資料３－２

変更点を赤字で記載

「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（修正版）

（JEAC4620-2020 及び JEAG4609-2020）

令和４年３月７日
※令和４年４月26日修正
（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．安全保護系へのディジタル計算機の適用に関する規程

○　第１回会合資料１－２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№.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、本規格のディ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ィジタル計算機」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ィ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はなく、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「ディジタル安全保護系」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，ディ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，ディ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 ディ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ィ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．ディ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 等のディ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

１．安全保護系へのディジタル計算機の適用に関する規程

○　第１回会合資料１－２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№.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 の回答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ア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，従来型とディ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，従来型とディ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，従来型とディ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，現状のディジタル型を示しているのか明確になっておりません。

ディ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一つであり，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。

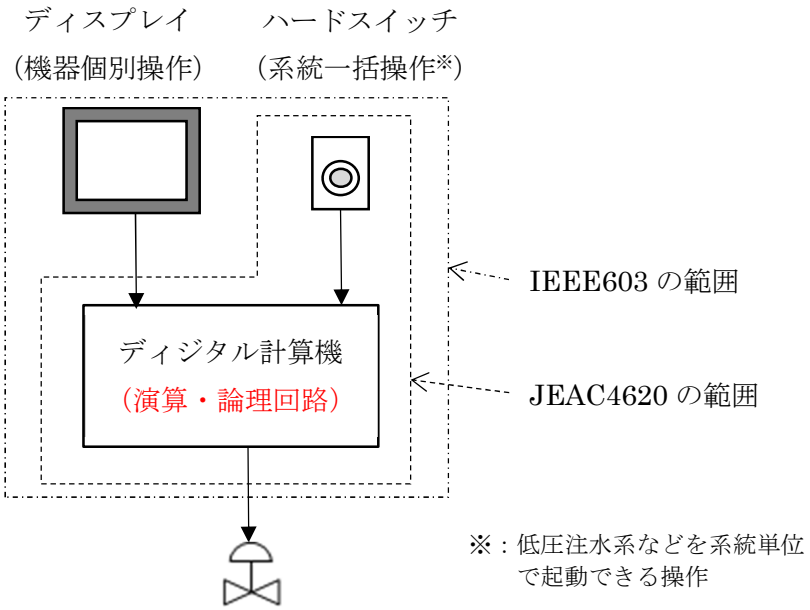
回答 2）

国内のディ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（ポンプの起動／停止，弁の開／閉 等）とハードスイッチによる系統一括操作（原子炉停止，ECCS作動 等）に大別されます。原子炉停止系及び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。系統一括操作のハードスイッチの信号はディジタル計算機に入力され，ディジタル計算機内の演算・論理回路を経て弁やポンプなどの起動信号として出力されます。

一方，機器の個別操作のためのディスプレイは，ディ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。機器の個別操作のための操作信号や，安全保護系のブロックやリセットの操作信号は安全保護系を直接作動させるための操作信号ではありませんが，ディジタル計算機に入力され，原子炉停止系および工学的安全施設作動系の演算・論理回路において安全保護系が適切に作動できるようロジックが構成されています。

なお，IEEE603-2018 は“safety system”を対象としており，機器個別操作もは全て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。


ディスプレイ
（機器個別操作）
ハードスイッチ
（系統一括操作※）
IEEE603 の範囲
ディジタル計算機
（演算・論理回路）
JEAC4620 の範囲
※：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、本規格のディ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ィジタル計算機」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ィ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はなく、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）

個別回答に先立ち，本規程における”ディジタル安全保護系”及び“安全保護系としての機能を実現するソフトウェア”の意味を改めてご説明します。

○ディジタル安全保護系とは

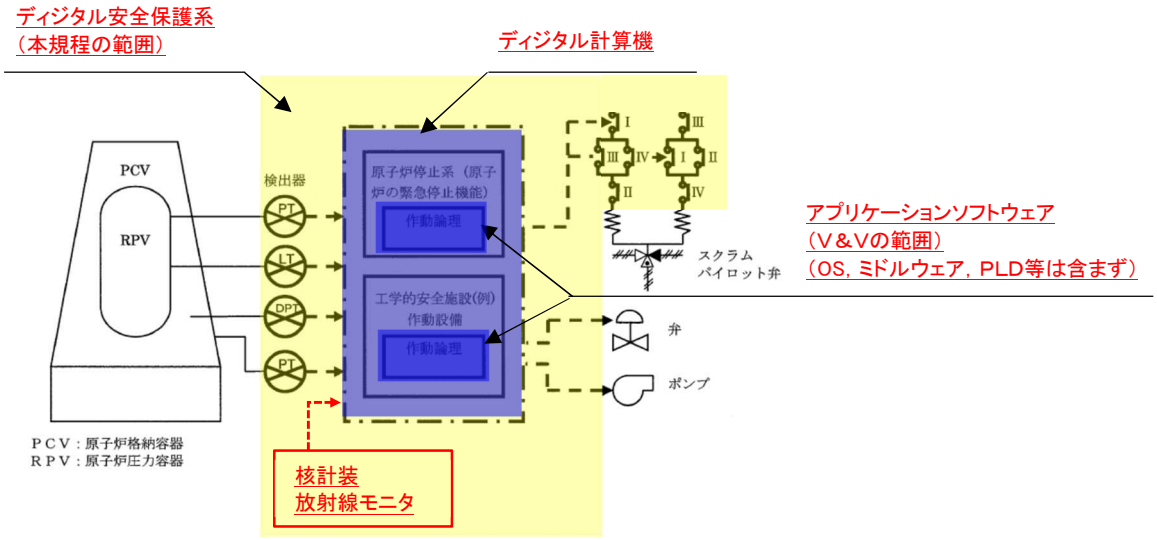
安全保護系の機能を，~~中でも，特に高い信頼性が求められる「原子炉停止系及び工学的安全施設作動系の演算・論理回路」（下図の青色ハッチング）を~~ディジタル計算機のアプリケーションのソフトウェアで~~実装~~実現している場合，その検出器から動作装置入力端子までを含めて「ディジタル安全保護系」（下図の黄色ハッチング）としています。~~を指します~~。

○「ディジタル計算機」とは

本規程におけるディジタル計算機とは，安全保護系としての機能を実現するソフトウェアが実装されたディジタル計算機（下図の青色ハッチング）を指しています。

○「安全保護系としての機能を実現するソフトウェア」とは

「原子炉停止系及び工学的安全施設作動系の演算・論理回路を実装したアプリケーションのソフトウェア」を指します。よって，本規程におけるソフトウェアへの要件は，それらの演算・論理回路を実装するソフトウェアに対して適用することを意図しています。



回答 ３ ①）

第１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を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。この考え方は，内部処理の内容によらず，同様となります。

一方で，ソフトウェアに関しては，品質保証活動の中で信頼性を担保しております。ここで，本規定の適用範囲については回答３）で記載の通り，核計装や放射線モニタを検出器として取り扱っており，本規程におけるディジタル計算機としての要求~~適用~~範囲外としておりますので，核計装や放射線モニタにソフトウェアが適用される場合，そのソフトウェアに関してはJEAC4111/JEAG4121 で規定されている原子力の通常の品質保証活動の中で信頼性を担保することとなります。一方で，回答３）で記載した「原子炉停止系及び工学的安全施設作動系の演算・論理回路を実装するソフトウェア」に対しては，原子力の通常の品質保証活動に加えて，本規定で V&V の実施を要求しております。

（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「ディジタル安全保護系」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ことを指しており，「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，安全保護系としての機能を実現する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		関連する解説	安全保護系としての機能を実現するｿﾌﾄｳｪｱへの要件
1.	目的	1 目的**【次頁参照】**	（本規程の目的を記載）
2.	適用範囲	2 適用範囲(概念図)	（適用範囲はﾃﾞｨｼﾞﾀﾙ安全保護系）
3.	用語の定義	3 機能を実現する S/W	（用語の定義を記載）
4.	ﾃﾞｨｼﾞﾀﾙ安全保護系に対する要求事項	4 ｱﾝｱﾍﾞｲﾗﾋﾞﾘﾃｨ及び誤動作率の評価	（ｿﾌﾄｳｪｱを含むﾃﾞｨｼﾞ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	5 過渡時及び地震時の機能	
4.2	事故時の機能	—	
4.3	精度及び応答時間	6 ﾘｱﾙﾀｲﾑ性能	
4.4	多重性	—	
4.5	独立性	7 多重化されたﾁｬﾝﾈﾙ間の通信	
4.6	計測制御系との分離	8 計測制御系との分離	
4.7	故障時の機能	—	
4.8	試験可能性	9 S/W の試験	
4.9	外的要因(環境条件,耐震性等)	10 外的要因(関連規格･指針), 11 外的要因(設計の確証)	
4.10	非常用電源の使用	—	
4.11	設定値の変更	12 適切な設計変更	
4.12	入力変数の選定	13 直接検出できない変数の例	
4.13	保護動作の完全性	—	
4.14	手動操作	14 手動操作の機能	
4.15	動作及びﾊﾞｲﾊﾟｽの表示	—	
4.16	自己診断機能	15 自己診断機能	
4.17	ｿﾌﾄｳｪｱの管理外の変更の防止	16 S/W の管理外の変更防止	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	17 不正ｱｸｾｽ行為等の被害の防止	（ｿﾌﾄｳｪｱを含むﾃﾞｨｼﾞﾀﾙ安全保護系全体への要件）
4.19	品質保証	18 品質保証活動	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	19 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	20 ｿﾌﾄｳｪｱの構成管理	
4.19.3	V&V	21 V&V(手順), 22 V&V(独立性), 23 V&V(文書化)	

＜解説-1 目的についての補足＞

本解説のなお書き※にある“一部にディジタル計算機を適用する場合”とは，上記の演算・論理回路の一部をディジタル計算機のソフトウェアで実装する場合を意図しています。

※：該当部分を以下に抜粋：

“なお，ディジタル計算機を適用していない従来型の安全保護系に対しては，「原子力発電所安全保護系の設計規程：JEAC4604-2009」に従うものとする。また，一部にディジタル計算機を適用する場合には，ディジタル計算機がシステムに影響を及ぼす範囲において，本規程に従うものとする。”

（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）

JEAG4620 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）※
ディジタルデバイス	ディジタル計算機（CPU ベース）	プログラマブル・ディジタル・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，ディ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，ディジタル計算機に「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」を実装したディジタル安全保護系（検出器～動作装置入力端子まで）~~（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ィジタル計算機）~~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，ディ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，2020 年版では耐雷指針の引用もしておりません。

なお IEEE323 では，耐環境試験の条件を定める際に考慮する「通常時及び異常時の運転条件の一例」として電磁的な影響や電力サージも含まれていますが，同規格では，通常時や事故時の環境が厳しくない設置環境にある設備への耐環境試験を要求していないことから，上記の対応と整合するものと考えております。

（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 規格を調査しています。これらは大枠では IEEE 7-4.3.2 に包含さ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。そのため以下 IEC 規格についてはそれぞれに記載されている要件については確認しましたが，JEAC4620 との項目対比は実施していません。

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 Part2: Software aspects of defence common cause failures, use of software tools and of pre-developed software
IEC 60880-2006	Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category A functions

なお，上記の IEC 60880 等の他に，原子力発電所の重要な計測制御全般に対する規格である IEC 61513，分離指針を示している IEC 60709 等については，ディジタル安全保護系への要件を直接的に記載しているものではないため，参考として調査しています。

（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 項の要求事項はディ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致します。

（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，ディ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」については，定義を規定するのではなく，ディ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して記載しております。

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）は多種多様であると共に，セキュリティ関連の技術革新に伴って新技術が導入されていくことが考えられ，具体的な要件を設定して限定することは，設計の柔軟性を損なったり，新たな技術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，ディ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）

今回の改定に際して，当該の記載については技術基準規則の解釈（第三十五条）より引用したため，現地に限定した記載となっていますが，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。

設計段階における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，反映要否を含め適切に対応~~反映する方向で検討したいと考えます。

（１０）２８ページ（１５）V&V について、「JEAG4609 ディ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ィ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ィ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て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て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，現状の国内のディ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ィ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て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。ディ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，ディ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系統の多様性（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要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，~~変更内容は設計・製作の図書に反映され，基本的な原子力品質保証活動に基づき，設計チームにて設計検証，妥当性確認が実施されます。さらに変更内容が反映された設計・製作の図書に対して V&V を行います。例えば変更箇所が上位図書の要件から相違がないことの検証等を含めて V&V として確認しています。また，V&V によって変更内容が上位図書の要件に不適切であることが分かった場合などには設計・製作者に対して是正を求めるような活動を実施しています。

２．ディ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 等のディ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）

ディ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「発電用軽水型原子炉施設に関する安全設計指針」及び「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事項並びに各プラント固有の設計要求である設置許可申請書を想定していることから，「JEAC4620 等」の記載としています。

（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，最終製品がディ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，実施する試験内容・判断基準，及び，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。試験を実施する行為自体は，V&V 作業ではありませんので「独立した体制」では実施しません。

V&V 作業を含む品質保証活動の全体概要については，（解説-1）の参考図 1 で示しております。ここで，基本的な原子力品質保証活動の中での妥当性確認は，JEAC4111/JEAG4121 で記載されている通り“試験”自体を指しており，設計チームが最終的な製品に対して要求事項を満たしていることを確認しております。一方で，V&V 作業では，設計，製作及び試験に携わった組織から独立した体制が，実施する試験内容・判断基準，及び，実施された試験結果を設計チームのそれとは別に妥当性確認を行うことで，独立性を確保しております。

また一方で，図 1 は V&V 作業の概要を説明するための図であり，（注 1）の一点鎖線で（解説-6）で説明している設計・製作作業の範囲を，（注 2）の破線で V&V の範囲を示しております。いずれも現状の記載に誤りはございませんが，試験行為も含めた形で V&V 作業と見えてしまう点など，本文の記載表現に関しては今回ご質問頂いた内容を踏まえ次回改定時に見直しを検討したいと考えます。

別紙

安全保護系へのディ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，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
>
> **3. 6各構成要素の記載事項**
>
> （８）本文等
>
> ｄ．解説に要求事項の必要性，背景，言葉の解釈などを記載できる。

2. JEAC4620 における本文及び解説の記載事項

JEAC4620 はディ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を満足するために採用する設計方針の例，その設計の考え方，又は設計を進める上で補足した方が良い事項等を示しております。ここで，解説に示した設計方針の例は必ず適用しなくてはならないというものではありません。また，この設計方針の例を適用すれば，必ず本文の要求事項を満足できるというものでもなく，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必要となります。

この解説は国内で既に導入実績があるディジタル安全保護系の設計や，最近のディジタル制御技術を基に，今後，ディ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し，その詳細な設計検討を

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，ディ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は多種多様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，特定の設計仕様を前提とした詳細設計例を要件として限定することは，設計の柔軟性を損なう，又は新たな技術の導入の障害になる等の可能性があり，必ずしもディ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，最終的に満たすべき要求のみを記載し，解説にそれを満足するための設計例等の参考事項を記載しております。JEAC4620 におけるこの考え方は基本的に今後も変わらないものと考えております。