資料４－１

「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）」に対する回答

令和4年8月25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。

〇説明依頼事項

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 2020 年版の適用範囲に関するもの

（１）「4. ディジタル安全保護系に対する要求事項」の規定毎の適用範囲を説明して下さい。

（２）ソフトウェア管理に関連する「4.17　ソフトウェアの管理外の変更の防止」、「4.18 不正アクセス行為等の被害の防止」、「4.19 品質保証」については、適用範囲の詳細を説明してください。

２．核計装・放射線計装に関するもの

（１）核計装・放射線計装の演算・論理回路を「ディジタル計算機」の対象としていない理由を説明してください。

（２）「4.18 不正アクセス行為等の被害の防止」は、核計装・放射線計装は適用範囲外とのことですが、技術基準規則では、核計装・放射線計装にも適用される要求事項です。同規程では適用対象外とした理由を説明してください。

（３）「4.16 自己診断機能」、「4.17 ソフトウェアの管理外の変更」、「4.18 不正アクセス行為等の被害の防止」及び「4.19 品質保証」については、核計装・放射線計装は適用範囲外とのことですが、これらの規定を核計装・放射線計装に用いることができるかについて説明してください。

３．その他

（１）「4.6 計測制御系との分離」における「通信」の定義と，機能的分離が適用される範囲について示してください。

（２）機能的分離には，安全系と非安全系信号の優先処理部(回路)が含まれるのか否か示してください。また，この処理がFPGA等のソフトウェアが介在する処理回路で実装される場合に，適用範囲となるか否かを示してください。

○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 2020 年版の適用範囲に関するもの

（１）「4. ディジタル安全保護系に対する要求事項」の規定毎の適用範囲を説明して下さい。

回答（1）

別添資料「JEAC4620 が「ディジタル安全保護系」,「ディジタル計算機」,「ソフトウェア」に要求している事項の整理」を参照ください。

（２） ソフトウェア管理に関連する「4.17　ソフトウェアの管理外の変更の防止」、「4.18 不正アクセス行為等の被害の防止」、「4.19 品質保証」については、適用範囲の詳細を説明してください。

回答（2）

○「4.17 ソフトウェアの管理外の変更の防止」:

原子炉停止系および工学的安全施設作動設備の作動論理に用いられる「ディジタル計算機」の「安全保護系としての機能を実現するソフトウェア」（以下，アプリケーションソフト）を対象としています。

○「4.18 不正アクセス行為等の被害の防止」:

原子炉停止系および工学的安全施設作動設備の作動論理に用いられる「ディジタル計算機」を対象としています。

○「4.19 品質保証」:

アプリケーションソフトを対象としています。この理由は，アプリケーションソフトは，設備ごとプラントごとに固有の設計として確実に作りこむ必要があるため，その設計を他の安全保護系設計よりも更にきめ細かく管理することが，ディジタル安全保護系の安全性及び信頼性確保の観点から重要であると考えているためです。（JEAG4609 の「2.適用範囲」参照）

この適用範囲の考え方は，2008 年版から特に変更はなく，一般の原子力品質保証を前提として更に JEAC4620 の要求事項を適用しています。

なお，ディジタル計算機に用いるハードウェアや，計算機の基本動作を制御するソフトウェア（以下，基本ソフト）については，その開発段階においては一般の原子力品質保証を適用した開発・設計プロセス，設計検証・妥当性確認などが実施されます。

これらのハードウェアや基本ソフトを組み合わせて，具体的に原子炉停止系および工学的安全施設作動設備の作動論理を実現するディジタル計算機を設計・製作する際には，アプリケーションソフトの品質保証を確実に実施するためにも，これらハードウェアや基本ソフトを組み合わせたディジタル計算機の仕様を正しく設定し，これを製作し，アプリケーションソフトを実装する必要があります。このため，アプリケーションソフトの品質保証としてのライフサイクルの考慮や構成管理・Ｖ＆Ｖの実施などにおいては，アプリケーションソフトに合わせてハードウェアや基本ソフトが適切に組み合わされることも確認しています。（JEAG4609 の図1参照）

また，核計装や放射線モニタ，あるいは温度計装などの安全保護系でディジタル技術を適用している装置は，基本的に一般の原子力品質保証に基づいて設計・製作を行っていますし，設計・保守用のソフトウェアツールは，一般の原子力品質保証の基で作業環境やツールとして管理されています。

なお，JEAC4620 では原子炉停止系および工学的安全施設作動設備の作動論理へのディジタル計算機の適用を念頭に要求事項を整備してきていますが，安全保護系におけるその他のディジタル装置の適用についての要求事項が不要であると判断しているものではありません。安全保護系全体におけるディジタル装置の適用への要求事項については再整理が必要と考えており，今後検討すべき課題と考えております。

２．核計装・放射線計装に関するもの

（１）核計装・放射線計装の演算・論理回路を「ディジタル計算機」の対象としていない理由を説明してください。

回答（1）

ディジタル安全保護系に関する規格は，安全保護系へのディジタル計算機適用にあたり，ソフトウェアの品質確保を目的に，V&V（検証及び妥当性確認）を中心とした手順をガイドラインとして，JEAG4609-1989「安全保護系へのディジタル計算機の適用に関する指針」を制定したところからはじまります。

この際，「安全保護系へのディジタル計算機適用」については，安全保護系として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を対象としており，つまり，「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」をアプリケーションソフトウェアとして実装したディジタル計算機を対象としています。このため，V&V の対象範囲も「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ソフトウェアとしています。

これは，それまでのリレー回路を中心としたハードウェアで構成された「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」をソフトウェアで実現するにあたり，その品質確保を最も重要視し，そこに焦点を絞って検討したことが理由です。

これには，「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」は，多重化された装置の論理演算結果（2/4 論理等）を出力し，原子炉停止系及び工学的安全施設作動系の動作に直結する回路であり，安全保護系全体の中でも最も重要な部分であるという点も関係しています。

また，1989 年当時，BWR プラントの核計装については既にディジタル制御技術を適用した装置が開発，導入されていましたが，ソフトウェアも含めて，十分な検証を実施した上で導入されており，問題なく稼働していたため，前記の対象には含めておりませんでした。逆に，核計装での経験も踏まえて，ディジタル安全保護系の対応方法を検討したという形です。

核計装，放射線モニタでは設定値比較機能等をディジタル制御回路で実現しておりますが，判定結果は「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」へ接点入力しております。このような判定結果を接点入力する構成は，設定値比較機能等をアナログ回路で構成しているという違いはありますが，CV 急閉の圧力スイッチ等他にも使用しており，検出器として扱っている部分になります。このような点も踏まえて，核計装・放射線モニタも検出器として扱っております。

上記のような点から，JEAC4620 では 2008 年の制定時から核計装，放射線モニタを「ディジタル計算機」の対象とはしておらず， 2020 年の改定においてもその考え方は変更しておりません。

現状の考え方は上記の通りですが，BWR プラントでは複数のプラントで核計装，放射線モ

ニタにディジタル制御技術を適用しており，その扱いについては今後検討すべき課題と考えております。

（２）「4.18 不正アクセス行為等の被害の防止」は、核計装・放射線計装は適用範囲外とのことですが、技術基準規則では、核計装・放射線計装にも適用される要求事項です。同規程では適用対象外とした理由を説明してください。

回答（2）

JEAC4620 では原子炉停止系および工学的安全施設作動設備の作動論理へのディジタル計算機の適用を念頭に要求事項を整備してきております（回答２（１）参照）。このため，JEAC4620としては，「原子炉停止系および工学的安全施設作動設備の作動論理」として扱っていない核計装・放射線計装については，「ディジタル計算機」への適用事項である「4.18 不正アクセス行為等の被害の防止」の適用対象としておりません。

但し，これは核計装・放射線モニタについて，技術基準規則 35 条で要求されている事項を満足しなくて良いという意味ではありません。

核計装・放射線計装に限らず，安全保護系全体におけるディジタル装置を適用（原子炉停止系及び工学的安全施設作動設備の作動論理以外への適用）する場合の要求事項については，「4.18 不正アクセス行為等の被害の防止」に限らず再整理が必要と考えており，今後検討すべき課題と考えております。

（３）「4.16 自己診断機能」、「4.17 ソフトウェアの管理外の変更」、「4.18 不正アクセス行為等の被害の防止」及び「4.19 品質保証」については、核計装・放射線計装は適用範囲外とのことですが、これらの規定を核計装・放射線計装に用いることができるかについて説明してください。

回答（３）

ディジタル安全保護系については，「原子力安全のためのマネジメントシステム規程：JEAC4111-2013」及び「原子力安全のためのマネジメントシステム規程（JEAC4111-2013）の適用指針：JEAG4121-2015[2018 年追補版]の「品質マネジメントシステムに関する標準品質保証仕様書」に基づいた品質保証活動が実施されます。これは，核計装，放射線モニタについても同様です。

一方で，「安全保護系としての機能を実現するソフトウェア」（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）については，上記の基本的な原子力品質保証活動を前提にして，特にきめの細かい管理を行い，かつその品質について第三者への立証性を確保することを目的として，V&V を実施することとしています。

ディジタル装置を適用した核計装，放射線モニタのソフトウェアは，「安全保護系としての機能を実現するソフトウェア」（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）ではないため，V&V の対象範囲とはしておりませんが，上記の基本的な原子力品質保証活動を前提にして，V&V を実施することで，より信頼性の高いソフトウェアとすることができます。このため，核計装，放射線モニタに「4.19.3 V&V」を適用することは問題ないものと考えております。「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」，「4.17 ソフトウェアの管理外の変更」についても同様です。

また，JEAC4620 ではディジタル装置を適用した核計装，放射線モニタをディジタル計算機（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）ではなく，検出器として扱っており，「4.16 自己診断機能」，「4.18 不正アクセス行為等の被害の防止」の適用対象としておりませんが，前記と同様に，より信頼性の高い設備を構築するために，核計装，放射線モニタにこれらの要求事項を適用することは問題ないものと考えております。

３．その他

（１）「4.6 計測制御系との分離」における「通信」の定義と，機能的分離が適用される範囲について示してください。

回答（1）

「通信」とは，複数の情報を伝送する手段を指しており，一般的に言えばネットワーク伝送やデータリンクなどに該当します。

機能的に分離することは，JEAC4604 にも示すように，ハードワイヤード回路を含むすべての安全保護系に適用されます。JEAC4620 の 4.5 項，4.6 項においても，機能的に分離する手段として電気的分離，物理的分離を要求しています。これらはチャンネル間や計測制御系との間で分離すべき機能が異なる装置で構成されている場合には，装置間で電気的分離，物理的分離を行うことが影響波及を防止するために必要であることを示しています。その上で，複数の情報を伝送する手段である「通信」については，特に注意すべき事項として異区分や計測制御系からの悪影響を防止するために「機能的分離」を要求するとともに，解説にその手段を例示しています。（JEAC4620-2020 においては「機能的分離」という表現は「通信」に対して用いています。）

（２）機能的分離には，安全系と非安全系信号の優先処理部(回路)が含まれるのか否か示してください。また，この処理が FPGA 等のソフトウェアが介在する処理回路で実装される場合に，適用範囲となるか否かを示してください。

回答(2)

ディジタル安全保護系にて優先処理部(回路)を使用する場合には，ソフトウェアで実現する場合もハードウェアで実現する場合も，安全保護系の一部に位置づけられ，JEAC4620 の適用範囲になります。

機能的分離としては，安全保護系の動作が優先する他，最終的に安全機能を阻害しないことを考慮することとなります。

なお，優先処理部(回路)に FPGA のようなプログラマブルなハードウェア素子を適用した場合には，ハードウェアの開発・設計として原子力品質保証活動の中で設計検証などの適切な対応を取ることとしており，「安全保護系としての機能を実現するソフトウェア」としては扱っていません。

また，原子炉停止系及び工学的安全施設作動系の演算・論理回路の安全保護系としての機能を実現するソフトウェアに相当する機能に FPGA を適用した場合，その品質向上のために JEAC4620 の「ディジタル計算機」への要求を準用することが考えられますが，現行の JEAC4620 では，このように FPGA を適用した原子炉停止系及び工学的安全施設作動系の演算・論理回路をディジタル計算機の適用範囲として考慮していない(想定していない)ため，その扱いについては今後の検討課題と考えております。

別添

JEAC4620が「ディジタル安全保護系」,「ディジタル計算機」,「ソフトウェア」に要求している事項の整理

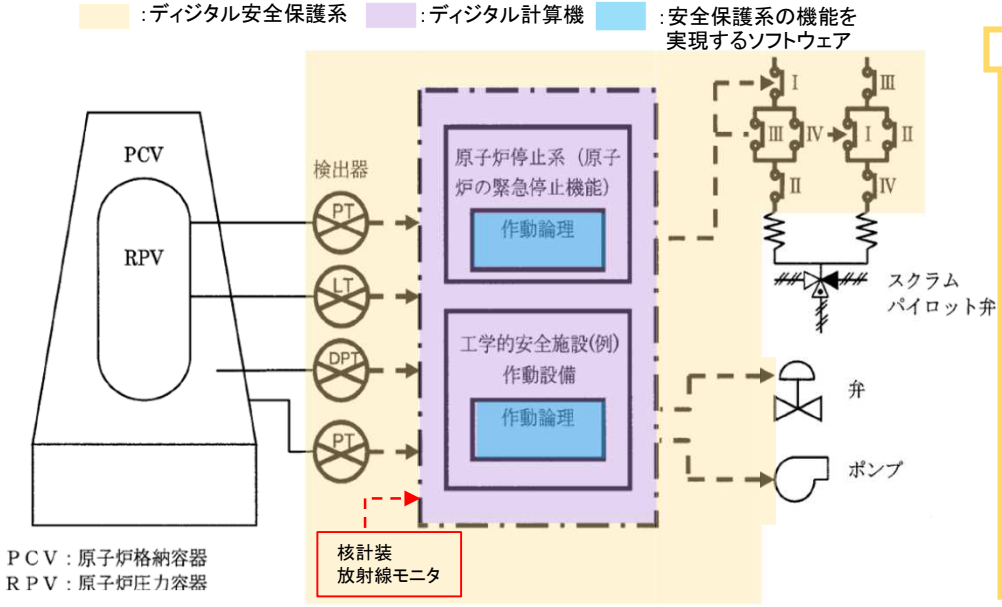
▼各用語の意味

○ディジタル安全保護系（下図の黄色ハッチング）
　安全保護系の機能を，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」としています。

○「ディジタル計算機」（下図の紫色ハッチング）
　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」（下図の青色ハッチング）
　「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。

▼各用語の示す範囲



▼JEAC4620-2020 4章における各要求事項との関係

ディジタル安全保護系全般への要求

- 4.1 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
- 4.4 多重性
- 4.5 独立性
- 4.6 計測制御系との分離
- 4.7 故障時の機能
- 4.8 試験可能性
- 4.9 外的要因（環境条件,耐震性等）
- 4.10 非常用電源の使用
- 4.11 設定値の変更
- 4.12 入力変数の選定
- 4.13 保護動作の完全性
- 4.14 手動操作
- 4.15 動作及びﾊﾞｲﾊﾟｽの表示

ディジタル計算機への要求

- 4.16 自己診断機能
- 4.18 不正ｱｸｾｽ行為等の被害の防止

ソフトウェアへの要求

- 4.17 ｿﾌﾄｳｪｱの管理外の変更の防止
- 4.19 品質保証
  - 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

▼一部ディジタルの場合，アナログの場合との比較

JEAC4620での要求事項	（上記論理・演算回路が全てソフトの）ディジタル安全保護系	一部ディジタルの安全保護系	アナログ安全保護系
ディジタル安全保護系全般への要求	対象となる	上記演算・論理回路をソフトウェアで実装した安全保護機能の，検出器から動作装置入力端子までのみ対象となる	対象外
ディジタル計算機への要求	上記演算・論理回路をソフトウェアで実装したディジタル計算機のみ，対象となる	上記演算・論理回路をソフトウェアで実装した部分のディジタル計算機のみ，対象となる	
ソフトウェアへの要求	上記演算・論理回路を実装したソフトウェアのみ，対象となる	上記演算・論理回路を実装したソフトウェアのみ，対象となる	