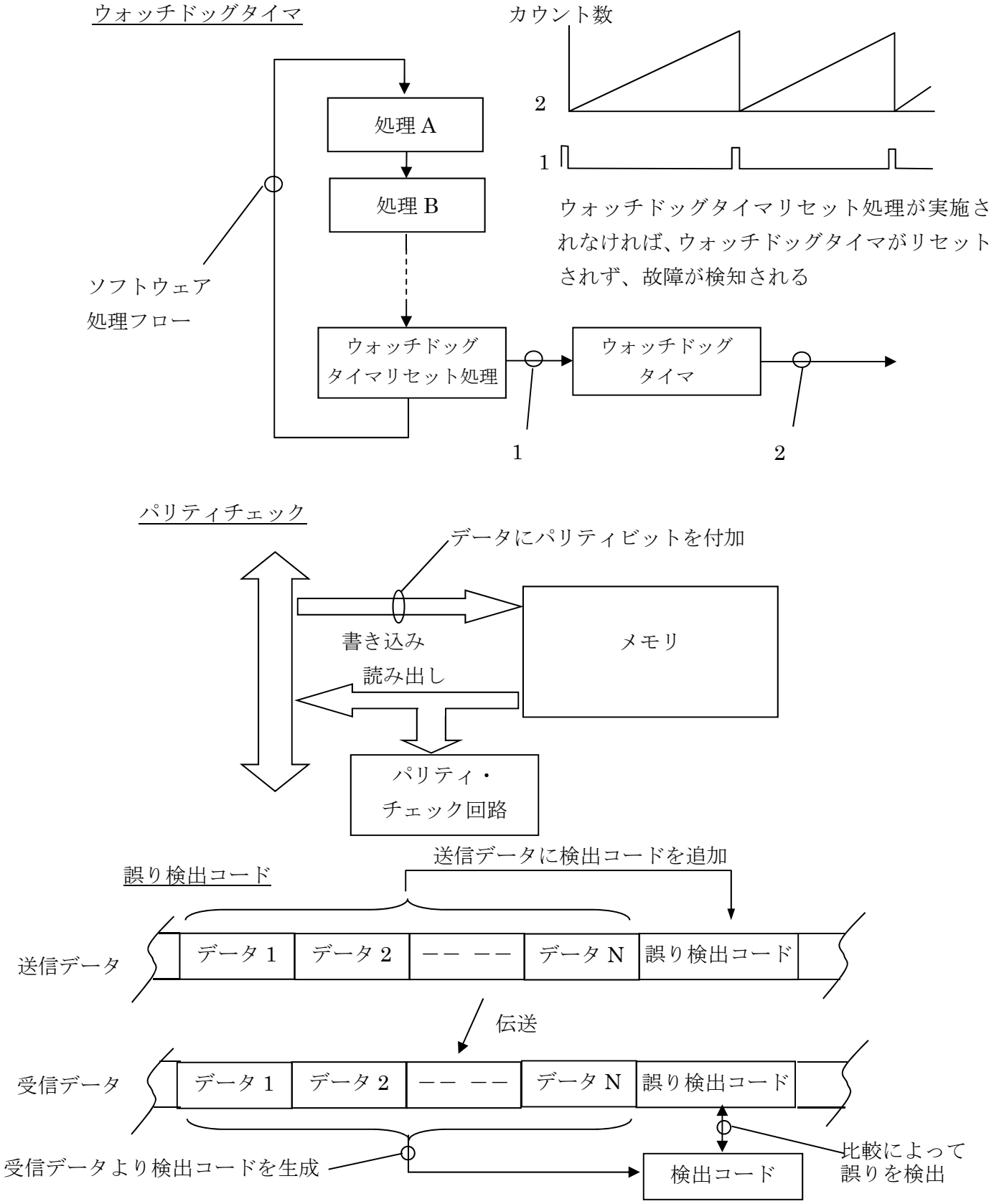
別記１　実用炉施設の技術基準条文ごとの検査の方法に係る特記事項
②第２号に規定する方法
　第２号に規定する機能及び作動の状況を確認するための十分な方法とは、表２に示す特性検査、機能・性能検査及び総合性能検査等を必要に応じ適切に組み合わせたものであることが必要である。また、確認対象となる技術基準の条項に対応して、以下の点については特に留意して検査の方法を設定する必要がある。
○技術基準第３５条（デジタル安全保護系）
　技術基準第３５条への適合性を確認するために行う検査のうち、デジタル安全保護系に関しては、技術基準解釈の「第３５条（安全保護装置）」の「４」に記載されている「日本電気協会「安全保護系へのディジタル計算機の適用に関する規程」（ＪＥＡＣ４６２０－２００８）」の要求事項に準じた文書体系を整備、維持し、ソフトウェア構成管理が適切になされていることの確認を行うこと。

２．４．２　マイクロプロセッサ等の健全性について

　デジタル安全保護系のマイクロプロセッサ等は経年的に劣化するものであることから、故障の早期発見のため自己診断機能を設け、運転中に常時、デジタル制御装置の健全性を確認できる設計としている。これらの健全性を確認する自己診断機能の具体的な内容は、伊方発電所第３号機設工認申請（デジタル保護系）（令和３年５月２７日認可）「資料７　デジタル制御方式を使用する安全保護系等の適用に関する説明書」のうち「別添　Ⅳ．デジタル安全保護系の自己診断機能について」より抜粋する。

第１表　自己診断機能の説明

自己診断機能名	診断の具体的内容
ウォッチドッグタイマ	CPUなどのプロセッサは、定周期で演算を繰り返している。この演算周期をプロセッサ外部に設けるハードウェアのタイマを用いて、第1図に示すような手順で監視し、プロセッサの異常を検知する。
演算時間チェック	CPUは、定周期で演算を繰り返している。1周期での演算時間が定周期の時間を越えていないか監視し、CPUの異常を検知する。
代表演算	あらかじめ答えを用意している演算を行い、演算結果が答えと一致しているかを監視し、CPU演算の異常を検知する。
ゼロ除算	通常ゼロで割る演算は存在しないため、ゼロ割り演算が行われないか監視し、CPU演算の異常を検知する。
パリティチェック	第1図に示すように、メモリ(RAM)への書き込み時にパリティビット（データ列の1が奇数の場合は1、偶数の場合は0）を付加し、次にメモリからの読み込み時にパリティビットを確認することにより、メモリデータの異常を検知する。
誤り検出コード	データ通信またはメモリ(ROM)のデータチェックにおいて、データをある数字で割った余りを誤り検出コードとして生成し、その変化の有無を監視し、データの異常を検知する。データ通信については、第1図に示すように送信側にてデータ毎に誤り検出コードを付加して送信し、受信側において生成した検出コードと比較する。
信号受信停止	データ通信の授受において、受信側がある一定期間以上データを受信できない状態や受信信号が得られない状態を監視し、送信側又は伝送経路の異常を検知する。
出力命令と出力信号の相違	接点信号出力部において、出力命令（マイクロプロセッサ部からの出力命令値）と出力信号（接点信号出力部が外部へ出力したハードワイヤード信号値）を比較し、相違の有無を監視し、出力部の異常を検知する。



第 1 図　自己診断機能の説明図

Ⅴ．デジタル安全保護系ソフトウェアの品質保証について

1. 概要

本資料は、安全保護系の論理演算機能にデジタル制御装置を適用するに当たり、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のソフトウェアに対する品質保証活動について説明する。

2. 基本方針

デジタル安全保護系は、「実用発電用原子炉に係る発電用原子炉設置者の設計及び工事に係る品質管理の方法及びその検査のための組織の技術基準に関する規則」及び「同規則の解釈」に基づく品質保証活動により、十分な品質を確保している。

デジタル安全保護系は、ソフトウェアの品質を高めるために、定周期処理、シングルタスク構成、割り込み処理を設けない簡素なソフトウェア処理構造にするとともに、可視化言語の適用により、第三者による確認、検証を容易としている。

また、デジタル安全保護系に採用予定の制御装置は、国内では原子力プラントの計測制御系及び安全保護系において多くの稼動実績を有しているが、これまでソフトウェアに起因する故障は発生しておらず、十分に高い信頼性が実証されている。

これらに加えて、デジタル安全保護系のソフトウェアの品質を確保するために、「安全保護系へのディジタル計算機の適用に関する規程」（JEAC4620-2008）に基づき以下の品質保証活動を実施する。

・ソフトウェアのライフサイクルのプロセス（設計、製作、試験、装荷、運転、変更、廃止）における品質管理方法を予め定め、実施するとともにその結果を文書化し管理する。
・各々のプロセスでのアウトプットについては、構成管理手法を予め定め、それに従ってソフトウェアの構成を管理する。
・設計、製作、試験、変更のプロセスの過程で、「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」（JEAG4609-2008）に基づく検証及び妥当性確認(V&V)を実施する。

3. 安全保護系ソフトウェアの品質保証活動

3.1 ライフサイクルプロセス

デジタル安全保護系のソフトウェアに対して、設計、製作、試験、装荷、運転、変更、廃止のライフサイクルを通じて品質の管理方法を定め、実施するとともに、その結果を文書化する。

3.1.1 設計プロセス

デジタル安全保護系の設計プロセスは、安全保護系のシステム要求事項に基づき、各々の設計アウトプットを文書化するとともに、システムの機能、多重性・独立性等が満足していることを確認する。

(1) システム設計要求仕様

「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」（以下、設置許可基準規則）、「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」（以下、技術基準規則）、「安全保護系へのディジタル計算機の適用に関する規程」（JEAC4620-2008）、「原子力発電所安全保護系の設計規程」（JEAC4604-2009）、「安全保護系基本設計要求」などのシステム要求事項に基づき、多重性・独立性の実現要求、安全保護系の機能要求などのデジタル安全保護系のシステム設計要求仕様を「基本設計方針書」として文書化する。

これらの文書は、システム要求事項を満足していることを確認する。

(2) ハードウェア・ソフトウェア設計要求仕様

システム設計要求仕様に基づき、多重性・独立性の具体的実現要求、安全保護系の作動ロジックの具体的機能要求などのデジタル安全保護系のハードウェア・ソフトウェア設計要求仕様を「ブロック図」として文書化する。

これらの文書は、システム設計要求仕様を満足していることを確認する。

3.1.2 製作プロセス

ソフトウェア設計要求仕様の文書から専用のツールを用いて、自動的にソフトウェアを製作する。製作したソフトウェアは、「ソフトウェア図」として文書化する。

これらの文書は、ソフトウェア設計要求仕様どおりに作成されていることを確認する。

専用のツールは、「実用発電用原子炉に係る発電用原子炉設置者の設計及び工事に係る品質管理の方法及びその検査のための組織の技術基準に関す

る規則」及び「同規則の解釈」に基づく品質保証活動により、適切に品質管理されたツールを使用する。

3.1.3 試験プロセス

製作したソフトウェアと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どおりに製作されていることを試験によって確認する。本プロセスでは、試験の対象範囲、実施要領、判定基準について「試験要領書」として文書化する。

これらの文書は、上流の要求事項、設計要求仕様を満足する試験内容であることを確認する。

また、「試験要領書」に基づき試験を実施し、判定基準内であることを確認し、その結果を「試験成績書」として文書化し、管理する。

(1) ハードウェア・ソフトウェア統合試験

デジタル安全保護系に対して、入出力機能試験、シーケンス・スタティック試験等を実施し、本設備に正しくソフトウェアが装荷されていることを確認する。

a. 入出力機能試験

外部から模擬入力を与え、ハードウェア入力とソフトウェア入力が一致することを確認する。

b. シーケンス・スタティック試験

デジタル安全保護系に対して、「ブロック図」に基づき、模擬信号を入力した後の出力信号を確認することにより、ソフトウェアで構成されるロジックが正しく動作すること、及び多重性を確保していること等を確認する。

(2) 組合せ試験

デジタル安全保護系、伝送装置等を組合せた状態で試験を実施し、応答性、故障時の機能等を確認し、デジタル安全保護系が正しく機能することを確認する。

3.1.4 装荷プロセス

デジタル安全保護系を発電所に搬入・装荷し、現場機器との接続を行う。本設備のソフトウェアの復元が妥当であること（工場出荷時の状態に復元されていること）を下記の試験によって確認する。

(1) 装置復元試験

据付けられたデジタル安全保護系に対して、自己診断機能による制御装置の健全性の確認、及び最新のソフトウェアが装荷されていることの確認を実施し、工場出荷時の状態に復元されていることを確認する。

本プロセスでは、装置復元試験に対して、作業、試験の内容を「要領書」として文書化する。

これらの文書は、正しく作成されていることを確認する。

また、「要領書」に基づき作業、試験を実施した結果を「報告書」又は「成績書」として文書化し、管理する。

3.1.5 運転プロセス

各プロセスを経て、デジタル安全保護系が正常に動作することが確認された後、プラントでの運転に用いる。

運転プロセスの期間中、デジタル安全保護系が健全に機能していることを定期的に確認する。本プロセスでは、この検査、試験の内容を「要領書」として文書化し、検査、試験を実施する。これらの文書は、正しく作成されていることを確認する。

また、検査、試験を実施した結果を「報告書」又は「成績書」として文書化し、管理する。

3.1.6 変更プロセス

デジタル安全保護系のソフトウェアの変更が生じた場合には、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、実施内容に応じて必要とされる各々のプロセスを順次推進する。この場合、各々のプロセスでの文書、ソフトウェアの変更を3.2項に示すソフトウェア構成管理に基づき行う。また、変更範囲について、必要に応じ3.3項に示す検証及び妥当性確認(V&V)を実施する。

3.1.7 廃止プロセス

デジタル安全保護系のソフトウェアの使用を停止し廃止する場合、それを宣言し、他設備への使用がないように管理する。

3.2 ソフトウェア構成管理

(1) 構成管理の実施内容

3.1項に示すソフトウェアライフサイクルの設計、製作、試験、装荷、運転の各プロセスでの文書、ソフトウェアについては、予め構成管理を行う単位を明

確にした上で、文書発行後などをベースラインとして構成管理を開始する。その文書、ソフトウェアの変更においては、構成管理の単位ごとの改訂番号、改訂日付、改訂内容を改訂履歴として文書化し、構成管理の単位ごとに最新の状態であることを管理しながら、承認プロセスを経て発行する。

文書、ソフトウェアに変更が生じた場合は、ライフサイクルプロセスを通じて構成管理の単位ごとの改訂履歴を記録する。

(2) 体制

構成管理を実施する体制は、設計、製作、試験の過程ではメーカにて構成し、運転以降の過程では当社又はメーカにて構成する。

(3) 文書管理

構成管理の開始に当たり、「ソフトウェア構成管理計画書」を文書化する。

また、ソフトウェアを構成する管理対象項目は、「ソフトウェア構成管理計画書」に基づき文書化する。

3.3 検証及び妥当性確認(V&V)

デジタル安全保護系の適用に当たっては、ソフトウェアの品質を確保することが重要であり、安全保護系としての機能を実現するソフトウェアに対して、設計、製作、試験、変更の各サイクルにおいて、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活動として検証及び妥当性確認(V&V)を行う。

検証は、設計、製作過程のステップごとに上位仕様と下位仕様の整合性チェックを主体として、以下の観点から検証作業を行う。

a. デジタル安全保護系システム要求事項がシステム設計要求仕様に正しく反映されていること。
b. システム設計要求仕様がハードウェア、ソフトウェアの設計要求仕様に正しく反映されていること。
c. 上記設計要求仕様に基づいてソフトウェアが製作されていること。
d. 検証及び妥当性確認が可能なソフトウェアとなっていること。

必要な検証を経て製作されたソフトウェアをハードウェアと統合した後の全体システムについて、最終的にデジタル安全保護系システム要求事項が正しく実現されていることの確認をするために、妥当性確認を行う。

(1) 検証と妥当性確認の手順と内容

以下に、検証と妥当性確認の手順と内容を示し、第1図にデジタル安全保護系の設計・製作及び検証と妥当性確認の流れを示す。

検　証　1：安全保護系システムへの要求事項が正しく設備のシステム設計要求仕様に反映されていることを検証
検　証　2：システム設計の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
検証 3、4：ソフトウェア設計要求仕様どおりに正しくソフトウェアが製作されていることを検証。ソフトウェア設計要求仕様図書から自動的にソフトウェアを製作するツールを適用し、ソフトウェアの設計と製作を一体化するため、検証3と検証4は統合
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どお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、デジタル安全保護系システム要求事項を満足していることを確認

(2) 体制

検証及び妥当性確認を実施する体制は、設計、製作、試験の過程ではメーカにて構成し、運転以降の過程では当社又はメーカにて構成することとし、検証及び妥当性確認作業は、設計に携わった人間以外の別の人間又はグループが行うこととする。また、検証及び妥当性確認の実施に関する人員配置及び工程を管理する人間又はグループについても、設計、製作、試験、運転の過程に携わった人間以外の別の人間又はグループとする。

(3) 文書管理

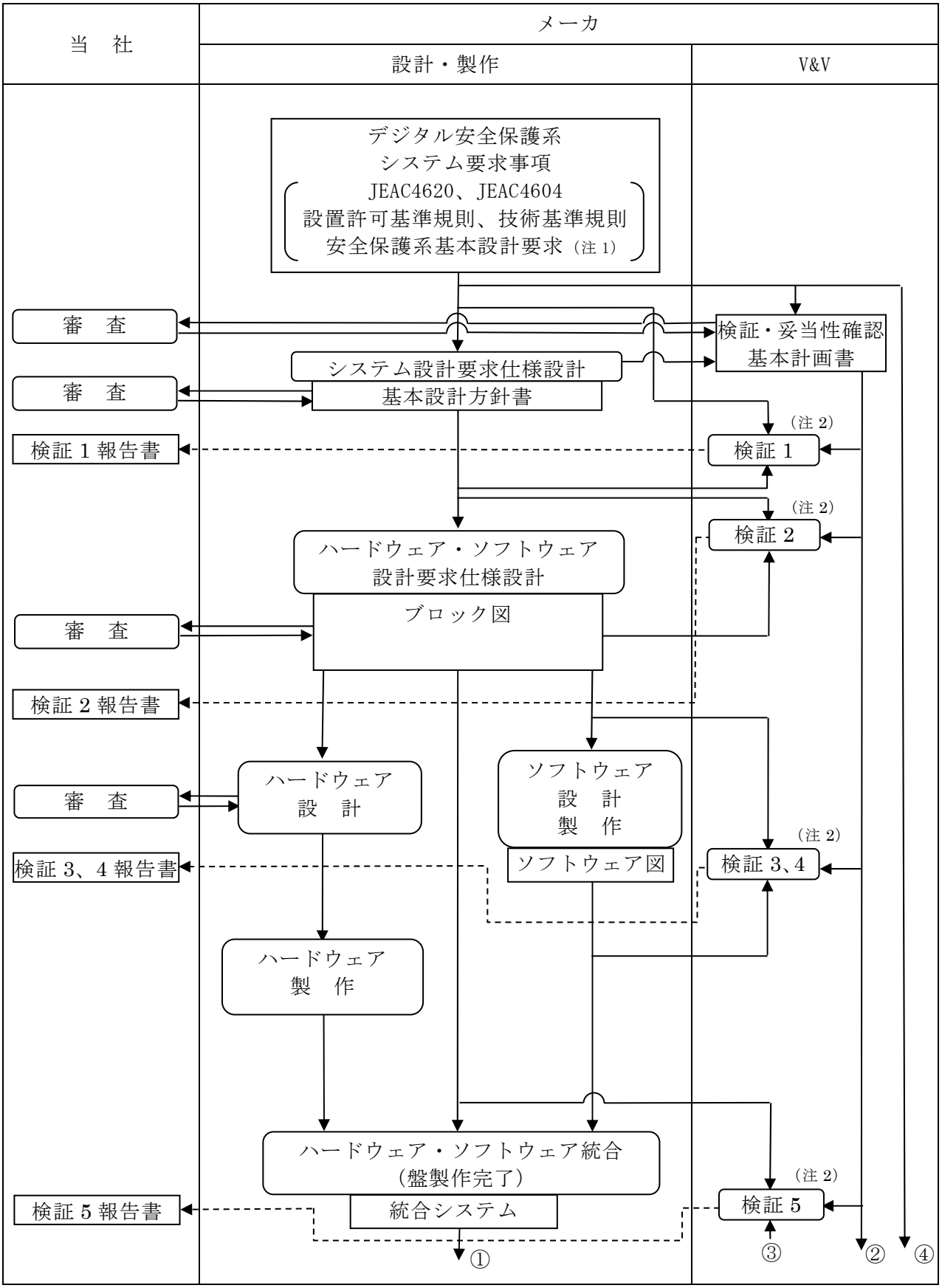
検証及び妥当性確認作業の開始に当たり、検証及び妥当性確認基本計画を「検証・妥当性確認基本計画書」として文書化する。

また、検証及び妥当性確認の各作業実施に当たっては、作業内容、合格基準、不良結果等に対する措置を「検証要領書」として文書化し、各ステップの検証ごとに結果を「検証報告書」として文書化する。

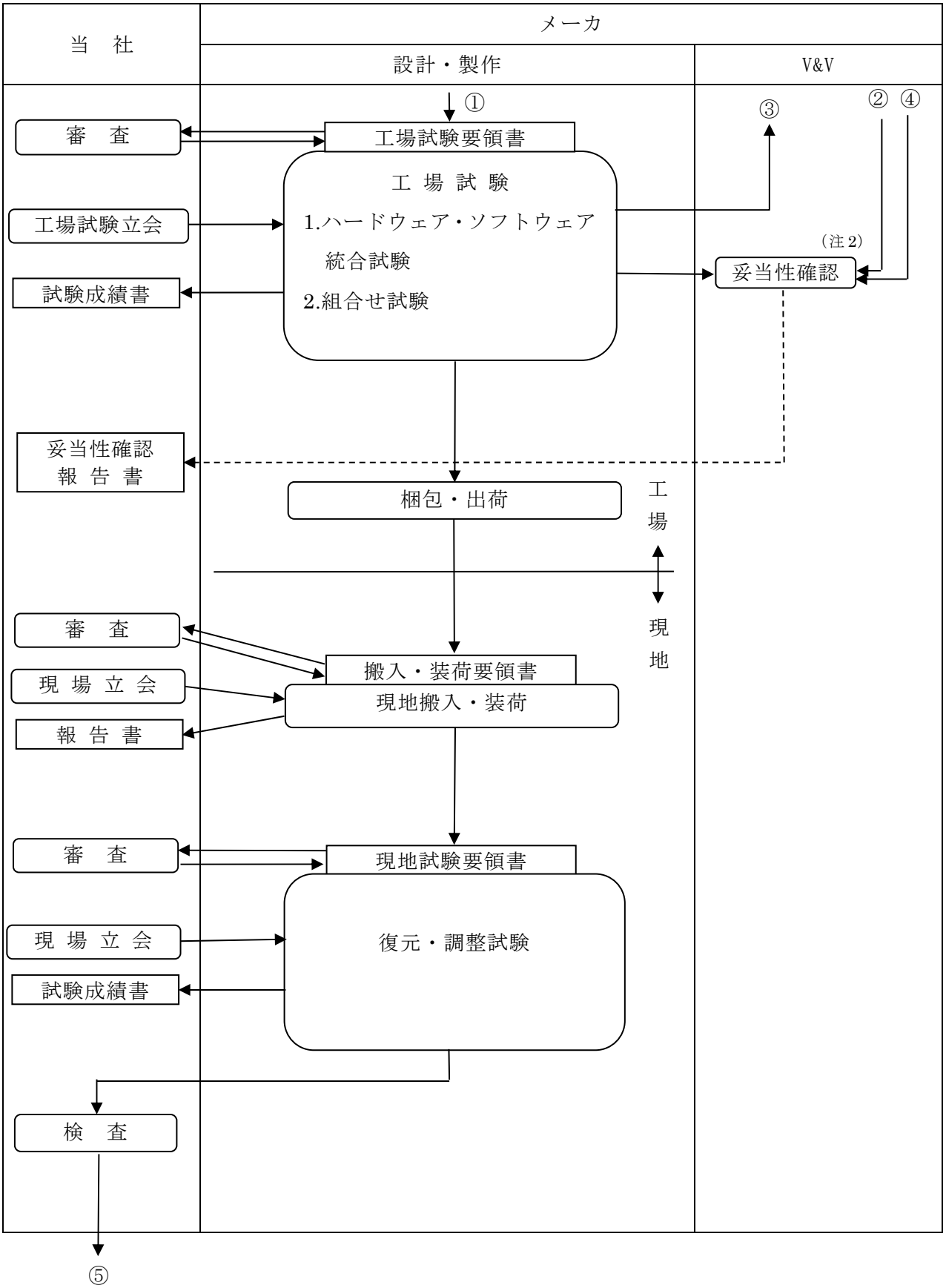
(4) ソフトウェアの再利用

ソフトウェアの再利用時においては、上流図書において要求する再利用範囲が明確に識別され、再利用の妥当性を示す根拠が文書化されていること。

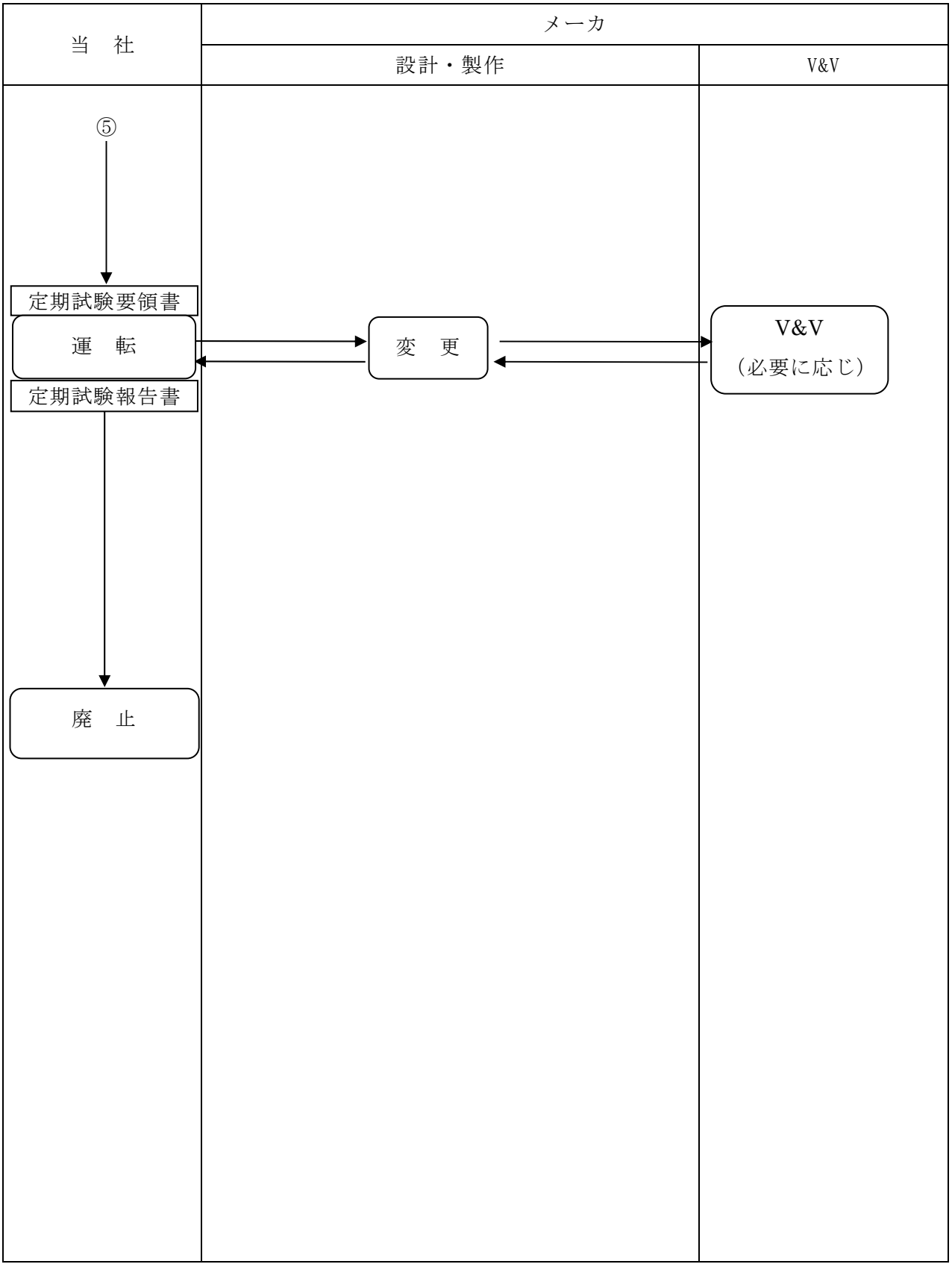
第１図　デジタル安全保護系の設計・製作及び検証と妥当性確認の流れ(1/3)



第１図　デジタル安全保護系の設計・製作及び検証と妥当性確認の流れ(2/3)



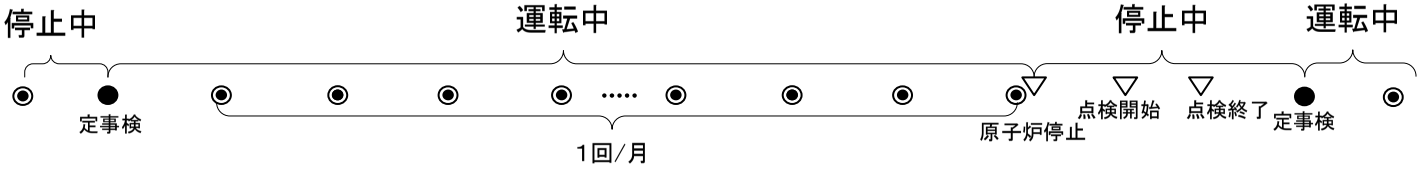
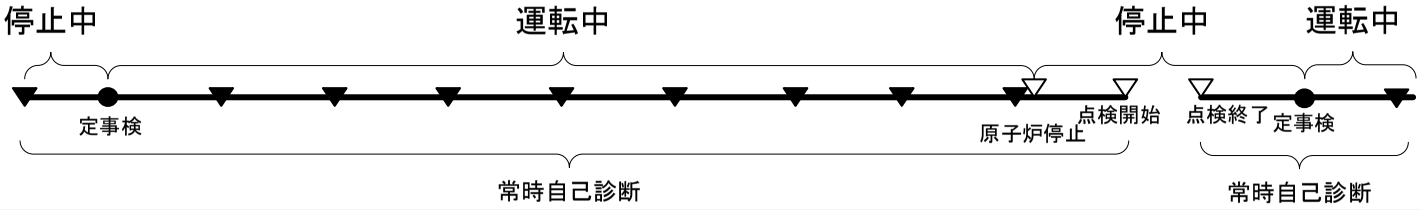
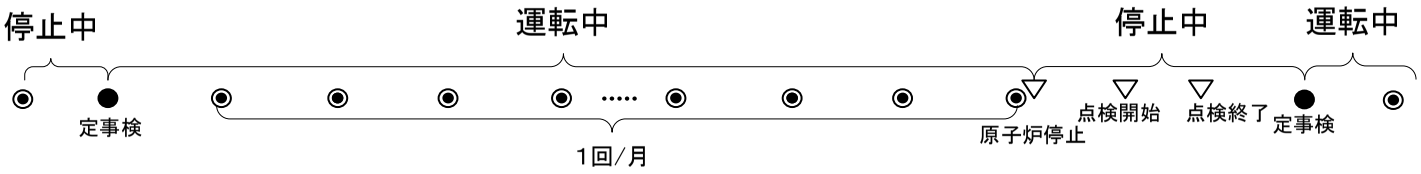
第１図　デジタル安全保護系の設計・製作及び検証と妥当性確認の流れ(3/3)



（注１）システム要求事項を示した図書であり、安全保護系の要求事項を示す基準書として扱う。
（注２）作業内容、合格基準、不良結果等に対する措置を「検証要領書」として文書化する。

運転上の制限を満足していることを確認する確認事項のイメージ

凡例
- ●：定期事業者検査にて実動作確認
- ◉：1回/月の実動作確認
- ━：自己診断にて常時確認
- ▼：外観確認

	確認対象	確認状況	備考
取替前	ソフトウェア部	――― （原子炉保護系論理回路は対象機器なし）	―――
	ハードウェア部		原子炉保護系論理回路にて確認
取替後	ソフトウェア部		検出器毎のチャンネルにて確認 なお、原子炉保護系論理回路の確認に合わせて、マイクロプロセッサ等に物理的な損傷がないことを確認
	ハードウェア部		原子炉保護系論理回路にて確認