| 伊方発電所保安規定審査資料 | |
|---|---|
| 資料番号 | TS(76)-05-05(r4) |

# 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９月

四国電力株式会社

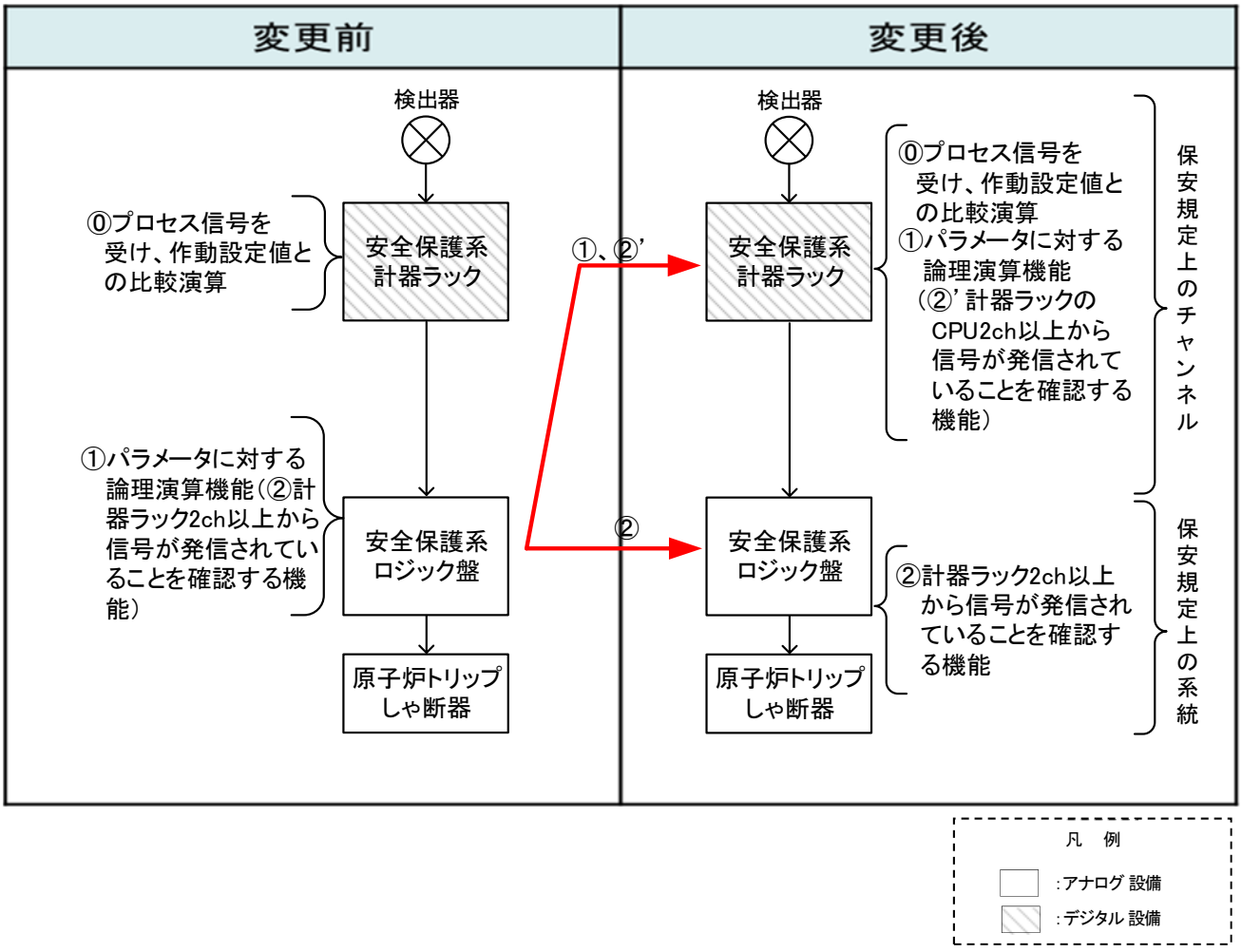
# 目　　次

## 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




保安規定においては、上記の原子炉停止系を「チャンネル」と「系統」に分けて、機能を確認する。

《保安規定　抜粋》

表３３－２　原子炉保護系計装

・チャンネル（代表例として原子炉圧力を記載）

表33－２つづき

| 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 | | | 確認事項 | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | 条件 | 要求される措置 | 完了時間 | 項目 | 頻度 | 担当 |
| 8．原子炉圧力 | 低 | 12.73MPa[gage]以上 | モード１(P-7以上) | 4※17 | 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 | A.1 計装計画課長は，当該チャンネルを動作可能な状態にする。※18 | ６時間 | 設定値確認および機能の確認を行う。 | 定期事業者検査時 | 計装計画課長 |
| | | | | | | | | 動作不能でないことを指示値により確認する。 | １日に１回 | 当直長 |
| | | | | | B. 条件Ａの措置を完了時間内に達成できない場合 | B.1 当直長は，P-7未満にする。 | 12時間 | | | |
| | 高 | 16.61MPa[gage]以下 | モード１および２ | 4※17 | 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 | A.1 計装計画課長は，当該チャンネルを動作可能な状態にする。※18 | ６時間 | | | |
| | | | | | B. 条件Ａの措置を完了時間内に達成できない場合 | B.1 当直長は，モード３にする。 | 12時間 | | | |

※17：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。
※18：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。

・系統

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　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として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として規定している。

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は、別紙－１のとおり、サーベイランスでの確認以外に日常管理も含めて評価している。

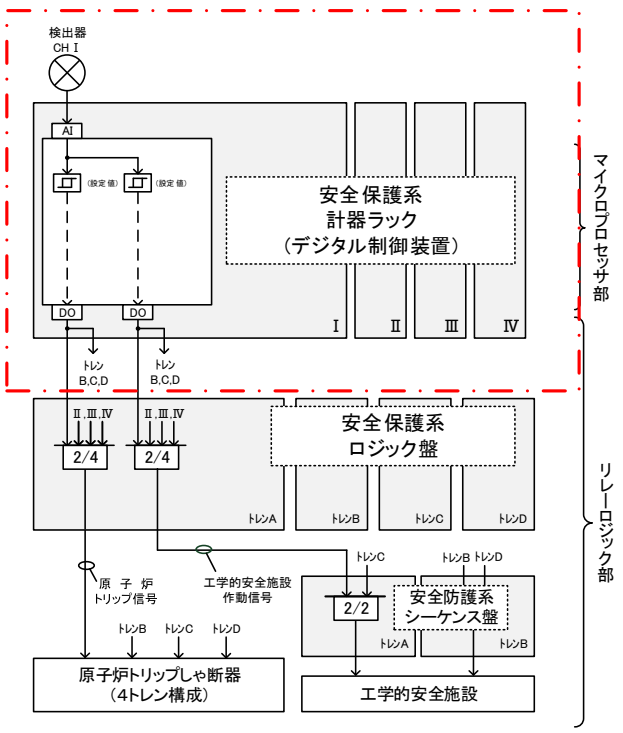
保安規定第３３条(計測および制御設備)表３３－２原子炉保護系計装に必要な性能とは、実用発電用原子炉及びその附属施設の位置、構造及び設備の基準に関する規則にある第２４条（安全保護回路）の機能が健全に作動することである。

原子力規制における検査制度の見直しに伴う保安規定変更認可(令和２年９月)以降の原子炉保護系計装の試験は、保安規定変更認可(令和２年９月)以前の方法と変わらないものの、検出器からの信号を検知して、自動で原子炉トリップするような事故時等の条件が模擬できないため、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として、実条件性能確認を行っている。

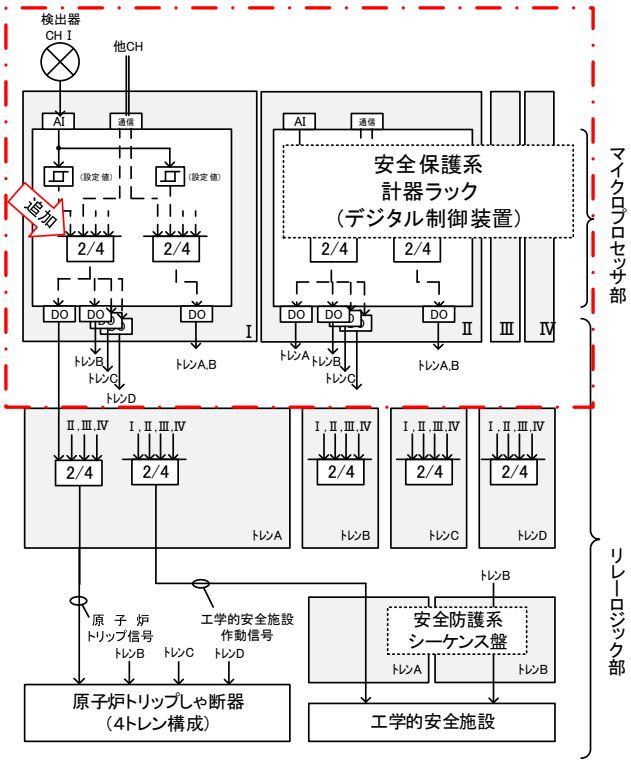
### ２．２　チャンネルの試験について

チャンネルの試験について、取替前は検出器、設定値比較回路および指示計等の機能の確認であったが、取替後は新たにソフトウェアによる論理演算機能の確認が加わる。

＜取替前＞




＜取替後＞



## ２．２．１　取替前後の実条件性能確認に相当する代替の方法について

取替前は、実条件性能確認に相当する代替の方法として、定期事業者検査時の設定値確認、機能の確認および動作不能でないことを１日に１回の指示値により確認するとともに、マイクロプロセッサ部（設定値比較回路を含む）についても、日常管理にて中央制御室に不要な警報が発信していないことにより動作可能であることを確認してきた。

取替後は、新たにソフトウェアによる論理演算機能が加わるが、従来から設定値比較回路の設定値確認にてソフトウェアの実条件性能確認に相当する代替の方法を行っており、確認するための方法は変わるものではない。

取替前後の実条件性能確認に相当する代替の方法について、以下の表に示す。

＜取替前＞

| 確認箇所 | 実条件性能確認に相当する代替の方法 | 具体的内容 |
|---|---|---|
| 伝送器、指示計等（ソフトウェアを含む） | 定期事業者検査時の機能の確認 | ・試験装置を用いて伝送器、指示計等にその動作要素の標準値を与え、その時の当該伝送器、指示計等の出力値を確認する。 |
| 設定値比較回路（ソフトウェア） | 定期事業者検査時の設定値確認 | ・制御装置搭載のアプリケーションソフトウェアの構成管理表の確認およびソフトウェア照合にて設定値確認する。 |
| 伝送器～指示計（経由するソフトウェアの回路も含む） | 動作不能でないことを１日に１回の指示値により確認 | ・中央制御室において指示値を確認する。 |
| マイクロプロセッサ部（設定値比較回路を含む） | 日常管理 | ・中央制御室にて不要な警報（自己診断（30msec に１回）による異常）が発信していないことを確認する。（設定値比較回路は自己診断による異常検知が可能） |

＜取替後＞　　注：表中の赤下線部の確認項目が追加

| 確認箇所 | 実条件性能確認に相当する代替の方法 | 具体的内容 |
|---|---|---|
| 伝送器、指示計等（ソフトウェアを含む） | 定期事業者検査時の機能の確認 | ・試験装置を用いて伝送器、指示計等にその動作要素の標準値を与え、その時の当該伝送器、指示計等の出力値を確認する。 |
| 設定値比較回路および論理演算機能（ソフトウェア） | 定期事業者検査時の設定値確認および機能の確認 | ・制御装置搭載のアプリケーションソフトウェアの構成管理表の確認およびソフトウェア照合にて設定値確認および論理演算機能を確認する。 |
| 伝送器～指示計（経由するソフトウェアの回路も含む） | 動作不能でないことを１日に１回の指示値により確認 | ・中央制御室において指示値を確認する。 |
| マイクロプロセッサ部（設定値比較回路および論理演算機能を含む） | 日常管理 | ・中央制御室にて不要な警報（自己診断（30msec に１回）による異常）が発信していないことを確認する。（設定値比較回路および論理演算機能は自己診断による異常検知が可能） |

（１）論理演算機能の実条件性能確認に相当する代替の方法について

取替前のロジック盤の論理演算機能は、実動作による確認が必要なアナログ制御装置で構成されていることから系統の試験として１ヶ月に１回、論理演算機能の上段からテスト信号を入力し、論理演算機能の

健全性を確認してきた。今回、ロジック盤取替工事により、ロジック盤の論理演算機能を計器ラックに移設し、装置もアナログ制御装置からデジタル制御装置に変更された。

デジタル制御装置のソフトウェアは、経年的に変化するものではないため、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の構成管理を開始し、ソフトウェアを処理するマイクロプロセッサ等が健全に動作していることを確認することで、ソフトウェアにて実現している論理演算機能の確認ができる。使用前事業者検査から始まる各検査で確認する内容、サーベイランスおよび日常管理にて確認する一連の内容を別紙－１に示す。

取替後の計器ラックの論理演算機能は、デジタル制御装置に搭載されることからソフトウェアの構成管理にて健全性の確認が可能であるとともに、ソフトウェアの自己診断（３０msec に１回）機能により、日常管理として、中央制御室の当直員による警報の発信状況の監視にて実施することができる。
万が一、異常を検知した場合は、中央制御室に警報が発信し、速やかに処置が実施できる。このため、日常管理として中央制御室の当直員により、常時、不要な警報が発信していないことを確認することで、マイクロプロセッサ等が健全に動作していることおよび論理演算機能が維持できていることが確認できる。
加えて、系統のサーベイランスの手順の中に、中央制御室にて不要な警報(自己診断による異常)が発信していないことを含めることで、論理演算機能が動作可能であることを記録として保管することとしている。

以上のことから、論理演算機能が運転上の制限を満足していることを確認するための方法は、論理演算機能の上段からテスト信号を入力して性能が維持されていることを確認する方法から自己診断による３０msec に１回の運転状態を監視する方法に変わったものの、実条件性能確認に相当する代替の方法として行うことができる。(実条件性能確認に相当する代替の方法の検証については、別紙－２参照。)

| 確認対象 | | 確認事項 | 確認頻度 |
|---|---|---|---|
| マイクロプロセッサ部 | ソフトウェア（設定値・論理演算機能を含む) | 「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。 | ・定期事業者検査時に確認する。<br><br>および<br><br>・動作不能でないことを１日に１回の指示値により確認する。<br><br>および<br><br>・中央制御室にて不要な警報(自己診断による異常)が発信していないことを確認する。 |
| | マイクロプロセッサ等 | 自己診断機能によりソフトウェアの処理を行うマイクロプロセッサ等が健全であることを確認する。 | |

（2）ソフトウェア照合等の頻度について
従来より、設定値比較回路をソフトウェア照合等にて確認する作業は、プラント運転中においても実施可能であるものの、定期事業者検査時に実施している。
この理由として、プラント運転中に原子炉保護機能に影響する設定値比較回路を変更することはなく、万が一、ソフトウェアを変更する場合は中央制御室に警報が発信することから、ソフトウェアを管理外で変更できない設計となっているためである。
更に、原子炉保護機能に影響する設定値比較回路を変更となるようなソフトウェアのアップデートが必要となる場合は、ソフトウェアをインストールする前に検証及び妥当性確認を実施し、設定値比較回路上段からテスト信号を入力し、要求される機能を満足していることを使用前事業者検査にて確認する。加えて、ソフトウェアが動作していることは自己診断機能により３０msec に１回確認している。
このことから、ソフトウェアで実現された設定値比較回路の確認の頻度は、定期事業者検査時に実施することは妥当であり、これまでの運転経験を踏まえても、運用している。

なお、ソフトウェアは、「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に問題ないことを確認するとともに、当該のソフトウェアは、ＲＯＭに記録されることから経年的に変化することはなく、また、３０msec に１回の自己診断機能による誤り検出コードの確認に加えて、定期事業者検査において照合試験等を実施していることから、ソフトウェアの変化がないことは確認できている。

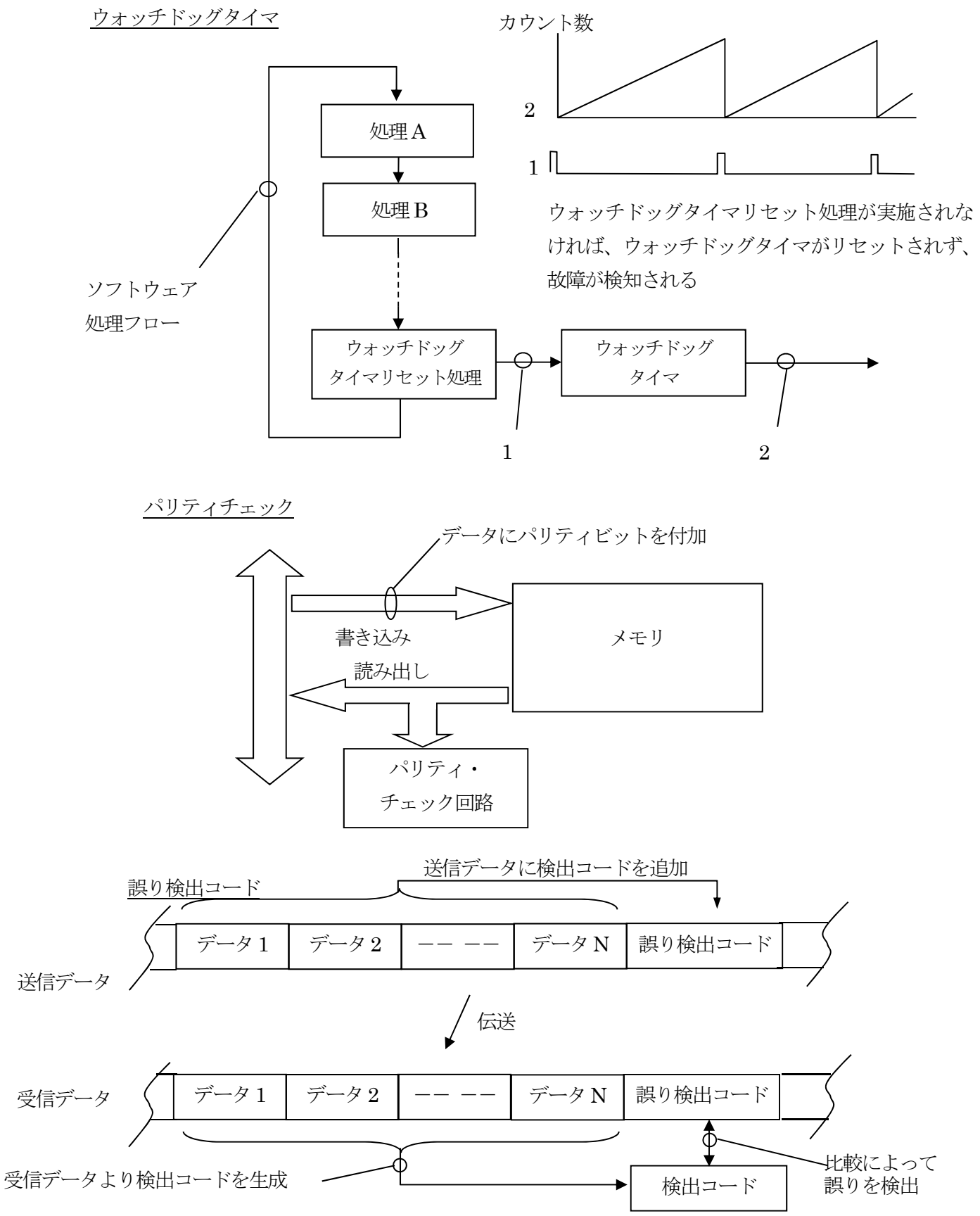
（3）自己診断機能について

デジタル安全保護系のマイクロプロセッサ等の故障に関しては、偶発的な故障の早期発見のため自己診断機能を設け、プラント運転中に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について、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」より抜粋し、第１表に示す。

また、経年劣化による故障への対応は、施設管理の保全プログラムにより適切に保守、交換を実施することとしている。

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

## ２．２．２　ソフトウェアで実現された論理演算機能を日常管理とする理由

取替前のロジック盤の論理演算機能は、系統の試験として、１カ月に１回、論理演算機能の上段からテスト信号を入力し、健全性を確認することで、運転上の制限を満足していることを確認してきたが、取替後の計器ラックの論理演算機能は、従来実施していたチャンネルの日常管理にて健全性を確認することにしており、以下に確認方法について整理する。

（1）保安規定の確認事項の目的

保安規定第１１条第２項にて、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。

（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。

以上より、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。

（2）保安規定の確認事項の方法

運転上の制限を満足していることの確認は、以下の理由から系統にて実施していた月例で実施する定期試験（以下、「月例のサーベイランス」という。）からチャンネルの日常管理に変更する。

・保安規定変更に係る基本方針には、「運転上の制限を満足していることの確認は、これまでもサーベイランスでの確認以外でも巡視点検等により実施されており、例えば、運転員、保修員による日常の巡視により設備の不具合が確認された場合は、サーベイランスによる設備の健全性確認にかかわらず運転上の制限からの逸脱を宣言し適切な処置を実施している。」と記載されており、運転上の制限を満足

していることを確認する方法として、日常管理についても有効である。

・運転上の制限を満足していることの確認は、原子力規制における検査制度の見直しに伴う保安規定変更認可の審査において、実条件性能確認に相当する代替の方法として、日常管理、巡視点検、月例のサーベイランスおよび定期事業者検査時に行う試験の組み合わせにて確認することで、実条件性能の確認ができると評価している。

・取替前において、ロジック盤のアナログ制御装置で構成された論理演算機能が動作可能であることの確認は、論理演算機能の上段からテスト信号を入力して、性能が維持されていることを確認するため、月例のサーベイランスで確認していた。

　取替後においては、計器ラックの論理演算機能がデジタル制御装置へ変更されたことから、動作可能であることの確認は、自己診断（３０msec に１回）機能により、日常管理として、中央制御室の当直員による警報の発信状況の監視にて実施することができる。

なお、日常管理とは、保安規定第１２条の２第１項（１）号の運転管理業務等において実施される。

（運転管理業務）
第 12 条の２　各課長は，運転モードに応じた原子力安全への影響度を考慮して原子炉施設を安全な状態に維持するとともに，事故等を安全に収束させるため，運転管理に関する次の各号の業務を実施する。
(1) 当直長は，原子炉施設（(4)号で定める設備を除く）の運転に関する次の業務を実施する。
　(a) 中央制御室における監視，第 13 条第１項および第２項の巡視点検によって運転監視を実施し，その結果，機器に異状があれば関係各課長に連絡する。
　(b) 警報発信時の対応を実施する。
　(c) 設備故障および事故発生時の対応を実施する。

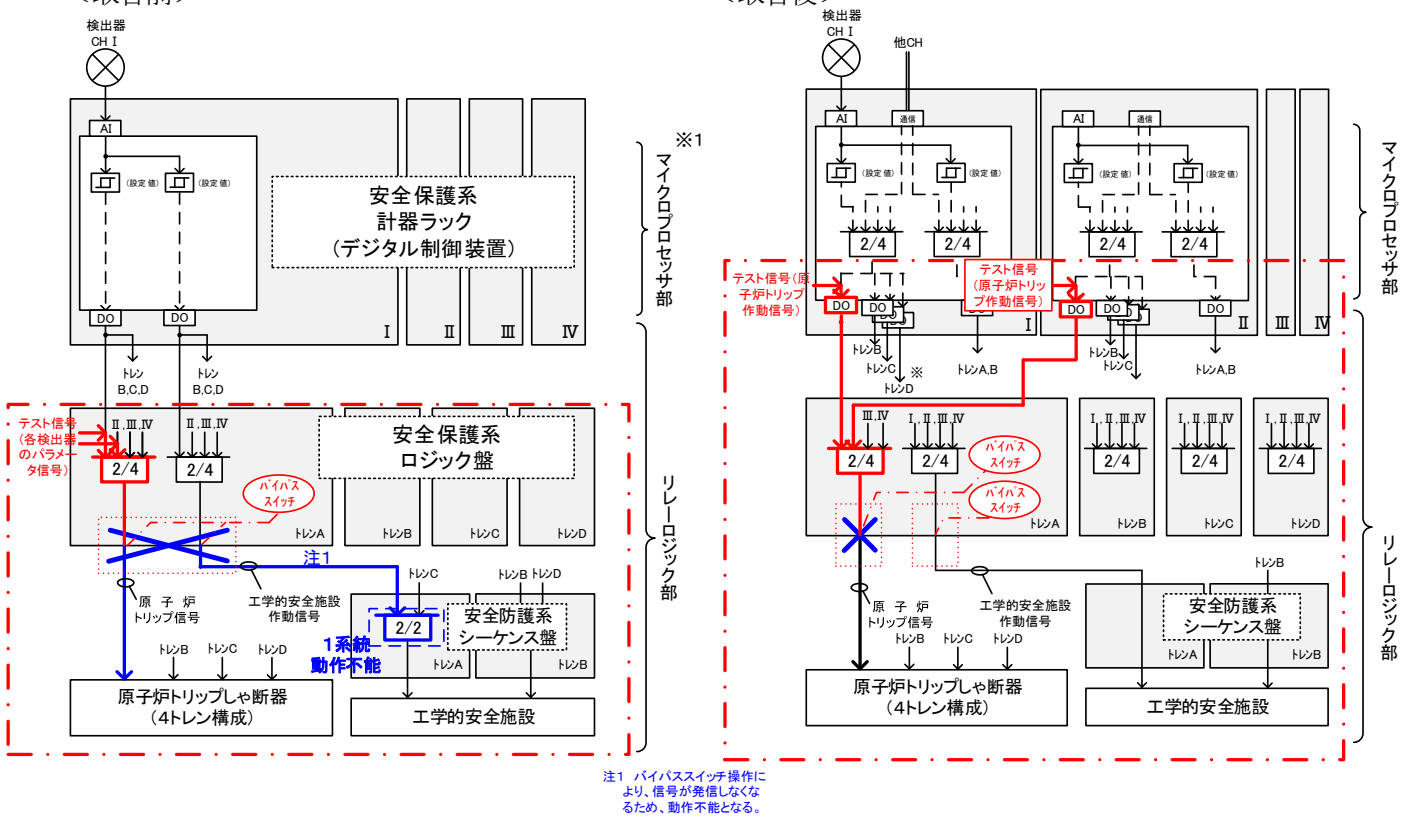
（中略）

(5) 各課長は，第３節（第86条から第89条を除く）各条第２項の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原子炉施設の定期的な試験・確認等の計画を定め，実施する。なお，原子炉起動前の施設および設備の点検については，第16条に従い実施する。

## ２．３　系統の試験について

系統の試験は以下のとおり実施する。入力箇所がチャンネルから入力するように変更となっているものの、ロジック盤の保障回路へテスト信号を模擬入力し、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表示等の発信により確認する方法は、取替前と同等の試験となっている。なお、取替前後で、機能を確認する頻度に変更はない。（１カ月に１回）

＜取替前＞　　＜取替後＞




＜取替前＞

| 確認箇所 | 実条件性能確認に相当する代替の方法 | 具体的内容 |
|---|---|---|
| ・ロジック盤の論理回路（論理演算機能を含む）<br>・原子炉トリップしゃ断器 | 定期事業者検査時の原子炉保護系論理回路の試験（全系統を行う。） | ・ロジック盤の論理演算機能の上流からテスト信号を入力し、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確認し、論理演算機能が問題ないことを確認する。 |
| ・ロジック盤の論理回路（論理演算機能を含む）<br>・原子炉トリップしゃ断器 | 月例の原子炉保護系論理回路の試験（1ヶ月に2トレンを交互に行う。） | ・ロジック盤の論理演算機能の上流からテスト信号を入力し、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確認し、論理演算機能が問題ないことを確認する。 |
| ・ロジック盤<br>・原子炉トリップしゃ断器 | 日常管理 | ・中央制御室にて不要な警報（電源異常等）が発信していないことを確認する。 |

＜取替後＞

| 確認箇所 | 実条件性能確認に相当する代替の方法 | 具体的内容 |
|---|---|---|
| ・ロジック盤の保障回路<br>・原子炉トリップしゃ断器 | 定期事業者検査時の原子炉保護系論理回路の試験（全系統を行う。） | ・計器ラックの論理演算機能の下流からテスト信号を入力し、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。 |
| ・ロジック盤の保障回路<br>・原子炉トリップしゃ断器 | 月例の原子炉保護系論理回路の試験（1ヶ月に2トレンを交互に行う。） | ・計器ラックの論理演算機能の下流からテスト信号を入力し、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。 |
| ・ロジック盤<br>・原子炉トリップしゃ断器 | 日常管理 | ・中央制御室にて不要な警報（電源異常等）が発信していないことを確認する。 |

## 3. まとめ

ロジック盤取替前後において、取替前は系統として管理していたロジック盤の論理演算機能を、取替後は計器ラックの論理演算機能として、チャンネルにて管理する。

チャンネルの確認方法は、新たに論理演算機能の確認方法が加わるものの、従来から設定値比較回路にてソフトウェアの実条件性能確認に相当する代替の方法を行っており、実条件性能確認する方法が変わるものではない。

また、論理演算機能の確認方法は、系統の月例のサーベイランスからチャンネルの日常管理となるものの、運転上の制限である機能が動作可能であることの確認は、日常管理にて確認することができる。

系統の確認方法は、取替前と同様に実動作にて確認している。

このことから、一部の機能の設備構成が変更となるものの、下記の表のとおり取替後のチャンネルの確認方法と系統の確認方法を組み合わせて実施することで取替前の原子炉停止系の試験と比較しても漏れなく機能の確認ができている。

以上の整理を踏まえて、保安規定への反映箇所を検討したところ、運用は現状の保安規定の記載に含まれるため、保安規定の記載を変更しなくても問題ない。

＜取替前後の原子炉停止系の確認方法＞　　注：表中の赤字下線部の確認項目が追加

| 区分 | 取替前の確認方法 | 取替後の確認方法 |
|---|---|---|
| チャンネル※ | 定期事業者検査時<br>・制御装置搭載のアプリケーションソフトウェアの構成管理表の確認およびソフトウェア照合にて設定値を確認する。<br>・試験装置を用いて伝送器、指示計等にその動作要素の標準値を与え、その時の当該伝送器、指示計等の出力値を確認する。<br>１日に１回<br>・中央制御室にて指示値を確認する。<br>日常管理<br>・不要な警報（自己診断による異常（30msec に１回））が発信していないことを確認する。（設定値比較回路は自己診断による異常検知が可能） | 定期事業者検査時<br>・制御装置搭載のアプリケーションソフトウェアの構成管理表の確認およびソフトウェア照合にて設定値および論理演算機能を確認する。<br>・試験装置を用いて伝送器、指示計等にその動作要素の標準値を与え、その時の当該伝送器、指示計等の出力値を確認する。<br>１日に１回<br>・中央制御室にて指示値を確認する。<br>日常管理<br>・不要な警報（自己診断による異常（30msec に１回））が発信していないことを確認する。（設定値比較回路および論理演算機能は自己診断による異常検知が可能） |
| 系統 | 定期事業者検査時<br>・実動作による機能確認する。（全系統）<br>１カ月に１回<br>・実動作による機能確認する。（１カ月に２系統を交互に行う）<br>・不要な警報が発信していないことを確認する。<br>日常管理<br>・不要な警報（電源異常等）が発信していないことを確認する。 | 定期事業者検査時<br>・実動作による機能確認する。（全系統）<br>１カ月に１回<br>・実動作による機能確認する。（１カ月に２系統を交互に行う）<br>・不要な警報が発信していないことを確認する。（チャンネルのソフトウェアの自己診断機能による警報を含む。）<br>日常管理<br>・不要な警報（電源異常等）が発信していないことを確認する。 |

※　取替前は系統として管理していた論理演算機能を、取替後はチャンネルとして管理する

以上

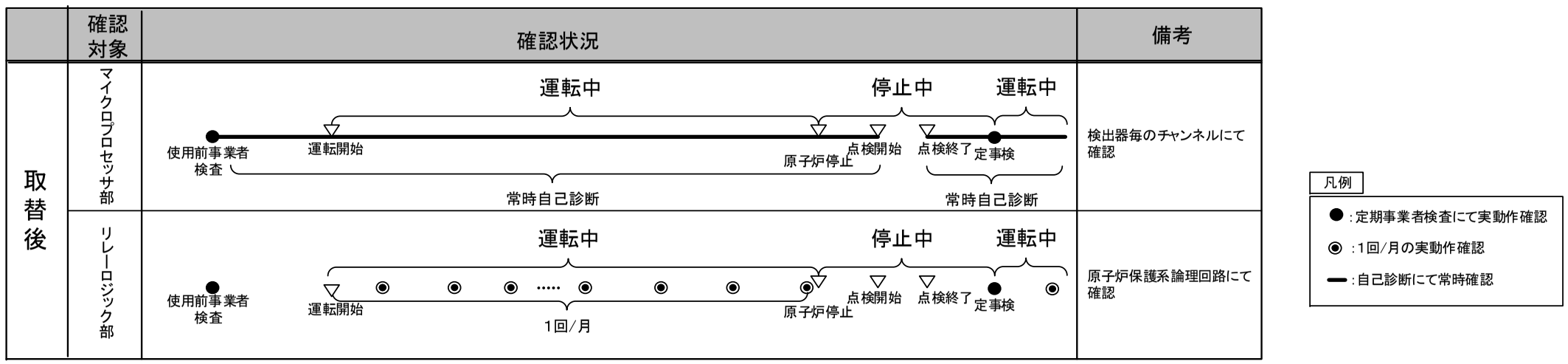
# 確認事項の整理

青字：マイクロプロセッサ部の健全性確認
赤字：リレーロジック部の健全性確認

＜取替後＞

| 系統名 | 実条件性能<br>（要求事項） | 区分 | 使用前事業者検査<br>（判定基準） | 定期事業者検査<br>（判定基準） | サーベイランス等<br>（判定基準） | 「実条件性能確認」適合の考え方<br>実条件性能確認との差異 | 「実条件性能確認」適合の考え方<br>実条件性能確認評価 |
|---|---|---|---|---|---|---|---|
| 第33条<br>計測および制御設備<br>（表33-2<br>原子炉保護系計装） | 【技術基準規則】<br>第35条(安全保護装置)<br><br>以下に設工認要求事項を抜粋する。なお、本資料においては原子炉保護系の機能として原子炉停止系統を説明する。<br><br>1.3 安全保護装置等<br>1.3.1 安全保護装置<br>(1) 安全保護装置の機能及び構成<br>安全保護装置は、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、その異常な状態を検知し、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工学的安全施設を自動的に作動させる設計とする。<br><br>1.3.3 試験及び検査<br>安全保護装置のうち原子炉保護装置は、各チャンネルのトリップ状態を模擬するテストスイッチ及び原子炉トリップ遮断器は“2 out of 4”ロジックを構成することにより、発電用原子炉の運転中にも原子炉保護装置の論理回路<br>及び原子炉トリップ遮断器に関する試験ができる設計とする。 | チャンネル | 【原子炉保護設備ロジック回路動作検査】(機能・性能検査)<br>＜判定基準＞<br>(a)トリップステータス、安全保護系ロジック盤のチャンネルトリップ動作表示灯が点灯すること<br>(b)警報(パーシャル、ファーストアウト)が発信すること<br>(c)原子炉トリップ遮断器UVコイル電圧計がOV相当になること<br>(原子炉トリップ遮断器が開放すること ※)<br>※検査において実動作の確認を1回以上行う。 | 【安全保護系設定値確認検査】<br>＜判定基準＞<br>(1) 設定値確認検査<br>・指示値または動作値は、保安規定に定める設定値を満足するほか、そのセット値に許容範囲(計器許容誤差)を加味した値が許容範囲内であること<br>・ソフトウェア設定値については、各制御装置搭載のアプリケーションソフトウェアと保守ツールに保管されているマスタソフトウェアが一致すること<br>(2) 伝送器性能検査<br>各点の出力値が許容誤差範囲内であること<br>(3) 指示監視計器性能検査<br>各点の指示値が許容誤差範囲内であること<br>【プラント状態監視設備機能検査】<br>＜判定基準＞<br>1. 特性検査<br>(1) 圧力・水位・流量監視計器性能検査<br>・指示計の各点の指示値が計器許容誤差範囲内<br>(2) 温度監視計器性能検査<br>・指示計の各点の指示値が計器許容誤差範囲内<br>2. 機能・性能検査<br>(1) 計測範囲確認検査<br>・検出器の検知レベルが許容誤差範囲内<br>(2) 事故時試料採取設備運転性能検査<br>C/V 内の気体が試料採取設備に吸引されること | 【サーベイランス】(1日に1回以上)<br>＜試験方法＞<br>・発電日誌による記録採取<br>＜判定基準＞<br>・各計器の値により動作不能でないこと<br><br>【日常管理】<br>＜試験方法＞<br>・常時中央制御室で警報確認する。<br>＜判定基準＞<br>・不要な警報(自己診断による異常)が発信していないこと。(常時) | ・原子炉運転中に原子炉保護系ロジック回路(論理演算機能+保障回路)を自動的に一気通貫で作動させること(論理演算機能の上流からテスト信号を入力する方法)は、以下の理由から実施することは原子力安全上困難である。<br>・保障回路のロジックが2/4から1/3相当となることから、誤動作率が上がり、設備の安全性に影響を及ぼす。 | 左記確認を原子炉運転中に実施することは原子力安全上および困難であることから実条件性能確認に対しては下記の通り実施する。<br><br>【定事検】<br>＜マイクロプロセッサ部＞<br>・各制御装置搭載のアプリケーションソフトウェアの構成管理票の確認およびソフトウェア照合により、原子炉保護設備ロジック回路動作検査時点からのソフトウェアに変更がないことを確認することで、ソフトウェアの健全性(論理演算機能の健全性)を確認する。<br>＜リレーロジック部＞(全トレン行う)<br>・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。<br>【月例】<br>＜リレーロジック部＞(1 ヶ月に 2 トレンを交互に行う。)<br>・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。<br>【日常管理】<br>・発電日誌による記録確認等、中央制御室において定期的にパラメータ監視をしている。<br>・不要な警報(自己診断による異常)が発信していないこと。(常時)<br>(・運転中に、ソフトウェアを変更しようと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確認している。<br>・計器ラックに備わっている自己診断機能(30msecの周期で実施)で計器ラックのマイクロプロセッサ等が健全であることを確認している。万が一、健全性が損なわれることとなれば中央制御室へ警報が発信する。)<br><br>・不要な警報(電源異常等)が発信していないことを確認する。(常時)<br><br>以上の組み合わせにより、原子炉保護系計装回路の実条件性能を確認していると整理する。 |
| | | 系統 | 【原子炉保護設備ロジック回路動作検査】(機能・性能検査)<br>【安全保護系ロジック盤ロジック回路動作検査(原子炉保護系)】<br>＜判定基準＞<br>b. 安全保護系ロジック盤ロジック回路動作検査(原子炉保護系)<br>(a)安全保護系ロジック盤のチャンネルトリップ動作表示灯が点灯すること<br>(b)原子炉トリップ遮断器UVコイル電圧計がOV相当になること<br>(原子炉トリップ遮断器が開放すること ※)<br>※検査において実動作の確認を各トレン1回以上行う。 | 【原子炉保護系ロジック検査】(全トレン行う。)<br>＜判定基準＞<br>a. トリップ状態表示およびロジック状態表示が点灯すること(手動要素)<br>b. ファーストアウト警報が発信すること(手動要素)<br>c. 原子炉トリップしゃ断器の「緑」表示または『W』ランプが消灯すること(手動要素およびPの各組合せ確認) | 【原子炉トリップ回路ロジック検査】(1 ヶ月に2 トレンを交互に行う。)<br>＜判定基準＞<br>a. トリップ状態表示およびロジック状態表示が点灯すること(手動要素)<br>b. ファーストアウト警報が発信すること(手動要素)<br>c. 原子炉トリップしゃ断器の「緑」表示または『W』ランプが消灯すること(手動要素およびPの各組合せ確認)<br><br>【日常管理】<br>＜試験方法＞<br>・常時中央制御室で警報確認する。<br>＜判定基準＞<br>・不要な警報(電源異常等)が発信していないこと。(常時) | | |

上記の表では、安全保護系計器ラック(以下、「計器ラック」という。)のソフトウェアで実現した論理回路を「論理演算機能」という。また、ロジック盤にあるリレー回路を「保障回路」という。



＜取替前＞

| 系統名 | 実条件性能<br>（要求事項） | 区分 | 定期事業者検査<br>（判定基準） | サーベイランス等<br>（判定基準） | 「実条件性能確認」適合の考え方 | |
|---|---|---|---|---|---|---|
| | | | | | 実条件性能確認との差異 | 実条件性能確認評価 |
| 第 33 条<br>計測および制御設備<br>（表 33-2<br>原子炉保護系計装） | 【技術基準規則】<br>第 35 条(安全保護装置)<br><br>以下に設工認要求事項を抜粋する。なお、本資料においては原子炉保護系の機能として原子炉停止系統を説明する。<br><br>1.3 安全保護装置等<br>1.3.1 安全保護装置<br>(1) 安全保護装置の機能及び構成<br>安全保護装置は、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、その異常な状態を検知し、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工学的安全施設を自動的に作動させる設計とする。<br><br>1.3.3 試験及び検査<br>安全保護装置のうち原子炉保護装置は、各チャンネルのトリップ状態を模擬するテストスイッチ及び原子炉トリップ遮断器は“2 out of 4”ロジックを構成することにより、発電用原子炉の運転中にも原子炉保護装置の論理回路<br>及び原子炉トリップ遮断器に関する試験ができる設計とする。 | チャンネル | 【安全保護系設定値確認検査】<br>＜判定基準＞<br>(1) 設定値確認検査<br>・指示値または動作値は、保安規定に定める設定値を満足するほか、そのセット値に許容範囲（計器許容誤差）を加味した値が許容範囲内であること<br>・ソフトウェア設定値については、各制御装置搭載のアプリケーションソフトウェアと保守ツールに保管されているマスタソフトウェアが一致すること<br>(2) 伝送器性能検査<br>・各点の出力値が許容誤差範囲内であること<br>(3) 指示監視計器性能検査<br>・各点の指示値が許容誤差範囲内であること<br>【プラント状態監視設備機能検査】<br>＜判定基準＞<br>1. 特性検査<br>(1) 圧力・水位・流量監視計器性能検査<br>・指示計の各点の指示値が計器許容誤差範囲内<br>(2) 温度監視計器性能検査<br>・指示計の各点の指示値が計器許容誤差範囲内<br>2. 機能・性能検査<br>(1) 計測範囲確認検査<br>・検出器の検知レベルが許容誤差範囲内<br>(2) 事故時試料採取設備運転性能検査<br>・C/V 内の気体が試料採取設備に吸引されること | 【サーベイランス】（1日に1回以上）<br>＜試験方法＞<br>・発電日誌による記録採取<br>＜判定基準＞<br>・各計器の値により動作不能でないこと<br><br>【日常管理】<br>＜試験方法＞<br>・常時中央制御室で警報確認する。<br>＜判定基準＞<br>・不要な警報（自己診断による異常）が発信していないこと。（常時） | 原子炉運転中に原子炉保護系ロジック回路をすべて自動的に作動させることは、以下の理由から実施することは原子力安全上困難である。<br>・原子炉トリップしゃ断器1台が動作している状態が長期間に渡るため、誤動作率が上がり、意図しないプラントの緊急停止に至るリスクがある。 | 左記確認を原子炉運転中に実施することは原子炉安全上困難であることから実条件性能確認に対しては下記の通り実施する。<br><br>【定期事業者検査】(全トレン行う)<br>・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。<br>【月例試験】<br>（1ヶ月に 2トレンを交互に行う。）<br>・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。<br>【日常管理】<br>・発電日誌による記録確認等、中央制御室において定期的にパラメータ監視をしている。<br>・不要な警報（自己診断による異常）が発信していないこと。（常時）<br>・不要な警報（電源異常等）が発信していないことを確認する。（常時）<br><br>以上の組み合わせにより実条件性能を確認していると整理する。 |
| | | 系統 | 【安全保護系機能検査】<br>＜判定基準＞<br>a. トリップステータスが点灯すること<br>b. 警報（パーシャル、ファーストアウト）が発信すること<br>c. 原子炉トリップ遮断器UVコイル電圧計がOV相当になること<br>（原子炉トリップ遮断器が開放すること ※）<br>※検査において実動作の確認を1回以上行う。 | 【原子炉トリップ回路ロジック検査】（1ヶ月に 2トレンを交互に行う。）<br>＜判定基準＞<br>a. トリップステータスが点灯すること<br>b. 警報（パーシャル、ファーストアウト）が発信すること<br>c. 原子炉トリップ遮断器UVコイル電圧計がOV相当になること<br>（原子炉トリップ遮断器が開放すること ※）<br>※検査において実動作の確認を1回以上行う。<br><br>【日常管理】<br>＜試験方法＞<br>・常時中央制御室で警報確認する。<br>＜判定基準＞<br>・不要な警報（電源異常等）が発信していないこと。（常時） | | |

# デジタル制御装置による実条件性能確認に相当する代替の方法の検証について

## 1. はじめに

取替前のロジック盤の論理演算機能は、実動作による確認が必要なアナログ制御装置で構成されていることから系統の試験として1ヶ月に1回、論理演算機能の上段からテスト信号を入力し、論理演算機能の健全性を確認してきた。今回、ロジック盤取替工事により、ロジック盤の論理演算機能を計器ラックに移設し、装置もアナログ制御装置からデジタル制御装置に変更されたため、変更前後で論理演算機能として以下の通り特徴が変更されている。

| 設備(論理演算機能)の変更前後の特徴 | |
|---|---|
| 取替前 | 取替後 |
| アナログ制御装置 | デジタル制御装置 |
| 論理演算機能の動作可能性は、アナログ部品であることから設備を運転することで確認していた。 | 論理演算機能の動作可能性は、ソフトウェアで実現されていることから、常時（自己診断）確認することができる。 |
| 確認頻度は1カ月に1回 | 確認頻度は常時（30msecに1回） |
| 論理演算回路の故障時は、中央制御室に警報が発信しない。 | 論理演算機能の故障時は、中央制御室に警報が発信する。 |
| 論理演算機能により原子炉トリップしゃ断器を動作させる。 | 論理演算機能および保証回路により原子炉トリップしゃ断器を動作させる。 |

## 2. 実条件性能確認に相当する代替の方法について

変更前後の論理演算機能の特徴を踏まえて、以下の代替の方法を検討する。

| デジタル制御装置のソフトウェアを用いた実条件性能確認に相当する代替の方法 |
|---|
| ソフトウェアは、経年的に変化するものではないため、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の構成管理を開始し、ソフトウェアを処理するマイクロプロセッサ等が健全に動作していることを確認することにより、ソフトウェアにて実現している論理演算機能が動作可能であることが確認できる。 |

## 3. 代替の方法の検証について

代替の方法を実施するに当たって、実条件性能確認するための十分な方法であることを検証する。

検証1. 取替前は論理演算機能が実動作することで動作可能を確認できたが、
取替後は論理演算機能が実動作はしていないにも関わらず、動作可能であることが確認できる理由について

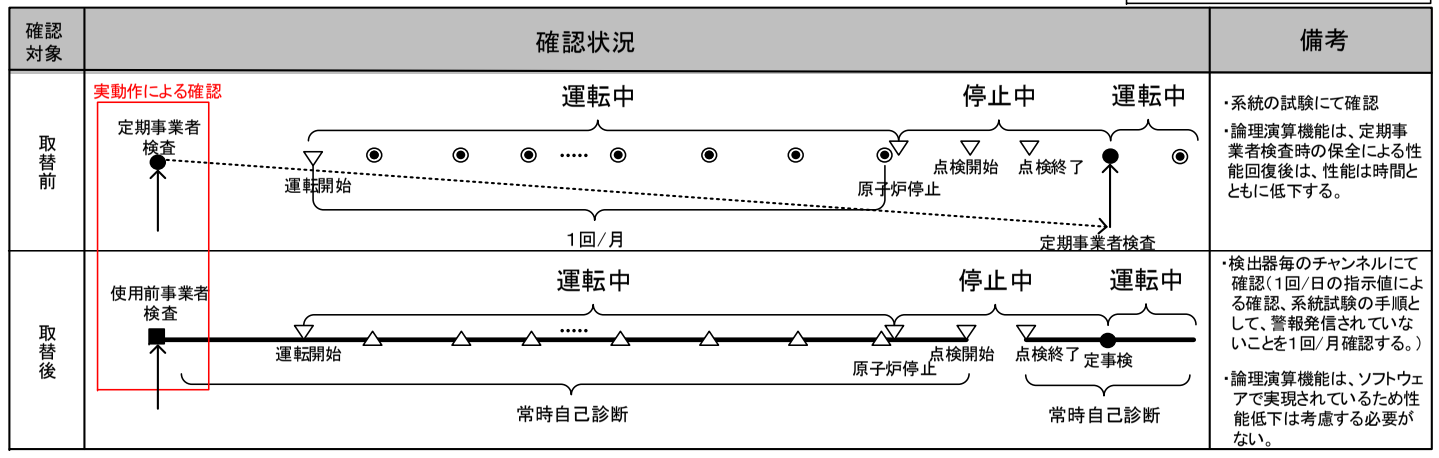
結果1. デジタル制御装置のソフトウェアは、経年的に変化するものではないため、ソフトウェアに変更がないこと、またはソフトウェアの処理をするマイクロプロセッサ等に偶発的な故障がない限りは、論理演算機能の動作可能性は維持されるものである。

このため、論理演算機能の動作可能性は、論理演算機能上段からテスト信号を入力し、実動作による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開始し、ソフトウェアを処理するマイクロプロセッサ等が健全に動作していることを確認することにより、維持できる。

これは、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。）においても、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、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は認められている。ガイドは、検査の確認として記載されているが、論理演算機能の作動の状況（動作可能）を確認するための方法として、使用前事業者検査等に限ったものではない。



凡例
- ■：使用前事業者検査にて実動作確認
- ●：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（1回/日の指示値による確認も含む）
- △：警報発信されていないことの確認（系統試験の手順内）




検証2. ソフトウェアに変更またはソフトウェアの処理をするマイクロプロセッサ等に偶発的な故障がないことを確実に確認できる理由について

結果2. 以下の理由から、確実に確認できる。

①ソフトウェアに変更がないことの確認

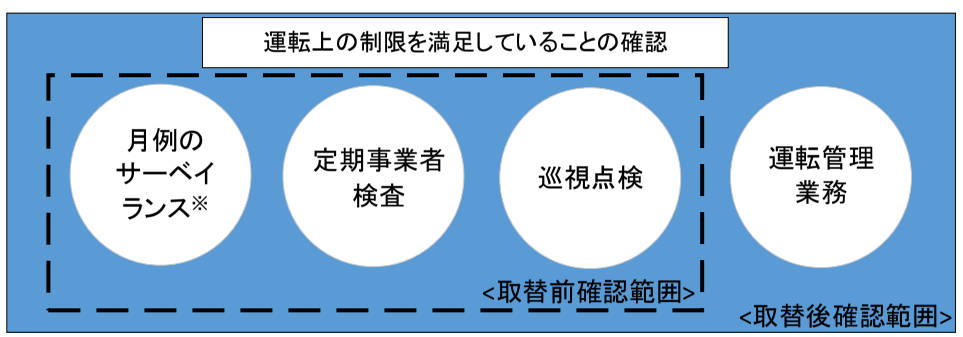
・ソフトウェアが変更する要因として、人為的な変更がある。人為的には、通常、プラント運転中に原子炉保護機能に影響する論理演算機能を変更することはない。万が一、ソフトウェアを変更する場合は中央制御室に警報が発信するため確実に確認できる。

②マイクロプロセッサ等に偶発的な故障がないことの確認

・電源、ファンユニット等の異常が発生した際には30msecに1回の自己診断機能による中央制御室へ警報を発信するため確実に確認できる。また、自己診断機能が停止するような故障が発生した場合でも、他チャンネルの計器ラックにより故障した計器ラックの異常を検知する自己診断機能が備わっているため、対応できる。

検証3. 論理演算機能が動作可能であることを確認する方法について

結果3. 取替前の論理演算機能は、1カ月に1回のサーベイランスおよび定期事業者検査により確認していた。
取替後の論理演算機能は、ソフトウェア上で実現されていることから、万が一、論理演算機能が偶発的に故障となった場合はマイクロプロセッサは停止することとなり、ソフトウェアを経由している指示計にも影響を与える。このため、論理演算機能が動作可能であることの確認は、チャンネルのサーベイランスである動作不能でないことを1日に1回の指示値により確認することができる。
　加えて、系統のサーベイランスの試験手順の一部として、自己診断による異常の警報がでていないことを確認することにより、確実に記録として保管されるとともに、新たに日常管理（運転管理業務）として、当直員が論理演算機能の動作可能性について管理することができることとなるため、これまで以上に、運転上の制限を満足していることの確認はできる。




※　取替前において、論理演算機能の確認は、系統のサーベイランスとして1カ月に1回の頻度で実施していた。
取替後において、論理演算機能の確認は、チャンネルのサーベイランスとして1日に1回の指示値により確認できるとともに、系統のサーベイランスの試験手順の一部として、中央制御室にて不要な警報（自己診断による異常）が発信していないことを確認することにより、論理演算機能が動作可能であることを記録として保管される。

以上より、デジタル制御装置のソフトウェアを用いた実条件性能確認に相当する代替の方法は、運転上の制限である論理演算機能の動作可能性の確認として、十分な方法である。