2021年9月1日
四国電力株式会社

# 伊方3号炉　安全保護系ロジック盤取替保安規定審査　コメント一覧

| No | 原子力規制庁コメント | | | 回答 | 反映先の資料名 | 該当ページ |
|---|---|---|---|---|---|---|
| | 日付 | 該当資料 | 内容 | | | |
| 1 | 8/17<br>ヒアリング | 審査資料TS(76)-05-05 | プラント運転中におけるソフトウェア照合の実施が可能か不可能かについて、審査資料に記載すること。 | ソフトウェア照合の実施が可能な旨を審査資料の2.2.1(2)に追加する。 | 審査資料TS(76)-05-05 | 5頁 |
| 2 | 8/17<br>ヒアリング | 審査資料TS(76)-05-05 | F－ROM(フラッシュROM)の用途、使用方法について、資料にまとめること。 | 本コメント一覧表の別紙－1にて回答する。 | 別紙－1 | ― |
| 3 | 8/17<br>ヒアリング | 審査資料TS(76)-05-05<br>P12 | 「ソフトウェアのアップデートが必要となる場合は、速やかに検証および妥当性確認を実施し」とあるが、具体的にソフトウェアをインストールする前に検証および妥当性確認を実施することを審査資料に記載すること。 | 審査資料に記載を追加する。 | 審査資料TS(76)-05-05 | 5頁 |
| 4 | 8/17<br>ヒアリング | 審査資料TS(76)-05-05<br>P13 | 「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」とあるが、経年的に劣化と記載すると、施設管理について説明しているとみることもできる。2．2項は施設管理を説明する項ではないことから、記載内容について検討すること。 | 経年的に劣化ではなく、偶発的な故障であるため記載を修正する。 | 審査資料TS(76)-05-05 | 6頁 |
| 5 | 8/17<br>ヒアリング | 審査資料TS(76)-05-05 | 偶発事象に対して、自己診断機能が果たす役割について、審査資料に記載すること。 | No4にあわせて記載を修正する。 | 審査資料TS(76)-05-05 | 6頁 |
| 6 | 8/17<br>ヒアリング | 審査資料TS(76)-05-05 | 初期不良(エージング等)、経年劣化(保守管理)の内容について、用語解説もつけたうえで、審査資料本文とは分け、別資料でまとめること。 | 本コメント一覧表の別紙－2にて回答する。 | 別紙－2 | ― |
| 7 | 8/17<br>ヒアリング | 審査資料TS(76)-05-05<br>P15 | 「以上より、～同等の機能の確認ができている」の2行について、「3．まとめ」に記載できるよう内容を整理のうえ、同項に記載すること。(2．2項の同2行は削除する。) | 「3.まとめ」に記載をまとめる。 | 審査資料TS(76)-05-05 | 12頁 |
| 8 | 8/17<br>ヒアリング | 審査資料TS(76)-05-05 | サーベランスについての保安規定の変更がないことから、運用の変更がないとの申請になっているが、計装ラック内の論理回路のサーベイランスはどのようにしているのか、整理し説明すること。(実条件性能試験か、代替の方法か) | 日常管理として振り分けるため、その理由について説明する。また、運用は現状の保安規定の記載に含まれるため、記載は現状のままとする。詳細については別紙－3および審査資料にて説明する。 | 別紙－3<br>審査資料TS(76)-05-05 | ・審査資料<br>8頁～9頁、12頁 |

資料－1

別紙－１

# F-ROM(フラッシュ ROM)の用途、使用方法について
# （8/１７ヒアリングコメント回答 No.2)

## １．フラッシュメモリ

論理演算機能は、安全保護系計器ラック（以下、「計器ラック」という。）のＣＰＵカード内蔵のフラッシュメモリ（以下、「Ｆ－ＲＯＭ」という。）に保存されている。

Ｆ－ＲＯＭは、不揮発性メモリであるリードオンリーメモリ（以下、「ＲＯＭ」という。）の１種であるが、データの書き換えができるＲＯＭである。

## １．１．ソフトウェア変更について

ソフトウェア変更は、ソフトウェアを変更するツールを用いて工場や現地にて作成したソフトウェアを計器ラックにダウンロードすることにより、Ｆ－ＲＯＭのデータが書き換わる。なお、ダウンロード後にソフトウェアの変更を有効化するためには、ＣＰＵを再起動する必要がある。

また、不用意な書き換えを防止するため、計器ラック内に設けられているハードウェアスイッチ（接続許可スイッチ、書き込み許可スイッチ）による操作※および専用ツールログイン時のパスワード管理によるセキュリティ機能を持たせた運用としている。

※操作時には中央制御室へ警報が発信する仕様となっている。

## １．２．フラッシュメモリに関する自己診断機能について

フラッシュメモリに関する自己診断機能について、以下に例を示す。

ＲＯＭガードエラー：

通常Ｆ－ＲＯＭはＲＯＭであるため、ソフトウェアがＲＯＭ領域に対して書き換えを行うことはなく、本診断によりＲＯＭ領域への書き換えを検知することでハードウェアまたはソフトウェアの誤動作を検出することができる。

Ｆ－ＲＯＭ書き換えエラー：

Ｆ－ＲＯＭ内容書き換え時に、規定時間待ってもＦ－ＲＯＭ内容が書き込んだ内容と一致しないことを検知し、フラッシュメモリ素子の健全性を確認している。

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。

以上

別紙－２

# 初期故障、経年劣化故障および偶発故障への対応について
# （8/１７ヒアリングコメント回答 No.6）

## 故障への対応

故障には、故障率曲線（バスタブ曲線）によると初期故障、経年劣化による故障、偶発故障に区分することができる。計器ラックにおける各々の故障への対応を以下に示す。

初期故障への対応としては、製品出荷までにエージング（２０００時間）を実施し、初期故障をなくすこととしている。

経年劣化による故障への対応としては、保安規定の施設管理に基づき、運転経験、使用環境、劣化故障モード等を考慮した保全計画を策定し、盤点検（電源電圧測定、演算周期測定等）や部品取替を行うこととしている。

使用部品および機器は可能な限り長寿命（定期取替が不要）であるものを使用しているが、供用期間中において経年劣化による故障が想定される部品（電源ユニット、ファンユニット用ヒューズ等）については、予防保全（時間基準保全）にて定期取替を行うことで経年劣化による故障への対応を行っている。

保全計画において部品取替を行うこととした部品の偶発故障への対応として、自己診断機能を設け、電源、ファンユニット等の異常が発生した際には中央制御室へ警報を発信する設計としている。また、警報発信後は、速やかに予備品への取替を行い復旧することとしている。

以上

# 安全保護系ロジック盤取替における論理回路が「動作可能であること」の確認行為について

○「サーベイランス」については、保安規定第 86 条にて「運転上の制限を満足していることの確認事項」としている。

（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。

○また、第 87 条第２項のとおり第２項で定める事項が実施されていない期間においても，「運転上の制限」を判断するとしている。
この判断は、「サーベイランス」以外の日常管理（警報、パラメータ、運転状況等）などから総合的に判断することとしている。

（運転上の制限を満足しない場合）
第 87 条 運転上の制限を満足しない場合とは，各課長が第３節第 19 条から第 85 条の２の第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をいう。なお，各課長は，この判断を速やかに行う。
２ 各課長は，この規定第２項で定める事項が実施されていない期間においても，運転上の制限に関係する事象が発見された場合は，運転上の制限を満足しているかどうかの判断を速やかに行う。

○ロジック盤取替後の論理回路（論理演算機能および保障回路）における「動作可能であること」の確認については以下のとおり。
ロジック盤取替前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は、取替後は計器ラックのソフトウェアに移設するとともに、取替後のロジック盤は新たに計器ラックのマイクロプロッセッサ故障等による原子炉トリップしゃ断器の誤動作等を防ぐためのリレー回路（保障回路）を設置する。ロジック盤取替後は、論理演算機能をチャンネル、保障回路を系統と整理し、機能毎に確認を実施する。
・チャンネル（論理演算機能）
常時運転状態の回路であり、論理演算機能が動作可能であることを実動作により確認した時点から、計器ラックの自己診断により、論理演算機能が動作可能であることが維持されていることを日常管理で確認する。
・系統（保障回路）
待機状態にある回路であり、保障回路が動作可能であることを実動作により１ヵ月に１回のサーベイランスで確認する。
以上より、チャンネルは論理演算機能の確認を日常管理で、系統は保障回路の機能の確認を１ヵ月に１回のサーベイランスで実施することにより、「動作可能であること」を確認し、保安規定第８６条第１項および第８７条第２項の定めのとおり、「運転上の制限」に対して、適切に管理している。

＜参考＞
運転機器のサーベイランスは、事故時に要求される系統構成や起動条件等を一定頻度で確認し、運転状態に問題がないことは日常管理として確認している。（運転状態を確認するサーベイランスを規定していない。）

（原子炉補機冷却海水系）
第 67 条 モード１，２，３および４において，原子炉補機冷却海水系は，表 67－１で定める事項を運転上の制限とする。
２ 原子炉補機冷却海水系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，次の各号を実施する。
(1) 発電課長は，定期事業者検査時に，施錠等により固定されていない原子炉補機冷却海水系の流路中の弁が正しい位置にあることを確認する。
(2) 発電課長は，定期事業者検査時に，海水ポンプが模擬信号により起動することを確認する。
(3) 当直長は，モード１，２，３および４において，海水ポンプまたは原子炉補機冷却水冷却器の切替を行った場合，切替の際に操作した弁が正しい位置にあることを確認する。

以　上