

ドラフト

「デジタル安全保護系に関する日本電気協会規格の技術評価に関する検討チーム会合  
における日本電気協会への説明依頼事項(その2)」に対する回答  
(JEAC4620-2020 及び JEAG4609-2020)

令和4年●月●日  
(一社)日本電気協会  
原子力規格委員会

標記につきましては、以下の通り回答いたします。

○説明依頼事項

1. 安全保護系へのデジタル計算機の適用に関する規程

○ 第1回会合資料1-2<sup>1</sup>に関する追加質問

(1) 5ページ(1)適用に当たっての条件の反映の回答No.6について、2008年版技術評価書には、「デジタル安全保護系のトリップ失敗確率及び誤トリップする頻度を評価し、従来型のものと比較して同等以下とすること。」としています。「動作に失敗する確率(アンアベイラビリティ)及び誤動作する頻度(誤動作率)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」を記載したとの説明でしたが、「同等以下」とはされていません。その理由を説明して下さい。

(2) 7ページ(2)において、IEEE規格、IEC規格から本規程に反映した事項について質問しました。IEEE603等では手動操作系も含め広く安全系のソフトウェアが対象となると理解しています。手動操作回路についてどのように対応したのかを説明して下さい。また、規格・ガイドが対象とする設備及び技術の範囲をIEEEの最新版と比較して示して下さい。

(3) 11ページ(3)において、規格本文において安全保護系の定義として検出器を含むとされているが、本規格のデジタル安全保護系の範囲は、検出器とみなす核計装や安全系の放射線モニタを含まない「原子炉停止系及び工学的安全施設作動系の演算・論理回路を有するデジタル計算機」のみを対象とした狭義の範囲を対象としているとの説明がありました。

① 16ページ(6)には「アンアベイラビリティや誤動作率の信頼性評価においては、システムを構成する各設備(ハードウェア構成要素)を適切

に考慮する必要があります。」とありました。今回検出器とみなすとされた核計装や放射線モニタのようにその内部処理として、燃料の許容限界を超えないようにするための安全に係る設定値に対する原子力特有のトリップ信号判定処理等にデジタル計算機が使われている場合、ハードウェア構成要素としてだけでなく、そのソフトウェア構成要素としてどのように考慮されるのか説明して下さい。

② 12 ページ (4) には、「PLD は安全保護系としての機能を実現するソフトウェアに係る部分には採用実績はないため」とあり、PLD は原子炉停止系及び工学的安全施設作動系の演算・論理回路には採用実績がないため、との説明がありました。他の質問回答において「安全保護系」及び「デジタル安全保護系」として「原子炉停止系及び工学的安全施設作動系の演算・論理回路」と限定して使用している部分を特定し、再度説明して下さい。

③ 安全系の核計装・放射線モニタは、米国の IEEE std 603 及び IEEE std 7-4.3.2 では適用範囲ですが、JEAC 4620 では適用範囲内ではありません。適用範囲の違いについて、表 (2) - 1 から 3 に倣って説明して下さい。

④ 第 1 回会合の説明において、JEAC 4620 は原子炉停止系及び工学的安全施設作動系の演算・論理回路に限定された規格ではあるものの、その他の設備に使用してはいけないというわけではないとの趣旨の説明がありました。規格として、その他の設備に使われることを想定して策定されているのか説明して下さい。

(4) 19 ページ (9) 環境条件について、想定される電源じょう乱、サージ電圧、電磁波等の外部からの外乱・ノイズへの対策を含む、環境条件に対する達成すべき水準を明確にしなければ、これらを考慮し、対策を取ることができません。2008 年版では、耐雷指針を引用していましたが、改訂により削除されています。「環境条件に対する達成すべき水準」を考慮した設計となっているかを、どのように判断するのか説明して下さい。

(5) IEC 規格について調査を行ったとの説明がありました。具体的にどの IEC 規格 (規格番号及び Edition 番号) について、どのような調査を行ったのかを説明して下さい。

(6) 17, 18 ページ (7) (8) 計測制御系との分離について、「解説-8 に示した例は、これらの例のいずれかを適用して、適切に設計することにより機能的分離を達成することが可能と考えます。」との回答ですが、これによ

ば、バッファメモリさえ用いれば他に制限はないとも読めますが、この場合、通信方向に関する制限はなくなり、非安全系との通信がある場合にそれからの影響を排除できなくなります。この課題に関して、国際的な動向としては、以下のように整理されていると理解しています。これらを反映しなかった理由があれば説明して下さい。

- 通信を行う場合の一般的な制限事項
- 通信の方向性に関する制限事項（例えば低位から高位への通信は安全を支援、又は強化する場合のみ許可）
- 非安全系からの信号により安全機能が損なわれないための考慮事項（優先度処理、及び共通原因故障としての考慮事項を含む）

(7) 21ページ(11) 動作及びバイパスの表示について、「表示する情報及びその表示方法等の詳細については、プラントごとの監視/操作設計の考え方に基づき決定されており」との説明がありました。「どのような情報（例えば第1原因）を「動作原因」とするのか」について実例での回答がありました。これを一般化し、以下の2つを満足することで要件を満たすと考えてよいですか。

- 安全保護系が1チャンネルでも動作すれば警報を発生し個々の動作状態を表示する
- 最初に発生したイベント及びその動作原因について表示する

(8) 23ページ(12) 遮断の定義について、「遮断に対する要求事項は、不正アクセス行為等により、デジタル計算機に対し影響を与えない状態を作ること」とし、定義ではなく実例を回答されています。「遮断」を満足する具体的な要件は、実例を一般化して以下と捉えてよいですか。

- 「外部ネットワークとの直接接続をしない。」は、物理的な接続を制限し最小限とすることをいう。
- 「外部ネットワークからの不正アクセスを物理的又は、機能的に遮断する防護装置」は、前項に係わらず外部との接続が必要な場合には物理的又は機能的に遮断できる防護装置を適用することをいう。
- 「信号を一方向（送信機能のみ）通信に制限」は、上記において可能な限り外側向けの通信を適用することをいう。

- (9) 24ページ(13)不正アクセス行為等の被害の防止について、「不正アクセス行為における対策の基本は、デジタル計算機そのものに対する防護手段であり、現地に限定しています。」との説明でした。フルライフサイクル管理の考え方を適用しない理由を説明して下さい。
- (10) 28ページ(15)V&Vについて、「JEAG4609 デジタル安全保護系の検証及び妥当性確認(V&V)に関する指針」によることと規定しなかった理由を説明して下さい。
- (11) 30ページ(17)多様性について、「多様性については留意事項としてデジタル安全保護系とは動作原理等が異なる追加の設備を設けることを推奨することにとどめております。」との説明でした。安全保護系内部の多様性については、規格の適用範囲内と思いますが、これについて規定していない理由を説明して下さい。

#### ○ その他の質問事項

- (12)「4. 5独立性」の「(解説-7)多重化されたチャンネル間の通信」には、独立性の要件として「(1)片方向通信」と「(2)バッファメモリ」の2項目が記載されています。これらは同時に適用するのか、それとも何れか一方でもよいのか、及びその理由を説明して下さい。
- (13)2008年版では(解説-16)において「新規設計や変更により検証及び妥当性確認が必要なプロセスとして、設計、製作、試験、変更を対象」としていましたが、2020年版では「(解説-21)V&V(手順)」において、V&Vとしての検証は設計プロセス及び製作プロセス、V&Vとしての妥当性確認は試験プロセスと、検証と妥当性確認が区別された形に改定されています。その改定理由について説明してください。また、「設計、製作、試験、変更」のうちの「変更」は2020年版で検証と妥当性確認のどちらに区分されるとしているのか説明して下さい。

#### 2. デジタル安全保護系の検証及び妥当性確認(V&V)に関する指針

- (1)「4. 1 V&Vの目的と概要」の(1)には、「V&Vは、JEAG4620等のデジタル安全保護系に対する要求事項が設計、製作、試験及び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。」と規

定しています。「JEAC4620 等」の「等」について、想定している規格を例示してください。

(2) 「4. 2 V&Vの実施」の「図1 V&V概要」には、検証（検証1～5）として各設計段階の文書を直接的なインプットとしてその間の整合を確認するように矢印が記載されていますが、妥当性確認については「試験」から直接矢印が1本だけ引かれており、妥当性確認の対象（例えば試験要領書/成績書等の文書か、試験行為自体か）が具体的に記載されていません。

- ① 妥当性確認の対象と実施内容を説明して下さい。
- ② 妥当性確認に関連して、「試験」が(注2)の破線内に記載されています。試験は、妥当性確認を実施する独立した体制で実施すると理解してよいですか。

○回答

1. 安全保護系へのデジタル計算機の適用に関する規程

○ 第1回会合資料1-2<sup>2</sup>に関する追加質問

(1) 5ページ(1)適用に当たっての条件の反映の回答No.6について、2008年版技術評価書には、「デジタル安全保護系のトリップ失敗確率及び誤トリップする頻度を評価し、従来型のものと比較して同等以下とすること。」としています。「動作に失敗する確率(アンアベイラビリティ)及び誤動作する頻度(誤動作率)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」を記載したとの説明でしたが、「同等以下」とはされていません。その理由を説明して下さい。

回答 1)

アンアベイラビリティ及び誤動作率の評価については、第1回公開会合資料1-2 P.13の(5)に記載させていただいた通り、ハードウェア構成要素ごとに分割した信頼性評価モデルを使用して信頼度を算出しております。信頼度の算出には構成要素のベイラビリティを使用しますが、その値は導入時期や構成要素の種類、基となるデータベースの構築方法等によって異なる部分があり、従来型とデジタル型を比較評価しても、同じ条件での評価にはなりません。また、従来型とデジタル型では構成要素の点以外にも、自己診断機能の有無、信号処理方法、回路構成、システム構成の相違等、機能面、構成面における相違があり、これらも同じ条件での評価を阻害する要因となる可能性があります。このため、従来型とデジタル型のアンアベイラビリティ及び誤動作率をその数値だけで単純に比較することは、技術的に妥当な評価とならない可能性があるものと考えます。

また、従来型の定義もアナログ型を示しているのか、現状のデジタル型を示しているのか明確になっておりません。

デジタル安全保護系の信頼性は、様々な要求事項を満足することで確保されるものです。アンアベイラビリティ及び誤動作率はその評価方法の1つであり、これだけを満足していれば信頼性を確保できるというものではありません。つまり、アンアベイラビリティ及び誤動作率の評価は、耐震性や耐環境性、品質保証、ソフトウェアの信頼性等を確保した上で、システムを構築し、そのシステムが非常時の動作やプラントの通常運転に大きな影響を与えない構成であることを確認することが主な目的であり、ある一定の数値を満足するから信頼性が十分であると判断できるものではないと考えております。

このような点から、設計を行う上で従来型と比較することは、一つの指標となりえますが、適用するシステムに合った信頼性を評価、確保することが重要と考えており、その数値自体が設計の要求事項になるものではないと考えております。このため、JEAC4620 では「アンアベイラビリティ及び誤動作率について、従来型と比較して同等以下であること」を要求事項としてはおりません。

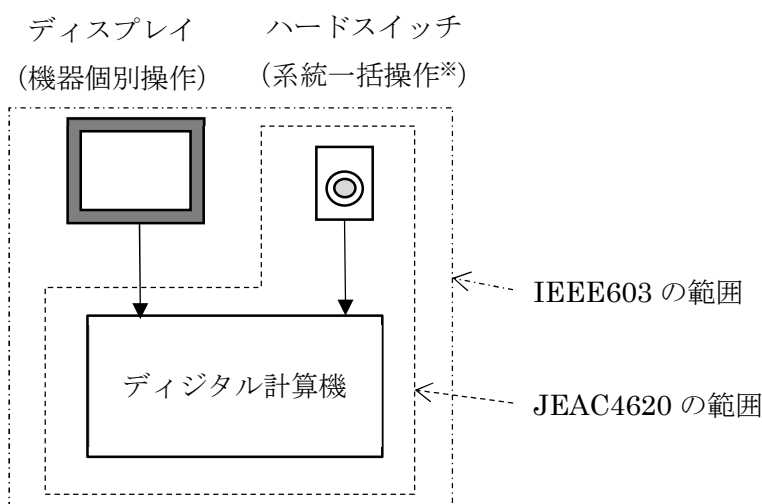
なお、海外の規格等でもこのような従来型と比較するような基準を適用しているケースは確認されておりません。

(2) 7 ページ (2) において、IEEE 規格、IEC 規格から本規程に反映した事項について質問しました。IEEE603 等では手動操作系も含め広く安全系のソフトウェアが対象となると理解しています。手動操作回路についてどのように対応したのかを説明して下さい。また、規格・ガイドが対象とする設備及び技術の範囲を IEEE の最新版と比較して示して下さい。

回答 2)

国内のデジタル安全保護系に関する手動操作としては、ディスプレイによる機器個別操作とハードスイッチによる系統一括操作に大別されます。工学的安全施設系を作動させる設備として系統一括操作のハードスイッチは安全保護系相当であり、JEAC4620 の対象としています。一方、機器の個別操作のためのディスプレイは、デジタル計算機による工学的安全施設作動系の演算・論理回路に含まれず、JEAC4620 の対象外としています。なお、IEEE603-2018 は“safety system”を対象としており、操作部はすべて含まれていると考えます。

JEAC4620 の「4.14 手動操作」については、2008 年制定当時の安全保護系の規格である JEAG4604-1993 の要件を参照しています。IEEE603 の手動制御の項の中でこれ以外の要件として、操作部の設置場所や操作回数などの最少化などがありますが、これらは制御室の設計や誤操作防止対策などによるものと考え、JEAC4620 に反映しておりません。



※：低圧注水系などを系統単位で起動できる操作



(3) 11 ページ (3) において、規格本文において安全保護系の定義として検出器を含むとされているが、本規格のデジタル安全保護系の範囲は、検出器とみなす核計装や安全系の放射線モニタを含まない「原子炉停止系及び工学的安全施設作動系の演算・論理回路を有するデジタル計算機」のみを対象とした狭義の範囲を対象としているとの説明がありました。

① 16 ページ (6) には「アンアベイラビリティや誤動作率の信頼性評価においては、システムを構成する各設備（ハードウェア構成要素）を適切に考慮する必要があります。」とありました。今回検出器とみなすとされた核計装や放射線モニタのようにその内部処理として、燃料の許容限界を超えないようにするための安全に係る設定値に対する原子力特有のトリップ信号判定処理等にデジタル計算機が使われている場合、ハードウェア構成要素としてだけでなく、そのソフトウェア構成要素としてどのように考慮されるのか説明して下さい。

### 回答 3 ①)

第一回会合の回答 5) と同様の回答となりますが、ソフトウェアに関しては、ハードウェアのように偶発的に故障が発生するものではなく、設計製作段階における人為的なミス起因とするものであるため、定量的に故障率を扱うことはできません。そのため、信頼性評価にはハードウェアの構成要素のみ考慮しております。

核計装や放射線計装は本規程の対象範囲外としておりますが、仮に、核計装や放射線計装を含めるとした場合であっても、信頼性評価においてソフトウェアは健全であることが前提条件となりますので、ソフトウェアの故障率を考慮しないという考え方は変わりません。

(3) ② 12 ページ (4) には、「PLD は安全保護系としての機能を実現するソフトウェアに係る部分には採用実績はないため」とあり、PLD は原子炉停止系及び工学的安全施設作動系の演算・論理回路には採用実績がないため、との説明がありました。他の質問回答において「安全保護系」及び「デジタル安全保護系」として「原子炉停止系及び工学的安全施設作動系の演算・論理回路」と限定して使用している部分を特定し、再度説明して下さい。

回答 3 ②)

前回回答における「安全保護系としての機能を実現するソフトウェアに係る部分」とは、アプリケーションのソフトウェアの事を指しており、「原子炉停止系及び工学的安全施設作動系の演算・論理回路をソフトウェアで実装している」ことを意味しています。

JEAC4620 のうち、アプリケーションのソフトウェアに特化した要件を記載しているのは以下の通りです。

節名称	ソフトウェアに特化した要件の記載箇所
1. 目的	(本規程の目的を記載)
2. 適用範囲	(デジタル安全保護系全体を適用範囲とする)
3. 用語の定義	(用語の定義を記載)
4. デジタル安全保護系に対する要求事項	(ソフトウェアを含むデジタル安全保護系全体への要件)
4.1 過渡時及び地震時の機能	(ソフトウェアを含むデジタル安全保護系全体への要件)
4.2 事故時の機能	(ソフトウェアを含むデジタル安全保護系全体への要件)
4.3 精度及び応答時間	(ソフトウェアを含むデジタル安全保護系全体への要件)
4.4 多重性	(ソフトウェアを含むデジタル安全保護系全体への要件)
4.5 独立性	(ソフトウェアを含むデジタル安全保護系全体への要件)
4.6 計測制御系との分離	(ソフトウェアを含むデジタル安全保護系全体への要件)
4.7 故障時の機能	(ソフトウェアを含むデジタル安全保護系全体への要件)
4.8 試験可能性	(ソフトウェアを含むデジタル安全保護系全体への要件)
4.9 外的要因(環境条件, 耐震性等)	(ソフトウェアを含むデジタル安全保護系全体への要件)
4.10 非常用電源の使用	(ソフトウェアを含むデジタル安全保護系全体への要件)
4.11 設定値の変更	(ソフトウェアを含むデジタル安全保護系全体への要件)
4.12 入力変数の選定	(ソフトウェアを含むデジタル安全保護系全体への要件)
4.13 保護動作の完全性	(ソフトウェアを含むデジタル安全保護系全体への要件)
4.14 手動操作	(ソフトウェアを含むデジタル安全保護系全体への要件)
4.15 動作及びバイパスの表示	(ソフトウェアを含むデジタル安全保護系全体への要件)
4.16 自己診断機能	(ソフトウェアを含むデジタル安全保護系全体への要件)
4.17 ソフトウェアの管理外の変更の防止	ソフトウェアの変更管理を要求
4.18 不正アクセス行為等の被害の防止	(ソフトウェアを含むデジタル安全保護系全体への要件)
4.19 品質保証	ソフトウェアの品質確保を要求
4.19.1 ソフトウェアライフサイクル	
4.19.2 ソフトウェア構成管理	
4.19.3 V&V	

(3) ③ 安全系の核計装・放射線モニタは、米国の IEEE std 603 及び IEEE std 7-4.3.2 では適用範囲ですが、JEAC 4620 では適用範囲内ではありません。適用範囲の違いについて、表(2) - 1 から 3 に倣って説明して下さい。

回答 3 ③)

JEAC4620 と IEEE7-4.3.2 対象とする範囲の比較を以下に示します。

	JEAC4620	IEEE 7-4.3.2
対象システム	安全保護系	安全系(safety system) <sup>※</sup>
デジタルデバイス	デジタル計算機(CPU ベース)	プログラマブル・デジタル・デバイス (PLD や FPGA を含む)
ソフトウェアに対する要件の範囲	原子炉停止系及び工学的安全施設作動系の演算・論理回路 (核計装・放射線モニタは検出器とみなし対象範囲外)	検出器から駆動装置入口まで、及びそれらの電源のうち、デジタル化された設備

※: safety system については、IEEE 603 で対象範囲が定義されている

(3) ④ 第1回会合の説明において、JEAC 4620 は原子炉停止系及び工学的安全施設作動系の演算・論理回路に限定された規格ではあるものの、その他の設備に使用してはいけないというわけではないとの趣旨の説明がありました。規格として、その他の設備に使われることを想定して策定されているのか説明して下さい。

回答 3 ④)

JEAC4620 の適用範囲は、デジタル安全保護系（安全保護系のうち、原子炉停止系及び工学的安全施設作動系の演算・論理回路を有するデジタル計算機）を対象としており、その他の設備に使われることを想定して策定してはおりません。

一方で、その他の設備を設計する際に、その設備に対する要求事項を踏まえた上で、JEAC4620 の一部又は全部を適用することで信頼性の高い設備を構築することは問題ないものと考えております。

(4) 19ページ(9)環境条件について、想定される電源じょう乱、サージ電圧、電磁波等の外部からの外乱・ノイズへの対策を含む、環境条件に対する達成すべき水準を明確にしなければ、これらを考慮し、対策を取ることができません。2008年版では、耐雷指針を引用していましたが、改訂により削除されています。「環境条件に対する達成すべき水準」を考慮した設計となっているかを、どのように判断するのか説明して下さい。

回答 4)

電磁的な外乱・ノイズ等に対して計測制御装置に施す設計上の考慮事項は、フィルタや接地など、原子力発電所の設備に限らず、一般産業の設備と共通的なものです。そのため、デジタル安全保護系の設計に際しても、設置条件等を踏まえつつ、一般的な規格、基準を適宜活用することで十分に対応できると認識しています。よって本規程においては、これらの外乱・ノイズに対して原子力固有の考慮事項を記載する必要はないと考え、具体的な規格・基準を指定しないこととし、耐雷指針の引用も取りやめた次第です。

(5) IEC 規格について調査を行ったとの説明がありました。具体的にどの IEC 規格 (規格番号及び Edition 番号) について、どのような調査を行ったのかを説明して下さい。

回答 5)

JEAC4620 の 2008 年版制定及び 2020 年版改定のそれぞれの検討時において、以下の IEC 規格調査しています。これらは大枠では IEEE 7-4.3.2 に含まれているものと判断いたしました。また、従来より国内の原子力発電所の計装制御に関する規制、規格の多くは米国の規制、規格を参考にしている経緯もあり、最終的には IEEE7-4.3.2 をベースに検討することとしました。

- |                  |  |
|------------------|--|
| IEC 880-1986     | Software for computers in the safety systems of nuclear power stations   |
| IEC 60880-2-2000 | Software for computers important to safety for nuclear power plants<br>Part2: Software aspects of defence common cause failures, use of software tools and of pre-developed software |
| IEC 60880-2006   | Nuclear power plants<br>- Instrumentation and control systems important to safety<br>- Software aspects for computer-based systems performing category A functions                   |

(6) 17, 18 ページ (7) (8) 計測制御系との分離について、「解説-8 に示した例は、これらの例のいずれかを適用して、適切に設計することにより機能的分離を達成することが可能と考えます。」との回答ですが、これによれば、バッファメモリさえ用いれば他に制限はないとも読めますが、この場合、通信方向に関する制限はなくなり、非安全系との通信がある場合にそれからの影響を排除できなくなります。この課題に関して、国際的な動向としては、以下のように整理されていると理解しています。これらを反映しなかった理由があれば説明して下さい。

- 通信を行う場合の一般的な制限事項
- 通信の方向性に関する制限事項（例えば低位から高位への通信は安全を支援、又は強化する場合のみ許可）
- 非安全系からの信号により安全機能が損なわれないうための考慮事項（優先度処理、及び共通原因故障としての考慮事項を含む）

#### 回答 6)

解説-8 に記載している具体例は、本文要求事項を満足するために採用する設計方針の例であり、このいずれかを必ず適用しなければならないというものではありません。また、逆に例に記載された一文が設計のすべてを説明しているものでもなく、例に記載された設計方針を採用した場合でも、本文要求事項を満足するように詳細な設計検討が行われます。

計測制御系全般に言えることではありますが、特にこのような通信機能については、これを実現する接続構成・回路構成・適用素子・適用ソフトウェアなどはきわめて多種多様であり、特定の設計仕様を前提とした詳細設計例を要件として記載することは、かえって設計の柔軟性を損なったり、新たな技術の導入の障害になってしまう可能性があります。したがって、本文においては、最終的に満たすべき要求のみを記載し、個々の設計の選択枝については解説に例を載せることとしています。

記載されている例は、当時の省令 62 号・別記7に示された「具体的仕様の例」を参考に、実際に適用する可能性のあるものを記載するとともに、IEEE 7-4.3.2 などでも検討されていたバッファメモリの利用についても記載しました。なお、省令 62 号の別記7に記載された「具体的仕様の例」については、これらを必ず適用するという性格のものではありませんでしたが、設計に際して有用な事例であると考え、JEAC4620 に反映しました。なお、その後の技術評価や技術基準規則の解釈では、この「具体的仕様の例」で示されていた内容の一部が、例であるか否かを明示されない形で記載されておりますが、技術基準規則本文で要求される事項の

本質は特段変化していないと認識していることから、本規程では「具体的仕様の例」として扱っています。

ご参考ですが、特定の設計を前提として仕様を制限するような要件の記載方法については、米国でも解消する方向で検討が進んでおり、現行の IEEE 7-4.3.2 に記載されている仕様を限定する要求の多くは、次回改定時に本文から削除する方向で検討が進んでいます。この中には安全上の利点を条件とする要求も含まれています。



(7) 21ページ(11)動作及びバイパスの表示について、「表示する情報及びその表示方法等の詳細については、プラントごとの監視/操作設計の考え方にに基づき決定されており」との説明がありました。「どのような情報(例えば第1原因)を「動作原因」とするのか」について実例での回答がありましたが、これを一般化し、以下の2つを満足することで要件を満たすと考えてよいですか。

- 安全保護系が1チャンネルでも動作すれば警報を発生し個々の動作状態を表示する
- 最初に発生したイベント及びその動作原因について表示する

回答 7)

4.15 項の要求事項はデジタル安全保護系の動作原因が中央制御室に表示されることであり、このうち安全保護系に対する設計要件としては、動作原因を中央制御室で表示できるように、警報装置等のヒューマンマシンインターフェイスに情報を提供する(信号を出力する)ことまでと考えております。表示する情報や表示の具体的な実現手段については、プラントごとの監視/操作設計で考慮すべき事項であり、安全保護系に対する要求として規定するものではないと考えております。

なお、安全保護系の動作・状態を表示する実例については前回会合で回答した通りです。また、ファーストヒット/ファーストアウトに関しては、安全保護系以外の要素(タービントリップや発電機トリップの動作原因)も含んでいることを補足しておきます。

(8) 23 ページ (12) 遮断の定義について、「遮断に対する要求事項は、不正アクセス行為等により、デジタル計算機に対し影響を与えない状態を作ること」とし、定義ではなく実例を回答されています。「遮断」を満足する具体的な要件は、実例を一般化して以下と捉えてよいですか。

- 「外部ネットワークとの直接接続をしない。」は、物理的な接続を制限し最小限とすることをいう。
- 「外部ネットワークからの不正アクセスを物理的又は、機能的に遮断する防護装置」は、前項に係わらず外部との接続が必要な場合には物理的又は機能的に遮断できる防護装置を適用することをいう。
- 「信号を一方向（送信機能のみ）通信に制限」は、上記において可能な限り外側向けの通信を適用することをいう。

回答 8)

遮断に対しては定義を規定するものではなく、デジタル計算機に対し影響を与えない状態を作るための手段となります。

これは遮断を実現するための方法(制御方式、通信方式、回路構成など)は多種多様であることや、セキュリティ関連規格の今後の動向とともに技術革新による設備への導入に際し障害になってしまう可能性があることから、解説-17 では不正アクセス行為等の被害の防止に必要な措置の例として挙げ、手段としての記載としています。

(9) 24ページ(13)不正アクセス行為等の被害の防止について、「不正アクセス行為における対策の基本は、デジタル計算機そのものに対する防護手段であり、現地に限定しています。」との説明でした。フルライフサイクル管理の考え方を適用しない理由を説明して下さい。

回答 9)

規格化にあたっては、技術基準規則の解釈(第三十五条)より引用しているため現地に限定していますが、フルライフサイクル管理の必要性は認識しており、設計段階においてメーカー工場での入域管理やセキュリティ教育により管理しています。

規格への反映については今後のセキュリティ関連規格の動向とともに必要に応じ検討の上、反映可否を含め適切に対応したいと考えます。

(10) 28ページ(15) V&Vについて、「JEAG4609 デジタル安全保護系の検証及び妥当性確認 (V&V) に関する指針」によることと規定しなかった理由を説明して下さい。

回答 10)

JEAC4620 では、基本的な品質保証活動に加えて V&V 活動を実施することを要求しています。この V&V の実施方法は、ガイドラインである JEAG4609 の趣旨に沿った形で、また、実際の V&V 対象の仕様等を踏まえて個別に具体化することを想定しています。

実際に、V&V の対象となる設備の種類や設計・制作にあたる組織の構成などによって設計の手順や関連する図書の構成などが異なってくることから、JEAG4609 では典型的な設計のステップを例示して V&V の内容を解説しています。

したがって、V&V の実施にあたっては、JEAG4609 を参照しながら具体的な V&V 計画を適切に立案し実行することになります。

(11) 30ページ(17) 多様性について、「多様性については留意事項としてデジタル安全保護系とは動作原理等が異なる追加の設備を設けることを推奨することにとどめております。」との説明でした。安全保護系内部の多様性については、規格の適用範囲内と思いますが、これについて規定していない理由を説明して下さい。

回答 11)

JEAC4620 は耐震性, 耐環境性, ソフトウェアの信頼性等の要求事項を満足すると共に必要な多重性を確保することで高い信頼性を有するデジタル安全保護系を構築し, 運用することを目的としたものです。

共通要因故障を防止する手段として, 多様性を持たせることが効果的であることは認識しており, 異なる設計のハードウェアを組み合わせるシステムを構築する等, 内部の多様性を持たせることで共通要因故障を低減できる可能性があります。一方で, 内部で多様性を持たせるということは, その多様な装置間の伝送等, 新たな技術を必要とします。全く異なる設計の装置を組み合わせるシステムを構築するには, 新たに詳細な設計調整を必要とし, 場合によっては, この部分の設計ミスが信頼性低下の要因となる可能性があります。このため, 内部の多様性を持たせるには十分な設計検討, 場合によっては技術開発が必要となります。

JEAC4620 は海外規格を踏まえつつも, 現状の国内のデジタル安全保護系設計を考慮して設定したものです。このため, 現在又は近い将来に国内で導入されるデジタル安全保護系の設計を考慮した際に, その採用が技術的に現実的でないものについては記載しておりません(但し, 採用を否定するものではありません)。異なる設計のハードウェアを組み合わせるシステムを構築する等, 内部の多様性については, 前記のような点も踏まえて, その採用がまだ技術的に現実的でないものと考えております。デジタル安全保護系の設計については, 現状の JEAC4620 における要求事項を満足することで十分に高い信頼性を確保できると考えており, 内部の多様性については, 海外動向, 技術動向等を考慮しながら, 今後, 必要性も含めて検討していく部分と考えております。

なお, デジタル安全保護系に限定したものではありませんが, 安全保護系としてはシステムの多様性(高圧注水系, 低圧注水系等), 検出方法の多様性(原子炉水位, 格納容器内圧力等)等も考慮されております。

○ その他の質問事項

(12)「4. 5 独立性」の「(解説-7) 多重化されたチャンネル間の通信」には、独立性の要件として「(1) 片方向通信」と「(2) バッファメモリ」の2項目が記載されています。これらは同時に適用するのか、それとも何れか一方でもよいのか、及びその理由を説明して下さい。

回答 12)

解説-7 で示した適用の例は、同時に適用することを要求するものではありません。  
ご質問(6)への弊回答をご参照いただきたいですが、本解説についても、省令 62 号・別記7の「具体的仕様の例」を参考に例を選定しており、これにバッファメモリの適用を加えています。

(13) 2008年版では(解説-16)において「新規設計や変更により検証及び妥当性確認が必要なプロセスとして、設計、製作、試験、変更を対象」としていましたが、2020年版では「(解説-21) V&V (手順)」において、V&Vとしての検証は設計プロセス及び製作プロセス、V&Vとしての妥当性確認は試験プロセスと、検証と妥当性確認が区別された形に改定されています。その改定理由について説明してください。また、「設計、製作、試験、変更」のうちの「変更」は2020年版で検証と妥当性確認のどちらに区分されるとしているのか説明して下さい。

回答 13)

2008年版の記載では、すべてのプロセスにおいて、「検証」と「妥当性確認」の両方の実施が必要であるように解釈されかねないと考え、2020年版ではそれぞれをどのプロセスで実施すべきかを明記しました。

また、変更プロセスについては、(解説-19)に示すように変更の可否を調査する段階であり、実際の変更内容は設計、製作及び試験におけるそれぞれのプロセスに従うため、V&Vとしては変更プロセスそのものは対象から外しています。変更の決定を受けて実施する設計、製作及び試験はV&Vの対象となります。

## 2. デジタル安全保護系の検証及び妥当性確認 (V&V) に関する指針

(1) 「4. 1 V&Vの目的と概要」の(1)には、「V&Vは、JEAC4620等のデジタル安全保護系に対する要求事項が設計、製作、試験及び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。」と規定しています。「JEAC4620等」の「等」について、想定している規格を例示してください。

### 回答 1)

デジタル安全保護系は、原子炉施設の異常状態を検知し必要な場合に各信号回路を直接動作させる設備であり、その要求事項は JEAC4620 以外に「発電用軽水型原子炉施設に関する安全設計指針」や「実用発電用原子炉及びその付属施設の技術基準に関する規則」を代表とする、プラント安全設計に必要な要求事項を含む規制又は規格を想定しています。



(2)「4. 2 V&Vの実施」の「図1V&V概要」には、検証(検証1～5)として各設計段階の文書を直接的なインプットとしてその間の整合を確認するように矢印が記載されていますが、妥当性確認については「試験」から直接矢印が1本だけ引かれており、妥当性確認の対象(例えば試験要領書/成績書等の文書か、試験行為自体か)が具体的に記載されていません。

- ① 妥当性確認の対象と実施内容を説明して下さい。
- ② 妥当性確認に関連して、「試験」が(注2)の破線内に記載されています。試験は、妥当性確認を実施する独立した体制で実施すると理解してよいですか。

回答 2)

① 妥当性確認の対象は、試験要領書/成績書などの文書であり、試験行為自体はV&Vの対象とは考えておりません。妥当性確認では、最終製品がデジタル安全保護系に対する要求事項を満たしていることを、実施された試験結果を確認することで確認します。

② 4.2(2)で記載している通り、V&V作業は、設計、製作及び試験に携わった組織から独立した体制で行うこととしておりますが、試験行為自体はV&Vの対象ではありませんので「独立した体制」では実施しません。

なお、妥当性確認においては、デジタル安全保護系に対する要求事項を満たしていることを確認する観点から、通常の製品試験以外のV&V特有の試験(例えば、添十解析の模擬など)を実施した結果を確認する場合があります。このような場合、試験計画の立案及び結果の確認をV&Vを実施する者が行うこととなります。つまり、試験行為自体はV&Vの対象とはしないものの、試験プロセス自体がV&V活動の一部とみなすことができるため、(注2)の破線内に記載しております。

## 安全保護系へのデジタル計算機の適用に関する規程/指針

JEAC4620/JEAG4609

## 本文及び解説記載事項について

## 1. 日本電気協会規格における本文及び解説の記載事項

日本電気協会規格において、本文及び解説に何を記載するかについては、日本電気協会の「規格作成手引き」のP. 1の「3. 規格作成における要求事項」として、以下の通り、規定されております。以下、当該部抜粋を示します。

## 3. 規格作成における要求事項等

## 3.1 要求事項と推奨事項

- (1) 必ず実施しなければならない事項（要求事項）及び代替案がある事項（推奨事項）は規格本文のみで網羅される記載とする。また、規格本文中の要求事項及び推奨事項は参考や解説がなくても理解、履行できる様な記載とする。
- (2) 要求事項と推奨事項については、利用者に誤解を生じさせないように、明確に分けて表現しなければならない。（詳細は、附属書添付1「文章・用語等の書き表し方」7. 参照）

[例]

- ・要求事項：「～しなければならない。」「～とする。」等
- ・推奨事項：「～することが望ましい。」「～するのがよい。」等

## 2. JEAC4620 における本文及び解説の記載事項

JEAC4620 はデジタル安全保護系に対し、その機能と設計に関する要求事項及びそのソフトウェアに対する品質上の要求事項を規定したものです。本文は、計測制御装置という設備の特性上、主に機能的な要求事項を規定しており、解説は本文の要求事項に対して具体的な事例を踏まえた設計の考え方、又は設計を進める上で補足した方がよい事項等を示しております。この解説は国内で既に導入実績があるデジタル安全保護系の設計や、最近のデジタル制御技術を基に、今後、デジタル安全保護系を設計する際に参考とすべき事項をまとめたものです。解説に記載した設計例を単独又は組み合わせて適用することで、本文の要求事項を満足することができますが、その設計手法を解説に記載した内容に限定するものではありません。これは、デジタル制御技術の特性上、本文の要求事項を満足する方法に様々な方法があること及び次々と新しい方法が開発されてくることから、これを限定することは必ずしもデジタル安全保護系の信頼性向上につながらないと考えられるためです。このため、JEAC4620 は現状のように本文には「要求事項又は推奨事項」として、機能的な内容を記載し、解説にそれを実現するための設計例等の参考事項を記載しております。