JEAC4620「安全保護系へのディジタル計算機の適用に関する規程」(制定案)
の公衆審査意見対応について

意見その１

JEAG 4609-200x 及び 4620-200x は，米国の標準審査指針(SRP の 7 章)等を参考に，ディジタル計算機を安全保護系(原子炉保護系や工学的安全施設等)に適用するための規程や，その検証及び妥当性確認に関する指針として作成されたものと考えます。

ここで本規程や本指針は，原子力発電プラントを建設する場合に適用される形になると思いますが，既にディジタル計算機を安全保護系に使用して運転を行っているプラント，並びに安全保護系のディジタル化改造工事を実施するプラントについても，同様に本規程及び本指針を適用する形になると考えて宜しいでしょうか。

回答

基本的には，建設プラント及び安全保護系のディジタル化改造工事を実施するプラントに対して適用するものと考えています。また，本規程，指針は JEAG4604-1993 や JEAG4609-1999 等従来規格に従ったものであり，既設プラントにおいて新規格を適用しても問題ないものと考えております。

意見その２

現在，米国において NRC と事業者側(NEI 等)で実施しているディジタル I &C に関する TWG（タスクワーキンググループ）での議論内容等については，最終的に TWG がクローズしてから JEAG 4609-200x，JEAG 4620-200x にその成果を反映するという理解で宜しいでしょうか。

回答

ご指摘頂いた米国の動向は認知しておりますが，本規程，指針の改訂は，米国の議論の進捗とは必ずしも一致しません。今後，本規定，指針の定期見直しなどで，米国の IEEE 規格などを参考とし，必要に応じて内容を反映することとします。

意見その３

本文，3.2 節の検証に記載されています「～ソフトウェアの設計・製作・変更の各過程～」の ”設計・製作・変更 ” の項目に， ”試験 ” を追加する方が好ましいと考えます。
(JEAG 4609-200x でも試験が入っております)

回答

本規程は JEAG4604-1993 や JEAG4609-1999 等の従来規格をベースに，ディジタル計算機を適用した原子力発電所の安全保護系に対し，その性能及び信頼度の面から必要とされる事項を規定するものです。

従って，品質保証活動の各プロセスは JEAG4609-1999 の参考図 3 に示した考え方が踏襲されており。3.2 節の「検証」は，設計・製作の各プロセスで発生する作業が対象，また，「妥当性確認」は，試験のプロセスで発生する作業が対象となっています。

しかしながら，今回のご指摘を受け，本規程の内容を見直した結果，3.2 節「検証」，3.3 節「妥当性確認」の用語の定義には上記の意図が十分に反映されていないことがわかりました。そのため，3.2 節の「検証」には試験プロセスを含まないこと，また，3.3 節の妥当性確認は，試験プロセスにおける作業であることを追記したいと考えます。

意見その４

「～満足すること」のように具体的な設備の状態を規定している文章と，「～な設計とすること」と設計行為のみに限定した文章とが混在している。本規定の目的などでは設計行為のみを規定するとは記載されていないため，「～な設計とすること」との表現は，具体的な設備の状態を規定する文末に変更すべきである。具体的な対象は以下。

4.6 故障時の機能
4.8 環境条件
4.12 保護動作の完全性
4.13 手動操作
4.14 動作及びバイパスの表示
4.17 ソフトウェアの管理外の変更に対する防護措置

回答

品質管理等の要求（4.18～21）を除いては，運転中の管理や安全保護系の機器そのものに対する要求も含めて，広義に「設計とすること」で統一します。また，一部「設計であること」という記載も「設計とすること」とします。

意見その５

「ディジタル安全保護系と計測制御系とを部分的に共用する場合には，計測制御系で故障が生じてもディジタル安全保護系に影響のないよう，ディジタル安全保護系と計測制御系を電気的に分離すること。更に，通信を共用する場合にはさらに機能的に分離すること。（解説－6）」については，下線部で「さらに」の言葉が重なっているので，下記のように変更してはどうか。

「……。更に，通信を共用する場合には機能的にも分離すること。」

回答

拝承。

意見その６

（解説－7）で**「ディジタル安全保護系のロジックや設定値はソフトウェアとしてディジタル値で与えられる。ソフトウェアは経年的に変化するものでなく，これをディジタル値として保有している回路も，ディジタル値が変化するような経年変化は極めて生じにくいという特性がある。このため，ディジタル安全保護系のロジック確認や設定値確認は，プラント停止時の定期点検も含め，ソフトウェアコンペアチェックやソフトウェア上でのディジタルデータの確認，自己診断等で実施することが可能である。」**とされているが，本内容が要求に十分に反映されていないため，本文 4.7 は修正すべきと考える。

修正案：「ディジタル安全保護系は，故障信号発生時等の異常時に，安全保護機能の健全性及び多重性の維持が確認できるように原子炉運転中でも試験ができる機能を有していること。なお，原子炉運転中において設定値確認及びロジック確認ができるため試験は実施する必要はない。」

回答

コメントは，ディジタル安全保護系の特徴を考慮した試験とすべきとの趣旨と考えますが，“運転中の”設定値確認やロジック確認については，現状も特に要求された項目ではなく，追記しなくても良いと考えます。

意見その7

本規程で非常用電源に対し「高度の信頼性を有する」ことを要求するわけではなく，非常用電源（保安電源）については，JEAG4603 等他の指針に基づいた設計がなされるものであるため「高度の信頼性を有する」は削除すべきではないか。

回答

拝承。

意見その8

ディジタル安全保護系が有する自己診断機能は，信頼性をさらに向上させるのに有効な一手段であり，安全保護機能ではないことが不明確である。従って，次の通り修正すべきと考える。

「ディジタル安全保護系は，信頼性をさらに向上させる手段として，各チャンネル独立に適切な周期で実施される自己診断機能を有すること。また，~~とし，~~自己診断機能によりディジタル計算機の異常を検知した場合には，ディジタル計算機の異常を運転員へ報告~~を~~する。」（エディトリアルなコメントであるが，報告「を」する。の「を」は不要。））

回答

文章を分割するよう反映いたします。

なお，解説－11 に既に同様の文面があるため，「信頼性をさらに向上させる手段として，」という文面は追加しないものとします。

また，「報告する」は JEAG4617 の表現に合わせて「告知する」と見直します。解説－11 も併せて見直します。

意見その9

本文，4.15 節の自己診断機能の記載に，自己診断機能よりも安全機能を優先させる意味も含めて，下記の記述を追加しておいた方が好ましいと考えます。「自己診断の機能は，ディジタル計算機がその安全機能を実行する能力に悪影響を及ぼしてはならない。あるいは安全機能の誤動作を引き起こす要因となってはならない。」

(IEEE Std 7-4.3.2-2003 にも同様の記載があります)

回答

安全保護系は，4.1 節に記載の通り，高い信頼性を有するよう要求されており，更に，解説－11 に，自己診断機能は「システムの信頼性を更に向上させる有効な一手段である」と記載しています。それらから，安全機能に悪影響を及ぼさないということを読み取れると思われますので，現状のままと致します。

意見その 10

文末が「～すること」との要求事項の表現になっていない。また，文章が長いので前後２文に分けて，一例として下記のようにしてはどうか。

「ディジタル安全保護系は，各チャンネル独立に適切な周期で実施される自己診断機能を有すること。自己診断機能によりディジタル計算機の異常を検知した場合には，ディジタル計算機の異常を運転員へ報告すること。（解説－11）」

回答

拝承。

意見その 11

表現が適切ではないと思われる箇所が確認されました。

「ディジタル安全保護系は，外部ネットワークと遮断することにより外部影響の防止された設備であること。」とありますが，文章内容からすると，「ディジタル安全保護系は，外部ネットワークと遮断することにより外部からの影響を防止し得る設備であること。」がより適切な表現ではないかと考えます。

回答

拝承。

意見その 12

「ディジタル安全保護系に装荷するソフトウェアは，管理外の変更に対して適切な防護措置を講じ得る設計とすること。(解説－12)」については「適切な」と「講じ得る」とが重なり非常に間接的な表現になっているが，そこまでの配慮は不要と考えるので，以下に変更してはどうか。「‥‥，管理外の変更に対して適切な防護措置を講じること。」

回答

意見その４の回答に準じます。

意見その 13

省令については，「改訂」ではなく「改正」の用語が適切ではないか。

回答

拝承。

意見その 14

記載ミスと思われる箇所が確認されました。

解説－2 に句点がありません。「…参考図 2 に示す。」

回答

拝承。

意見その 15

記載ミスと思われる箇所が確認されました。

参考図-1,参考図-2 の「－」は，P6 解説-2 の記載内容から不要と思われます。

回答

拝承。

意見その 16

途中で「その品質について第三者への立証性を確保することが必要と考えられる。」と記載されているが，「第三者への立証性」の話は V&V（JEAG 4609）の話であり，本規定での種々の要求事項は「品質の確保」そのものについて必要なものと考えられる。したがって，下記のように変更してはどうか。「その品質を確保することが必要と考えられる。」

回答

拝承。
但し，第三者への立証性確保も重要な事項であるので，以下のように記載を見直します。
「その品質を確保し，またその品質について第三者への立証性を確保することが必要と考えられる。」

意見その 17

記載ミスと思われる箇所が確認されました。
「・安全保護系と計測制御系との信号取り合いは，光／電気変換などのアイソレーシ　ョンデバイスを･･･」と記載がありますが，「アイソレーションデバイス」に不要なスペースが入っており，修正が必要と考えます。

回答

拝承。

意見その 18

１行目「ディジタル安全保護系のソフトウェアの信頼性を確保するために，」については，広い意味で「信頼性」を確保するとの主旨はわかるが，より一般的な用語としては「品質」のほうが適切ではないか。

回答

拝承。

意見その 19

(2)各プロセスで実施すべき品質管理項目のうち，5）運転プロセスについて，以下のとおり追記すべきと考える。
「運転中はシステムに異常が無いことを自己診断機能等により確認する。」

回答

ソフトウェアの品質管理の手段としては，自己診断機能が代表ではないと考えますので，現状のままと致します。

意見その 20

解説-14「参考図 3　ソフトウェアライフサイクルプロセスの状態」に点線で「検証及び妥当性確認の対象」と記されておりますが，「検証及び妥当性確認」は後の「解説-16」に記載されるべき内容であり，「解説-14」の参考図 3 には「検証及び妥当性確認」の注書きは不要と考えます。
もし，参考図 3 に「検証及び妥当性確認の対象」という注書きを残すのであれば，カッコ書き等で「(解説-16 参照)」と後の解説-16 の内容である旨がわかる記載とした方がよいと考えます。

回答

拝承。「（解説-16 参照)」を追記し，後の解説-16 に参考図３を呼び込むよう追記します。

意見その 21

全体的に文章がわかりにくいため，以下の通り修正すべきと考える。
「~~ソフトウェアの構成管理手法の骨子とは，管理対象を決定すること及びトレーサビリティを実現することである。~~

~~すなわち，~~構成管理とは，管理対象要素~~（品質に関する情報を含む。）~~の特定・識別と，要素の管理方法，及びソフトウェア供給者に対する~~全体の~~監査或いは審査方法を予め定め，計画に基づき，実施することである。具体的には以下を示す。

(1) ソフトウェア及び関連文書を特定し，相互に識別~~し，明確な状態にすることを保証~~するために，予め構成管理計画を策定し，実行する。

構成管理計画で，以下の内容を定める。

① ソフトウェア及び関連文書~~など~~について，管理対象~~となる~~要素~~と実施すべき活動~~を定める~~決定する~~。~~ディジタル安全保護系に使用するソフトウェアとして~~管理~~すべき~~対象要素の例としては以下がある。

- 要求仕様
- 設計仕様
- 製作仕様
- 試験仕様／試験結果
- 検証手順／検証結果
- 取扱説明
- 製作したソフトウェア

② ~~（3）各設備単位で，構成~~管理対象~~となる~~要素の管理手法を定める。管理する項目の例~~を~~としては以下~~に示す~~がある。

- ~~レビジョン（~~改訂番号，改訂日付~~）~~
- ~~ステータス（~~変更要求有無，他の管理対象要素との整合状況などの状態~~）~~
- ~~インターフェース（~~他の管理対象要素との取り合い~~）~~

③ ~~（4）~~ソフトウェア~~を~~の変更~~するときの~~手法を定める。

④ ~~（5）ベンダー~~ソフトウェア供給者への~~管理や~~監査或いは審査方法~~など含め，体制を決定する~~定める。

以上の項目を実施するための体制を定める。

回答

拝承。

なお，最後の文章は，管理計画として実施する項目であるので，(2)⑤とします。

「⑤ 以上の項目を実施するための体制を定める。」

意見その 22

記載ミスと思われる箇所が確認されました。

「ディジタル安全保護系に使用するソフトウェアとして管理すべき対象要素の例としては以下がある。」のインデントにずれがあり，修正が必要と考えます。

回答

拝承。

意見その 23

記載ミスと思われる箇所が確認されました。

(1)，(2)のインデントにずれがあり，修正が必要と考えます。

回答

拝承。

意見その 24

表現が適切ではないと思われる箇所が確認されました。

「ここで示したハードウェア設備は，この低い可能性を一層低減するものとして位置付けられるため，原子炉設置者が自主的に整備するものとする。」とありますが，文章内容からすると「整備」ではなく「設置」がより適切な表現ではないかと考えます。

「…原子炉設置者が自主的に設置するものとする。…」

回答

拝承。

意見その 25

表現が適切ではないと思われる箇所が確認されました。

「ここで示したハードウェア設備は，この低い可能性を一層低減するものとして位置付けられるため，原子炉設置者が自主的に整備するものとする。」とありますが，文章内容からすると「整備」ではなく「設置」がより適切な表現ではないかと考えます。

「…原子炉設置者が自主的に設置するものとする。…」

回答

拝承。

意見その 26

表現が適切ではないと思われる箇所が確認されました。

「ここで示したハードウェア設備は，この低い可能性を一層低減するものとして位置付けられるため，原子炉設置者が自主的に整備するものとする。」とありますが，文章内容からすると「整備」ではなく「設置」がより適切な表現ではないかと考えます。

「…原子炉設置者が自主的に設置するものとする。…」

回答

・中央制御盤→中央制御室 ・現場盤，計装盤：BWR/PWR の相違によらない，より一般的な用語とするため，BWR の「原子炉圧力，ドライウェル圧力の監視」及び PWR の「蒸気発生器水位，原子炉圧力の監視」を，いずれも「現場計器の信号を，ソフトウェアを介さずに中央制御室にハードウェアで接続する」と変更します。 ・手動閉止操作→一括手動閉止操作

意見その 27

「ハードウェア設備の範囲は「止める」「冷やす」「閉じ込める」機能の必要最小限の範囲とする。」とありますが，「止める」「冷やす」「閉じ込める」機能について明確な定義も併記したほうがより分かりやすくなると考えます。

具体的には，「「止める」（原子炉の反応度停止），「冷やす」（炉心の冷却），「閉じ込める」（放射能の外部放出防止）機能」という内容の追記です。

回答

拝承。 ただし，「止める（原子炉の緊急停止）」とします。