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3)(案)」
に対する回答

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．安全保護系へのディジタル計算機の適用に関する規程
（１）機能的分離（「4.6 計測制御系との分離」）について質問します。
①通信
「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。
（質問の趣旨）
○技術基準規則第３５条第６号では「計測制御系の一部を安全保護装置と共用する場合」に機能的分離を求めている一方，同規程では通信が係わる部分に限定的に機能的分離の要件が適用されるようにも読めます。「4.5 独立性」ではチャンネル間に「通信を用いる場合」，「4.6 計測制御系との分離」では計測制御系と「通信を共用する場合」とされていることから，機能的分離の適用範囲を確認するものです。
（補足）
○技術基準規則第３５条では一般的な要求事項が記載されている一方，その解釈として規程を引用した場合に適用範囲が一部に限定されてしまうことを懸念しての確認です。「通信」の用語がネットワークを用いた多重伝送を意味するのか，それとも広義の「信号インタフェース」を意味するのか等により適用範囲が異なってくると考えられます。

②優先回路
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等のソフトウエ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。
（補足）

〇例えばソフトウエア共通原因故障対策の自動作動信号，手動操作信号等（非安全系の信号）が，個別のハードウエア信号として安全保護系へ入力される場合に，これらの信号と安全保護系内で生成される信号，あるいは安全保護系に入力される他の安全系/非安全系の手動操作信号との優先度制御に，機能的分離の要求が果たされるのか確認するための質問です。（これに該当する非安全系からの信号が無い場合は，その旨回答頂いてかまいません。）

（２）品質保証（「4.19 品質保証」），及びセキュリティ要件（「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」）に関する要件の適用範囲を示してください。

（質問の趣旨）

〇ライフサイクル管理，及び構成管理は，本来的には相互に関連のあるハードウエア及びソフトウエアの全ての構成要素を対象とすべきとの観点から，現状の規程がそれをどの程度カバーしているか，またそれが妥当な考え方に基づくものかを確認するものです。

（補足）

〇規程の解説３では，規程におけるソフトウエアを「安全保護系としての機能を実現するソフトウエア」としていますが，現行の技術基準規則解釈ではこれに対応する「規程 2008 年版の解説３」は引用しておらず，規程の対象範囲と規則解釈の対象範囲は必ずしも一致しないとも考えられます（つまり，規則解釈では適用範囲に制限を設けていないことから，規則第 35 条本文の対象範囲である安全保護装置全体とも解釈されうる）。こうした背景も踏まえ，規程 2020 年版における対象範囲及びその考え方について確認するものです。

〇基本ソフトウエアのうち OS は，本体部分と個々のアプリケーションに依存して設定されるデータの部分に分類できる場合があると考えますが（例えば，前者は ROM として H/W と一体的に実装される部分，後者はデータとしてダウンロードされる部分など），ライフサイクル管理，構成管理，V&V の対象となるのはどの範囲か示してください。

〇規程の解説３ではデジタル計算機のソフトウエアについて分類を記載していますが，解説-2 の参考図１，２に示すデジタル計算機以外の部分に，組込デジタルデバイス(組込ソフトウエア含む)がある場合に，どのように扱われるか示してください。規程 4.19.1～ 4.19.3 は何れも「デジタル安全保護系のソフトウエア」と記載されているため，解説３における「特にことわりの無い場合」は適用されず，デジタル安全保護系全体を対象とし

ているように解釈される可能性があると考えられます。

〇上記を総合して，ソフトウエアに関連する規程の各々の適用範囲について分かり易く示してください。回答方法は問いませんが，例えば以下のような表にまとめることが考えられます。(回答が不明のものは空欄)

(補足)

〇④組込回路が FPGA による場合であって，その品質保証が V&V による場合(S/W と見なす場合)と，フルカバーの試験による場合（H/W と見なす場合）に分かれる場合は，各々の場合について示してください。

〇デジタル化された核・放射線計装については，これまでの回答では④S/W に該当すると考えられますが，この理解が正しいか確認の上で，4.17～4.19 の適用範囲を示してください。

〇デジタル化された温度計装については，デジタル化範囲の機能・実装方法等に基づいて②④の何れが適用範囲となるのか，あるいは範囲外かを示してください。また国際的に V&V によらず定性評価を適用可能となる部分(検出器等)か否かについて示してください。

〇回答

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

（１）機能的分離（「4.6 計測制御系との分離」）について質問します。

①通信

「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。

（質問の趣旨）

〇技術基準規則第３５条第６号では「計測制御系の一部を安全保護装置と共用する場合」に機能的分離を求めている一方，同規程では通信が係わる部分に限定的に機能的分離の要件が適用されるようにも読めます。「4.5 独立性」ではチャンネル間に「通信を用いる場合」，「4.6 計測制御系との分離」では計測制御系と「通信を共用する場合」とされていることから，機能的分離の適用範囲を確認するものです。

（補足）

〇技術基準規則第３５条では一般的な要求事項が記載されている一方，その解釈として規程を引用した場合に適用範囲が一部に限定されてしまうことを懸念しての確認です。「通信」の用語がネットワークを用いた多重伝送を意味するのか，それとも広義の「信号インタフェース」を意味するのか等により適用範囲が異なってくると考えられます。

回答(1)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。

機能的分離は，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，機能的分離を達成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。その上で，さらにディジタル特有の「通信」に対して特に注意すべき事項として記載しています。

安全保護系全体に機能的分離を要求することがわかるよう，表現の見直しを次回 JEAC4620 改定時に考慮したいと考えます。

②優先回路

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 等のソフトウエ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。

（補足）

〇例えばソフトウエア共通原因故障対策の自動作動信号，手動操作信号等（非安全系の信号）が，個別のハードウエア信号として安全保護系へ入力される場合に，これらの信号と安全保護系内で生成される信号，あるいは安全保護系に入力される他の安全系/非安全系の手動操作信号との優先度制御に，機能的分離の要求が果たされるのか確認するための質問です。(これに該当する非安全系からの信号が無い場合は，その旨回答頂いてかまいません。)

回答(1)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 の適用範囲ではなく，詳細は今後の改定で検討してゆきます。

（２）品質保証（「4.19 品質保証」），及びセキュリティ要件（「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」）に関する要件の適用範囲を示してください。

（質問の趣旨）

〇ライフサイクル管理，及び構成管理は，本来的には相互に関連のあるハードウエア及びソフトウエアの全ての構成要素を対象とすべきとの観点から，現状の規程がそれをどの程度カバーしているか，またそれが妥当な考え方に基づくものかを確認するものです。

（補足）

〇規程の解説３では，規程におけるソフトウエアを「安全保護系としての機能を実現するソフトウエア」としていますが，現行の技術基準規則解釈ではこれに対応する「規程 2008 年版の解説３」は引用しておらず，規程の対象範囲と規則解釈の対象範囲は必ずしも一致しないとも考えられます（つまり，規則解釈では適用範囲に制限を設けていないことから，規則第 35 条本文の対象範囲である安全保護装置全体とも解釈されうる）。こうした背景も踏まえ，規程 2020 年版における対象範囲及びその考え方について確認するものです。

〇基本ソフトウエアのうち OS は，本体部分と個々のアプリケーションに依存して設定されるデータの部分に分類できる場合があると考えますが（例えば，前者は ROM として H/W と一体的に実装される部分，後者はデータとしてダウンロードされる部分など），ライフサイクル管理，構成管理，V&V の対象となるのはどの範囲か示してください。

〇規程の解説３ではデジタル計算機のソフトウエアについて分類を記載していますが，解説-2 の参考図１，２に示すデジタル計算機以外の部分に，組込デジタルデバイス(組込ソフトウエア含む)がある場合に，どのように扱われるか示してください。規程 4.19.1～ 4.19.3 は何れも「デジタル安全保護系のソフトウエア」と記載されているため，解説３における「特にことわりの無い場合」は適用されず，デジタル安全保護系全体を対象としているように解釈される可能性があると考えられます。

〇上記を総合して，ソフトウエアに関連する規程の各々の適用範囲について分かり易く示してください。回答方法は問いませんが，例えば以下のような表にまとめることが考えられます。(回答が不明のものは空欄)

回答 （2）－1

○「4.19 品質保証」:

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」（一般的に言う，アプリケーションソフト）のみを対象としています。

その理由は，この「安全保護系としての機能を実現するソフトウェア」が，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，ソフトウェアの論理回路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「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，2011 年の NISA 技術評価書においても「ハードウェアと直接結びついて計算機の基本動作を制御するソフトウェア」（一般的に言う，OS やファームウェア）を V&V の対象から除外することは妥当だという見解が記載されていました。

○「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」（一般的に言う，アプリケーションソフト）のみ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」を適用範囲としています。

このように，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，今後の改定で検討してゆきます。

また，核計装および放射線モニタにおいてディジタル装置を適用している場合は，JEAC4620 の 4.16 から 4.19 の適用範囲外ではありますが，JEAC4620 と同様な要求事項を準用することによって，品質の向上を図ることは有用と考えられます。

○要求事項の 4.1 から 4.15 は，ディジタル安全保護系全般への要求事項であり，核計装および放射線モニタにも適用されます。

○要求事項の 4.16（自己診断機能）およびお 4.18（不正アクセス行為等の被害の防止）は，核

計装および放射線モニタに用いられる「ディジタル装置」について，解説-15 や解説-17 の例示を含め，同様に適用可能と考えます。

○要求事項の 4.17（ソフトウェアの管理外の変更の防止）は，核計装および放射線モニタのアプリケーションソフトウェアについて，解説-16 の例示を含め，同様に適用可能と考えます。

○要求事項の 4.19（品質保証）は，核計装および放射線モニタのアプリケーションソフトウェアについて，基本的な原子力品質保証の適用を前提として，ソフトウェアライフサイクル・ソフトウェアの構成管理・V&V に準じた活動を実施することは可能と考えます。

なお，これらの要求事項の適用性について下表に整理しました。

	安全保護系					設計・保守用ソフトウェア・ツール
	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」			ディジタル化された核計装・放射線モニタ	ディジタル化された温度計装	
	アプリケーションソフト	基本ソフト ファームウェア	ハードウェア			
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	○	○	○	―	―	―
4.19.1 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	○	―	―	―	―	―
(原子力品質保証)	(適用範囲)	(適用範囲)	(適用範囲)	(適用範囲)	(適用範囲)	(適用範囲)

○：JEAC4620 の適用範囲　　―：JEAC4620 の適用範囲外

（補足）

○④組込回路がFPGAによる場合であって，その品質保証がV&Vによる場合（S/W と見なす場合）と，フルカバーの試験による場合（H/W と見なす場合）に分かれる場合は，各々の場合について示してください。

○デジタル化された核・放射線計装については，これまでの回答では④S/Wに該当すると考えられますが，この理解が正しいか確認の上で，4.17～4.19の適用範囲を示してください。

○デジタル化された温度計装については，デジタル化範囲の機能・実装方法等に基づいて②④の何れが適用範囲となるのか，あるいは範囲外かを示してください。また国際的にV&Vによらず定性評価を適用可能となる部分（検出器等）か否かについて示してください。

回答（2）－2

ディジタル安全保護系の「ディジタル計算機」の入出力回路等にFPGAを使用しているケースがあり，その FPGA にはロジックが組み込まれていますが，これは「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 の対象としてはおりません。

また，この部分は，基本的にハードウェアとして扱っていますが，そこに組み込まれるロジックの検証及び妥当性確認は，基本的な原子力品質保証活動（JEAC4111 又は JEAG4121）に基づいて実施しており，その製造メーカや機種によって方法が異なります。

回答（2）－3

ディジタル化された核・放射線計装については，検出器として扱っており，「ディジタル計算機」には該当しません。このため，JEAC4620 としてはディジタル化された核・放射線計装を4.17～4.19の対象範囲としては扱っておりません。

回答（2）－4

ディジタル化された温度計装は，検出器として扱っており，「ディジタル計算機」には該当しません。このため，JEAC4620 としてはディジタル化された温度計装を 4.19.3 の V&V の対象範囲としては扱っておりません。

IEEE 7-4.3.2 に照らし合わせた場合は，本温度計装は V&V の対象になると思われます。