別紙

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（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

（１） 2008 年版の技術評価において、適用に当たっての条件としたもののうち、2020 年に反映しなかった内容について、その理由を説明して下さい。

（２） IEEE 規格、IEC 規格から本規程に反映した事項を説明して下さい。また、反映しなかった部分があれば、その内容と理由を説明してください[1]。

（３） 2020 年版において、「安全保護系」の用語の定義に、検出器が含まれることが明記されました。核計装や放射線計装などのデジタル化された装置に関する必要な要件は、本規程に含まれるのか説明してください。

（４） 「1.目的」には、「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」を対象とすると記載されています。「3.1 ディジタル計算機」には PLD[2]が適用される場合を含むのか説明してください（核計装や放射線計装のデジタル化では PLD（FPGA[3]等）が適用される場合があると理解しています。）。含む場合、PLD は「内蔵されたプログラム」又は「デジタルデータの算術演算や論理演算等の計算を行う装置」のいずれに該当するか、説明してください。

（５） 「4. ディジタル安全保護系に対する要求事項」には、「ディジタル安全保護系は、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、」とありますが、どのように考慮するのか例を示して説明してください。また、アンアベイラビリティや誤動作率の評価には、ソフトウェアも必要になりますが、記載していない理由を説明ください。

（６） 「解説-4 アンアベイラビリティ及び誤動作率の評価」には、アンアベイラビリティや誤動作率の評価において考慮するハードウエア構成要素として、異常の検出等デジタル安全保護系の機能が挙げられています。アンアベイラビリティや誤動作率の評価において必要となるものは、設備とその故障モードですが、機能を挙げている理由を説明してください。

（７） 「4.6 計測制御系との分離」には、「通信を共用する場合には機能的にも分離する設計とすること。」と規定され、「解説-8 計測制御系との分離」に

---

[1] 例えば、以下の内容は、規格に反映されていない。
○ 手動操作回路（4.14 に機能の記載有り）をデジタル化する場合の要件
○ デジタル技術として PLD（FPGA 等）を適用する場合の要件
○ デジタル技術として組込デバイス（EDD）を適用する場合の要件

[2] Programmable Logic Device

[3] Field Programmable Gate Array

は、ディジタル安全保護系と計測制御系との通信の機能的分離の措置の例として４例が記載されています。これらをどのように適用すれば（単独で、あるいは組み合わせて）規程の要求を満足できるのか説明してください。

（８） 「4.6 計測制御系との分離」に関連して、米国では通信の独立性に関して具体的な要件が定められていますが（例えば、DI&C-ISG-04[4]に記載の項目）、これに対応する要件のうち、規定していないものについてその理由を説明してください。

（９） 「4.9 外的要因」の「4.9.1 環境条件」には、「ディジタル安全保護系は，次の環境条件を考慮した設計とすること」の具体的な事項として、「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」があげられていますが、解説-10 には達成すべき水準が具体的な規格基準等により示されていません[5]。達成すべき水準（具体的な規格基準等）を説明してください。

（１０） 「4.9.4 設計の確証」には、「4.9.1 及び 4.9.2 で要求された設計」によりそれぞれの外的要因に対して機能維持できることを確証するとありますが、「4.9.3 その他の外的要因」に規定された火災防護上及び溢水防護上の措置を考慮した設計の確証が要求されていません。その理由として、解説-11 には、「ディジタル計算機の耐力を要求しているものではないため」とありますが、設計の確証が「機能維持」の確証ではなく、「耐力」の確証としている理由を説明してください。

（１１） 「4.15 動作及びバイパスの表示」には、「ディジタル安全保護系が動作した場合は，その動作原因が中央制御室に表示される設計とする」と規定されていますが、どのような情報（例えば第１原因）を「動作原因」とするのか説明してください。

（１２） 「解説-17 不正アクセス行為等の被害の防止」の(1)には、「外部ネットワークと遮断」とありますが、ここでいう「遮断」の定義を説明してください。

（１３） 「解説-17 不正アクセス行為等の被害の防止」の(2)には、「物理的及び電気的アクセスの制限を設けることにより、システムの据付け、更新、試験、保守等で、承認されていない者の操作、ウイルス進入等を防止する。」とありますが、管理の対象を設計開発段階からではなく、据付け以降に限定している理由を説明してください。

---

[4] Revision 1, Interim Staff Guidance on Highly-Integrated Control Rooms – Communications Issues (HICRc), March 2009

[5] 2008 年版解説-8 において「耐サージ性：「原子力発電所の耐雷指針：JEAG 4608-2007」」が記載されていたが、2020 年版解説-10「外的要因（関連規格・指針）」においては削除された。

（１４）「4.19 品質保証」には、「ソフトウェアの健全性を確保すること。」とあり、「ソフトウェアライフサイクル及び構成管理手法を定めた，品質保証活動」及び「V&V 活動」の手法で確保すると規定しています。ソフトウェアライフサイクル、構成管理手法及び V&V 活動に関する規格としては、「JIS X 0160:2021 ソフトウェアライフサイクルプロセス」があげられます。同規格の規定との違いを説明してください。

（１５）「4.19.3 V&V」には、V&V に関する要件として(1)～(3)として、実施体制の独立性、文書化、再利用が規定されています。何を実施すれば V&V として十分とみなせるかに関する基本的な事項が規程として記載されていない理由を説明してください。

（１６）「5.留意事項」には、「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が推奨される」とありますが、「推奨される」の意味を説明して下さい。

（１７）「5.　留意事項」には、「4.ディジタル安全保護系に対する要求事項」を遵守することにより、共通原因故障が発生する可能性は十分低いものとなっている」とあります。共通原因故障の可能性を大きく低減させるものとして、多様性があげられますが、その要求が規定されていません。「共通原因故障が発生する可能性は十分低い」とした理由を説明してください。

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）　「3.2 安全保護系」には、設備の範囲として検出器から動作装置入力端子までとされています。デジタル計算機のソフトウェアで処理する手前に、PLD 等を使用した論理回路が構築されている可能性があります。そのような場合、PLD 等の論理回路は V&V の対象となるのか説明してください。