第15回　計測制御検討会　議事録

1．日時　平成20年1月24日（木）　13:30～18：00

2．場所　日本電気協会　4階　D会議室

3．出席者（敬称略，五十音順）

出席委員：三嶋主査（東京電力），新屋（北陸電力），石合（電源開発），内海（三菱重工業），北村（三菱電機），小山（日立），佐藤（東北電力），滝田（原子力安全基盤機構），田中（原子力技術協会），中川（東京電力），永野（富士電機システムズ），長橋（日本原電），奈良間（中部電力），牧野（原子力安全基盤機構），矢吹（中国電力），渡辺（東芝）（16名）

代理委員：加藤（東芝・鈴木代理），白石（九州電力・岡代理）（2名）

オブザーバ：穐山（原子力技術協会），西（関西電力），原田（日立製作所），藤田（四国電力）（4名）

事　務　局：中島

4．配布資料

資料No.15-1　第14回　計測制御検討会　議事録（案）
資料No.15-2　原子力規格委員会 安全設計分科会 平成20年度活動計画（案）
資料No.15-3-1　JEAC4620およびJEAG4609へのパブリックコメントに対する回答案
資料No.15-3-2　安全保護系へのディジタル計算機の適用に関する規程 JEAC4620-200X
資料No.15-3-3　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 JEAG4609-200X
資料No.15-4　安全機能を有する計測制御装置の設計指針（JEAG4611-1991）改定案について
資料No.15-5-1　原子力発電所の中央制御室における誤操作防止に関する規程（仮称）案に対するコメントへの回答
資料No.15-5-2　JEAG46XX-200X「原子力発電所の中央制御室における誤操作防止に関する規程（仮称）」案
参考資料-1　原子力規格委員会 安全設計分科会 計測制御検討会 委員名簿（案）

5．議事

(1) 検討会委員の変更について

事務局より,参考資料-1に基づき，新委員候補として西氏（関西電力）の紹介があり，正式には安全設計分科会にて承認される旨補足があった。また，代理委員及びオブザーバ参加について報告があり，承認された。

(2) 前回の議事録確認

事務局より，資料No.15-1に基づき，前回（第14回 ）計測制御検討会 議事録（案）（事前に配布しコメントを反映済み）について説明があり，特にコメントなく原案どおり了承された。

(3) 平成19年度活動実績及び平成20年度活動計画について

中川委員より，資料No.15-2に基づき，計測制御検討会における平成19年度活動実績及び平成20年度活動計画について説明があり，特にコメント無く了承された。

また，三嶋主査より，JEAG4621「安全保護系計器のドリフト評価指針」が第27回原子力規格委員会（2007.12.5）で制定されたことを受けて，本指針については，今後定期的にデータを蓄積し，指針の技術的妥当性を評価していくことが重要であるとの補足があった。なお，平成20年度活動計画については，2月の安全設計分科会及び3月の原子力規格委員会での審議経過に応じて，適宜，見直すこととした。

(4) 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」制定案及び JEAG4609「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」改定案の公衆審査意見回答案の審議

加藤代理委員より,資料No.15-3-1，2,3に基づき，JEAC4620制定案及びJEAG4609改定案のパブリックコメントに対する回答案の説明があった。

議論の結果，回答案に対する修正の方向性について合意されたことから，今後検討会としての最終回答案を取り纏め，2月の安全設計分科会に諮ることとした。

（全般）

- No.1回答案は，改定前のJEAG4609に発行年版（1999）を追記する。また，「本規格」を「本規程及び本指針」の記載とする。
- No.2回答案は，回答案の前段に，米国におけるディジタルI&Cに関するタスクワークングの議論について承知していること，またそこでの議論の成果と本規定・指針の内容は必ずしも一致するものではないが，今後定期見直しに合わせて，米国IEEE規格等を参考とし，必要に応じて反映していく旨の記載とする。

これに関する意見は以下のとおりであった。

- No.1回答案は，JEAG4609が現在改定中のところ，“本規格（JEAC4620-200X,JEAG4609-200X）が従来のJEAG4609に従ったものである”旨記載しているが，どの時点のJEAG4609なのか明確でない。

→ 改定前の規格に従っているということを明確にする趣旨から，JEAG4609に発行年版（1999）を付記することでよいのではないか。

- 「本規格」がJEAC4620及びJEAG4609を指していることが明確となるように，「本規程及び本指針」とする方がよい。
- No.2回答案は，本規程及び本指針が国内におけるものというのは当然なので，むしろ回答案の前段には，米国におけるディジタルI&Cに関するタスクワークングの議論について承知していること，またそこでの成果と本規定・指針の内容は必ずしも一致するものではないが，今後定期見直しに合わせて，米国IEEE規格等を参考とし，必要に応じて反映していく旨を追記するほうがよい。
- 国（規制）の議論に民間指針の策定が追従するように，しっかり情報を共有していく必要がある。
- 既設プラントに対しても新規格を適用することが問題ないと回答しているが，JEAG4609については今回の改定でソフトウェアの構成管理について明確にしている。この点は従来のプラクティスにバックフィットしても問題ないか。

→ ソフトウェア構成管理については,既設プラントについても本規程及び本指針同等の管理を実施していることから問題ないと考える。

（JEAC4620）

- No.1回答案は，試験は検証の対象ではなく妥当性確認の対象である旨回答する。
- No.7回答案は，“自己診断機能が安全機能に悪影響を及ぼさないように設計することは重要なことと考えている。本規格では，ディジタル安全保護系に高い信頼性を要求しており，そ

のためシステムの更なる信頼性向上のための有効な一手段として自己診断機能を付加するとしており，これについては解説-11にも記載している”旨を回答する。

・ No.14回答案は，上位規定であるJEAC4620に要求事項を明確にする趣旨から，JEAC4620の解説-3（ディジタル計算機の用語の定義）に品質の確保と，第三者への立証性の確保を併記する。
・ No.16回答案は，「ソフトウェアの信頼性」から「ソフトウェアの品質」へ変更するが，規格案全体について該当箇所が無いか確認する。

これに関する意見は以下のとおりであった。

・ 試験そのものは妥当性確認で良いが，試験仕様については検証が必要ではないか？
→ 実態は上流図書と照合することで試験仕様の検証を行っている。したがって，ここでいう妥当性確認には検証行為が含まれている。
・ 試験仕様の作成は試験プロセスに含まれるもので，妥当性確認の対象に位置づけている。妥当性確認の中に検証行為が含まれるということを記載すべきではないか。
・ JEAG4609規格案P.10の参考図3の試験に対する妥当性確認が具体的にどのような行為なのか補足する必要があるのではないか。
・ JEAG4609規格案P.10参考図3で，「JEAG4101に基づく品質保証活動」に対する「JEAG4609に基づく品質保証活動」を明確にしているのであるから，JEAG4609における妥当性確認の実施内容がJEAG4101と同じであることを明確にする必要があると思う。
・ 検証，妥当性確認というのは行為を言葉で定義しているだけであって，例えば検証の目的は設計・製作作業の各段階の成果物が，直前の要求事項を満たしていることを確認する行為であって，その具体的な手法等については，規格の中に規定していない。パブコメにはその事実を回答しても良いのではないか。
・ 検証の対象に試験を含めないことは，本規程及び本指針がディジタル安全保護系に限定して適用されることを前提に内容を理解していれば，自ずと理解できると思う。
・ コメントの趣旨は，検証・妥当性確認の概要図には「試験」が存在するが，「検証」と「妥当性確認」の用語の定義には「試験」がないので追加すべきということではないか。したがって，試験は妥当性確認の対象であることを回答すればよいと思う。
・ No.1回答案の検証の対象に試験を追加すべきとのコメントに対しては，対象としないという回答でよいのではないか。
・ JEAG4609規格案の図1「検証・妥当性確認概要」の「検証」と「試験」は明確に分けた方が理解しやすいのではないか。
・ 用語の定義における「妥当性確認」では，試験プロセスを指していることが判らないので，それが判るように記載を追記した方がよい。
・ No.1回答案は，試験は検証の対象ではなく妥当性確認の対象である旨回答する。
・ No.7回答案では，自己診断機能が安全機能よりも優先されるものではないとの回答をしているが，パブコメは自己診断機能が安全機能を阻害するものではないという趣旨のものではないか。
・ 解説-11からは，自己診断機能が安全機能に悪影響を与えないことが読み取れるか。
・ 自己診断機能が安全機能を阻害してはいけないといった厳しい表現を入れてしまうと，本来はもっと自己診断機能に関して柔軟な設計が可能であるところに厳しい制限を強いることになるので，回答案のとおりシステムの信頼性を更に向上させる有効な一手段ということでよいと思う。
・ No.7回答案は，“自己診断機能が安全機能に悪影響を及ぼさないように設計することは重要なことと考えている。本規格では，ディジタル安全保護系に高い信頼性を要求しており，そのためシステムの更なる信頼性向上のための有効な一手段として自己診断機能を付加するとしており，これについては解説-11にも記載している”旨を回答する。

・ 解説-11文中の「報告する」を「告知する」に訂正する。
・ No.16回答案は，「ソフトウェアの信頼性」から「ソフトウェアの品質」へ変更するが，規格案全体について該当箇所が無いか確認する。
・ No.19回答案で，構成管理の監査あるいは審査をソフトウェア供給者に限定しているが問題ないか？
→ 変更前の「ベンダー」の表現を「供給者」に改めたものである。
・ ISO等の定義を引用しているのか？
→ ISO(JIS）の「供給者」の定義に基づいた記載としている。
・ ISOでいう監査は，商品の一部を請け負うベンダーに対する監査を指している。
・ 日本における監査の実態に合った記載とする必要がある。
・ 実態に即した記載なので，回答案のとおりとする。
・ No.14回答案について，JEAG4609の2.適用範囲には，安全保護系設備として機能を実現するソフトウェアの品質について第三者への立証性を確保する必要があると記載がある。上位規定であるJEAC4620の解説-3（ディジタル計算機の用語の定義）にも同様の記載があり，ここでは第三者への立証性について記載していないが何故か？
→ 上位規定であるJEAC4620は全般的な品質の確保ということで第三者への立証性については記載していないが，JEAG4609はそもそも本指針をV&V（検証及び妥当性確認）に特化して改定した背景に第三者への立証性の確保があったので敢えて記載している。
・ 今の記載では第三者への品質さえ確保すればよいと捉えられかねないので，品質を確保することと，第三者への立証性を確保することを併記してはどうか。
・ ディジタル安全保護系の導入に当たってNUPECが実証試験を行い，第三者への立証性の確保を目的としてV&V（検証及び妥当性確認）手法を確立した。そのような経緯からJEAG4609の目的に第三者への立証性の確保を掲げた。
・ 上位規定であるJEAC4620に要求事項を明確にする趣旨から，JEAC4620の解説-3（ディジタル計算機の用語の定義）に品質の確保と，第三者への立証性の確保を併記する。

（JEAG4609）
・ 検証及び妥当性確認の対象プロセスに変更を含めるかということについては，JEAC4620解説-14(2)（各プロセスで実施すべき品質管理項目）の変更プロセスの記載を削除し，同解説(1)（ライフサイクルプロセス）に，仕様変更等によるソフトウェアの変更要否を調査し変更が生じた場合は，設計・製作・試験に戻るプロセスとして定義する。また，JEAG4609では変更プロセスについて明確に定義していないが，JEAG4609は上流規定であるJEAC4620の要求事項に従うことから，JEAG4609においても検証及び妥当性確認の対象として変更プロセスを明記し，その定義はJEAC4620に従うものとする。
・ JEAC4620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）の変更プロセスを検証及び妥当性確認の対象として修正する（変更プロセスを点線で囲う）。

これに関する意見は以下のとおりであった。
・ 検証及び妥当性確認の対象に変更プロセスを含めることでよいのではないか。
・ 今回の修正案で検証及び妥当性確認の対象から変更プロセスを除くとしているが，JEAG4609規格案(P.5)の5.変更管理では，設計要求仕様及びソフトウェアの変更をする場合は，検証及び妥当性確認作業を再度実施するとあるので，対象とすべきではないか。
→ 今回の修正案で検証及び妥当性確認の対象から変更プロセスを除いたのは，変更は設計，製作，試験の各プロセスで発生するものであり独立に存在するものではなく，変更が発生した場合には，当該の各プロセスに戻って変更管理をするというのが趣旨である。
・ 解説-14(2)6)の「変更プロセス」の定義に，ソフトウェアに変更が生じる場合は，変更仕様を決定するとあるが，これに対する検証行為は発生しないのか？

→ ソフトウェアの仕様変更を行った場合は，検証及び妥当性確認（V&V）が必要となる。
・ ソフトウェアの仕様変更を行った場合は，検証及び妥当性確認（V&V）が必要と言いながら，変更プロセスが検証及び妥当性確認の対象に含まれるとの記載はどこにも無い。
・ 設計，製作，試験の各プロセスと変更プロセスの関係を図で表す場合は並列に記載することになるが，文章として記載する場合に変更プロセスが設計，製作，試験の各プロセスで生じることを表現してはどうか。例えば，“設計・製作・試験及びそれぞれの変更”といった記載にしてはどうか。
→ JEAC4620規格案の中では，設計・製作・試験の各プロセスで仕様変更が生じた場合について明記していないが，JEAG4609規格案 解説-4（変更作業）には，設計・製作・運転等のプロセスにおいて変更が生じた場合について記載している。
・ JEAC4620にある「変更プロセス」というのは，ソフトウェアの変更が生じた場合の影響度等を調査するところまでを言っていて，それ以降は設計・製作・試験の各プロセスに戻るというのが本来の趣旨だと思うが，今の記載では不十分ではないか。
・ 規格の中には「変更」の定義が無い。
・ JEAG4609の目的にはソフトウェアに関するプロセス全般を言う必要があるため「変更」の記載を残すが，それ以降の記載については変更が設計，製作，試験の各プロセスに含まれることから敢えて記載していないという理解であった。
・ JEAG4609の目的で検証及び妥当性確認の対象プロセスに「変更」を含めた場合，JEAG4609には5.変更管理しか規定されておらず，変更があった場合は設計，製作，試験の各プロセスに戻って検証及び妥当性確認を実施するとあるので，目的の“・・・検証及び妥当性確認に対する基本的事項を示した”の記載に対して違和感があるのではないか。
・ 実態としては変更プロセスを検証及び妥当性確認の対象とすることは問題ないと考えるが，「変更」には「変更作業」と「変更プロセス」があり，規格全般の「変更」の記載を「変更プロセス」としてしまうと，「変更」が「変更プロセス」と「変更作業」のどちらを指しているのか，混乱を招くのではないかとの懸念がある。
・ JEAG4609-1999改定検討の際に海外指針類との比較検討を行った結果，海外指針ではソフトウェアに変更が生じた場合もV&V（検証及び妥当性確認）の対象としていたことから，JEAG4609-1999についても変更に対して対応可能なように改定することとした。また，改定に当たっては変更を意識して，検証及び妥当性確認の範囲として，JEAC4620には変更プロセスを，JEAG4609には変更作業を明確にした。今回のパブコメは，JEAC4620には変更プロセスについて明確にしているが，JEAG4609には変更プロセスについて明確にしていないことへの指摘だと推測するので，JEAC4620とJEAG4609の主従関係からもJEAG4609に変更プロセスを明確にする必要があるため，検証及び妥当性確認の対象プロセスに変更を含めることが適切だと思う。
・ 設計，製作，試験（変更含む）としてはどうか。
・ JEAG4609では変更プロセスではなく変更管理を規定しているので，設計，製作，試験の各プロセス及び変更管理という記載にしてはどうか。
・ JEAG4609はJEAC4620の要求事項を受けた指針であるという位置付け（JEAG4609解説-1）から，JEAC4620で定義している「変更プロセス」をJEAG4609にも適用するという整理でよい。
・ そもそも「変更プロセス」は，ソフトウェアに変更が生じた場合に設計・製作・試験の各プロセスに従うとしているので，「変更プロセス」そのものには具体的な作業は定義していない。単純に検証及び妥当性確認の対象として全体を「変更プロセス」としてしまうと不整合が生じるかもしれない。
・ JEAC4620解説-14(1)変更プロセスの定義を，仕様変更等によるソフトウェアの変更要否を調査し変更が生じた場合は，設計・製作・試験に戻るプロセスといった記載にしてはどうか。

・ JEAC4620解説-14(2)（各プロセスで実施すべき品質管理項目）の変更プロセスの記載を削除し，同解説(1)（ライフサイクルプロセス）に，仕様変更等によるソフトウェアの変更要否を調査し変更が生じた場合は，設計・製作・試験に戻るプロセスとして定義する。また，JEAG4609では変更プロセスについて明確に定義していないが，JEAG4609は上流規定であるJEAC4620の要求事項に従うことから，JEAG4609においても検証及び妥当性確認の対象として変更プロセスを明確にし，その定義はJEAC4620に従うものとする。
・ JEAC4620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）の変更プロセスを検証及び妥当性の対象として修正する（変更プロセスを点線で囲う）。

(5) JEAG4611-1991「安全機能を有する計測制御装置の設計指針」改定案の検討について

小山委員より，資料No.15-4に基づき，前回検討会以降に集約したコメントに対する回答案及びJEAG4611改定案について説明があった。

これに関する意見は以下のとおりであった。

・ JEAG4611の3.3分類適用の原則において，計測制御装置の機能的隔離というのは当てはまるのか？

→ 重要度分類で下位クラスの機器が上位クラスの機器に影響を与えないとの趣旨で，計測制御装置においては機能的隔離及び物理的分離を適切に考慮しなければならないと記載している。

・ JEAG4611の3.3分類適用の原則(1)に二つ以上の安全機能を有する計測制御装置とあるが，何故二つ以上なのか，一つでも適用されるのではないか？

→ 一つの計測制御装置に設計上満たすべき要求事項が複数ある場合には，重要度分類の上位クラスの要求事項を満足すれば，安全機能が担保できるという趣旨である。

・ JEAG4611は分科会に上程可能なベースで仕上がっているが，今後更に編集上の修正を加え精度を高めていくこととする。

(6) 中央制御室誤操作防止に関する指針について

渡辺委員より，資料No.15-5-1，2に基づき，前回検討会以降に集約したコメントに対する回答案及び原子力発電所の中央制御室における誤操作防止に関する規程案について説明があった。

これに関する意見は以下のとおりであった。

・ 本規程の対象を中央監視操作盤（表盤）に限定する理由としては，重要度の観点からは，例えばサーベランス等で裏盤を使用するものは，裏盤の状態が表盤で監視可能なように工夫しコミュニケーションを図ることで整理できるが，緊急度あるいは使用頻度の観点で表盤に限定する理由はどのように整理されるのか。
・ 現場盤を対象としないということであれば，2.適用範囲（解説-1）の“通常運転時あるいは異常事故時に監視操作の対象とならない現場盤および中央制御室内裏側直立盤は本規程の対象外とする”と整合していないのではないか。

→ 中央制御室監視操作エリア及び中央監視操作盤に対象を限定した記載とする。

・ 4項以降の要求事項については，裏盤あるいは現場盤にも適用可能であるが，今回は中央制御室監視操作エリア及び中央監視操作盤に適用範囲を限定した。
・ JEAG4617「中央制御室の計算機化されたヒューマンマシンインタフェースの開発及び設計に関する指針」策定の際も，適用対象を表盤に限定するか否かについて議論があったと思う。
・ 技術基準省令62号別記-8を満たすのであれば表盤に限定しても良いが，民間指針としては過去の不具合事例を鑑みて裏盤及び現場盤まで対象を拡大しても良いのではないか。
・ 本規程の誤操作することなく適切に運転操作を行うという目的と対象設備がずれないように注意して規定することが重要である。

6．その他

次回検討会の開催については，別途調整することとした。

以　上