参考資料●－●

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）（案）

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[1]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、

1

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。