資料１－２

「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
（JEAC4620-2020 及び JEAG4609-2020）

令和4年1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。

○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） 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

[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

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。

[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。

（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。

（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。

○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）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。

回答 1）

No	NISA/JNES 技術評価書の適用条件	JEAC4620 への反映
1	**①過渡時，事故時及び地震時の機能** 運転時の異常な過渡変化が生じる場合又は地震の発生等により原子炉の運転に支障が生じる場合において，原子炉停止系統及び工学的安全施設と併せて機能することにより，燃料許容損傷限界を超えないよう安全保護系の設定値を決定すること。	「4.1 過渡時及び地震時の機能」及び「4.2 事故時の機能」に左記条件を考慮した記載を追記。 記載内容については，技術基準規則との整合性を考慮して反映。
2	**②検証及び妥当性確認** 検証と妥当性確認の実施に際して作成された文書は，構成管理計画の中に文書の保存を定め，適切に管理すること。	(解説-23)に左記条件を追記。
3	**③環境条件** デジタル計算機を設置するプラントで想定されるサージ電圧や電磁波等の外部からの外乱・ノイズについて，その対策の妥当性が十分であることを確証すること。	2008 年版における「4.8 環境条件」を「4.9 外的要因」として，「環境条件」，「耐震性」，「その他の外的要因」に関する要求事項とその確証に関する記載に変更。 「4.9.1 環境条件」に，左記条件を考慮して外部からの外乱・ノイズに関する記載を追記。
4	**④計測制御系との分離** デジタル安全保護系は，試験時を除き，計測制御系からの情報を受けないこと，又は計測制御系からの情報を受ける場合には，計測制御系の故障により，デジタル安全保護系が影響を受けないこと。 デジタル安全保護系及び計測制御系の伝送ラインを共用する場合，通信をつかさどる制御装置は発信側システムの装置とすること。	左記条件を踏まえて，「ディジタル安全保護系は，計測制御系と部分的に共用する場合には，計測制御系で故障が生じてもディジタル安全保護系に影響のないよう，計測制御系と電気的に分離する設計とすること。」を要求事項として，本文に反映。 「デジタル安全保護系は，試験時を除き，計測制御系からの情報を受けな

		いこと」，及び「通信をつかさどる制御装置は発信側システムの装置とすること」については，実際の対策例を考慮した上で，（解説-8）に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記載。
5	**⑤外部ネットワークとの遮断** 外部影響の防止された設備とすること。	2008 年版における「4.16 外部ネットワークとの遮断」を，「4.18 不正アクセス行為等の被害の防止」の措置の例として，左記条件を考慮して（解説-17）に記載。
6	**⑥アンアベイラビリティ及び誤動作率の評価** 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。デジタル安全保護系の信頼性評価において，ハードウェア構成要素に異常の検出，検出信号の伝送，入出力信号の処理，演算処理，トリップ信号の伝送，トリップの作動等，評価に必要な構成要素を含むこと。	左記条件については，「4. ディジタル安全保護系に対する要求事項」の本文に，「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，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。 信頼性評価に必要な構成要素については，（解説－4）として左記条件の記載を追記。
7	なお，別記-7 No.10 の要求事項に対して，「デジタル安全保護系規程」には該当する記載がないことから，安全保護系に用いられるデジタル計算機の健全性を実証できない場合，安全保護機能の遂行を担保するための原理の異なる手段を別途用意すること。	JEAC4620 については，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ある。 「ディジタル安全保護系と動作原理等が異なる追加の設備を設けること」については，ディジタル安全保護系への要求事項ではないことから，これまでと同様，留意事項にとどめており，要求事項としては反映していない。 【1.（16）（17）回答参照。】

（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]。

[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

回答 2）

2008 年に本規程を制定する際に，ディジタル安全保護系に関連する IEEE,IEC 規格などの海外規格及び国内規制／規格を調査しています。調査の結果，国内で初めてディジタル安全保護系の要件をまとめた規程（JEAC4620）を作成するにあたり，要件の項目を抽出するために参考とした規制／規格を，安全設計審査指針，技術基準（当時の別記―７含む），JEAG4604-1993，IEEE7-4.3.2-2003（そのベースとなる IEEE603-1998 含む）としました。それらの比較表を表（２）－１に示します。

2020 年版改定時においても同様の調査を実施していますが，調査段階においては IEEE7-4.3.2 の 2016 年版は未発行の状態であり，次回改定時に調査及び反映検討をすることとしていました。参考に IEEE7-4.3.2－2016 と JEAC4620-2020 との比較を表（２）－２に示します。

また，IEEE7-4.3.2－2016 のうち，JEAC4620-2020 に反映されていない項目の一覧を表（２）－３に示します。

次回改定時においても国内外の規制／規格の反映検討は実施していきます。

表（2）－1　安全保護系に関する各種基準・指針間での要求事項の対応整理　（2007 年当時の検討）

要求事項	国内規制要求			国内民間指針				米国民間指針	
	安全設計審査指針	技術基準	別記－７	JEAG-4604-1993	JEAG-4609-1999	JEAG-4611-1991	JEAC-4620	IEEE-603-1998	IEEE-7.4.3.2-2003
(a) 多重性（単一故障基準）	指針 34	第 22 条の二		3.1	解説-4 (3)	4.2 (1) a.	4.3	5.1, 6.3	←
(b) 分離・独立性	指針 35	第 22 条の三		3.2	解説-4 (4)	（同上）	4.4	5.6	5.6
(c) 過渡時の機能	指針 36	第 22 条の一		3.3	解説-4 (1)		4.1	－	－
(d) 事故時の機能	指針 37	（同上）		3.4	（同上）		（同上）	－	－
(e) 故障時の機能	指針 38	第 22 条の四		3.5	解説-4 (5)		4.5	－	－
(f) 計測制御系との分離	指針 39	第 22 条の五	7.	3.6	解説-4 (6)		4.6	5.6	5.6
(g) 試験可能性	指針 40	第 22 条の六		3.7	解説-4 (7)	4.3	4.7	5.7, 6.5	←, 5.5.2
(h) 環境条件			4.	3.8	解説-4 (8)	4.2 (1) b.	4.8	5.5	5.5.1
(i) 自然現象（地震他）	指針　2			3.9	（同上）	4.2 (1) c.	（同上）	5.5	←
(j) 外部人為事象（アクセス管理）	指針　3		3.(2)	3.10	4.(2)		4.17	5.9	←
(k) 内部発生飛来物	指針　4			3.11			－	5.5	←
(l) 火災	指針　5			3.12	解説-4 (8)	4.2 (5)	4.8	5.5	←
(m) ユニット間共用	指針　7			3.13	解説-4 (9)		－	5.13	←
(n) バイパス				3.14			4.3	6.6, 6.7, 7.4, 7.5	←
(o) 非常用電源	指針 48			3.15	解説-4 (10)	4.2 (1) d.	4.9	8.1	←
(p) 設定値の変更		第 22 条の七		3.16	解説-4 (11)		4.10	6.8	←
(q) 入力パラメータ選定				3.17			4.11	6.4	←
(r) 保護動作の完了				3.18			4.12	5.2, 7.3	←
(s) 手動操作				3.19			4.13	6.2	←
(t) 中央表示				3.20			4.14	5.8	←
(u) 保守・補修				3.21			－	5.10	←
(v) 精度・応答時間			5.		解説-4 (2)		4.2	6.8	←
(w) 品質管理						4.5	4.18	5.3	←
(w-1) ライフサイクルプロセス			1.(a)				4.19	－	5.3
(w-2) 品質指標			1.(b)				(4.19)	－	5.3.1
(w-3) ソフトウエアツール			1.(c)				(JEAG-4609)	－	5.3.2
(w-4) Ｖ＆Ｖ			2.(1),(2),(4),(5)		5.		4.21	－	5.3.3
(w-5) Ｖ＆Ｖ体制			2.(3)		5.2 (2)		4.21(1)	－	5.3.4
(w-6) 構成管理			3. 3.(1)				4.20	－	5.3.5
(w-7) プロジェクトリスク管理							－	－	5.3.6
(x) 機器認定							4.18	5.4	5.4.1
(x-1) ＣＯＴＳ			1.(c)				(4.18)	－	5.4.2
(y) 識別							－	5.11	5.11
(z) 補助機能							－	5.12	←
(A) 人間工学							－	5.14	←
(B) 信頼性評価			9.				4.	5.15	5.15
(C) 共通要因故障			10.		4.(1), 解説-5		5.	5.16	－
(D) 自己診断			6.				4.15	－	5.5.3
(E) 外部ネットワーク			8.				4.16	－	－

（注１：項目の対応のみであり，各要求事項の範囲・深さが同等であることを保証するものではない）

（注２：「－」は記載なしを意味する。　「←」は IEEE-603 の記載内容以外にディジタル設備としての追加要求がないことを意味する。）

表（2）－2　JEAC4620 と IEEE-603 および IEEE-7.4.3.2 の最新版記載項目の比較

JEAC-4620-2020	要求事項	IEEE-603-2009 (IEEE-603-2018)	IEEE-7.4.3.2-2016	（参考） JEAC-4604-2009	安全設計 審査指針	設置許可規則	技術基準規則
4.1	過渡時及び地震時の機能	6.1，7.1	←	3.3	指針 36	24 条の 1	35 条の 1
4.2	事故時の機能	6.1，7.1	←	3.4	指針 37	24 条の 2	
4.3	精度及び応答時間	6.8，5.5	←				
4.4	多重性	5.1，6.3	5.1	3.1	指針 34	12 条の 2，24 条の 3	35 条の 2
4.5	独立性（安全系間の分離）	5.6，5.6.1	5.6.4	3.2	指針 35	24 条の 4	35 条の 3
4.6	計測制御系との分離	5.6，5.6.3，6.3	5.6.4	3.6	指針 39	24 条の 7	35 条の 6
4.7	故障時の機能	－	5.5.1	3.5	指針 38	24 条の 5	35 条の 4
4.8	試験可能性	5.7，6.5	5.7，5.5.2	3.7	指針 40	24 条の 4	35 条の 7
4.9.1	環境条件	5.5	5.5	3.8		12 条の 3	14 条
4.9.2	耐震性	5.5	←	3.9	指針　2	4 条	5 条
4.9.3	その他の外的要因（火災・溢水）	5.5	←	3.12	指針　5	8 条，9 条	11 条，12 条
4.9.4	設計の確証	5.4	5.4				
－	優先ロジック	－	5.5.4				
－	内部発生飛来物	5.5	←	3.11	指針　4	12 条の 5	15 条の 4
－	バイパス	6.6，6.7,7.4，7.5	←	3.14			
4.10	非常用電源の使用	8.1	←	3.15	指針 48	33 条	45 条
4.11	設定値の変更	6.8	←	3.16			35 条の 8
4.12	入力変数の選定	6.4	←	3.17			
4.13	保護動作の完全性	5.2，7.3	←	3.18			
4.14	手動操作	6.2	←	3.19			
4.15	動作およびバイパスの表示	5.8	5.8	3.20			
－	保守・補修	5.10	←	3.21			
4.16	自己診断	－	5.5.3				
4.17	ソフトウエアの管理外の変更の防止	－	5.9				
4.18	不正アクセス行為等の被害の防止	5.9	5.9	3.10	指針　3	24 条の 6	35 条の 5
4.19	品質保証	5.3	5.3				
4.19.1	ライフサイクルプロセス	－	5.3.1				
4.19.2	構成管理	－	5.3.5				
(JEAG-4609・4.2)	ソフトウエアツール	－	5.3.2				
4.19.3	Ｖ＆Ｖ	－	5.3.3，5.3.4				
－	プロジェクトリスク管理	－	5.3.6				
－	識別	5.11	5.11				
－	補助機能	5.12	←				
－	ユニット間共用	5.13	←	3.13	指針　7	12 条の 6	15 条の 5
－	人間工学	5.14	←				
4.	信頼性評価	5.15	5.15				
5.	留意事項（共通要因故障）	5.16	5.16				
－	ＣＯＴＳ	－	5.17				
－	シンプルさ	－	5.18				

（注１：項目の対応のみであり，各要求事項の範囲・深さが同等であることを保証するものではない）

（注２：「－」は記載なしを意味する。　「←」は IEEE-603 の記載内容以外に 7-4.3.2 にディジタル設備としての追加要求がないことを意味する。）

表（2）－3　IEEE には項目があるが，JEAC4620 には項目がないもの

要求事項	IEEE-603-2009 (IEEE-603-2018)	IEEE-7.4.3.2-2016	JEAC4620 に記載がない理由
優先ロジック	－	5.5.4	今後検討（IEEE-7.4.3.2-2003 に無し）
内部発生飛来物	5.5	←	ディジタル安全保護系特有の要件ではないため（JEAC4604 には記載）
バイパス	6.6，6.7,7.4，7.5	←	ディジタル安全保護系特有の要件ではないため（JEAC4604 には記載）
保守・補修	5.10	←	ディジタル安全保護系特有の要件ではないため（JEAC4604 には記載）
プロジェクトリスク管理	－	5.3.6	プロジェクト管理の例であるため
識別	5.11	5.11	ディジタル安全保護系特有の要件ではないため
補助機能	5.12	←	ディジタル安全保護系特有の要件ではないため
ユニット間共用	5.13	←	ディジタル安全保護系特有の要件ではないため（JEAC4604 には記載）
人間工学	5.14	←	HFE の手法が国内では確立していなかったため
ＣＯＴＳ	－	5.17	国内では一般産業品の使用はなく，プラントメーカからの製品供給のみであるため
シンプルさ	－	5.18	今後検討（IEEE-7.4.3.2-2003 に無し）。ただし IEEE にも特段の要求事項はない

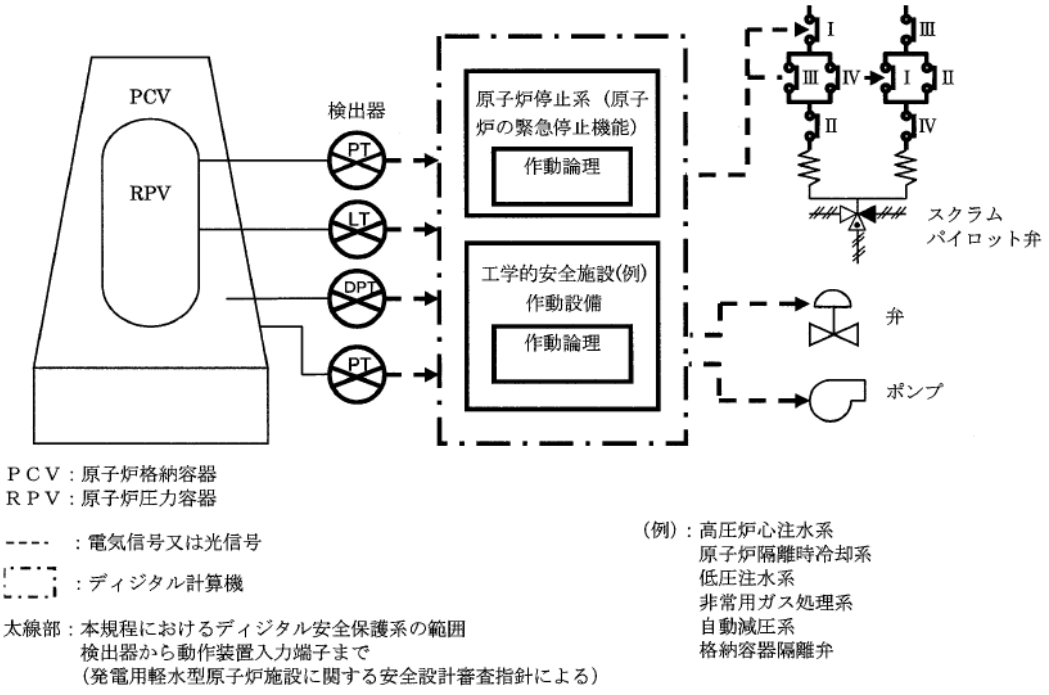
（3）2020 年版において、「安全保護系」の用語の定義に、検出器が含まれることが明記されました。核計装や放射線計装などのデジタル化された装置に関する必要な要件は、本規程に含まれるのか説明してください。

回答 3）

本規程は，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います。核計装や放射線計装は，演算部分を含め検出部として扱い，本規程の対象範囲外です。

なお，解説—2の適用範囲の概要図において，本規程の対象範囲であるディジタル計算機の箇所を┌ ╌ ╌ ┐└ ╌ ╌ ┘にて囲っております。

ただし，ご質問いただいたとおり，本規程の範囲に対する記載がわかりづらいことを認識いたしましたので，次回改定時には改善を図るよう検討致します。



参考図１　ディジタル安全保護系の概念図（BWR）

（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。

[2] Programmable Logic Device
[3] Field Programmable Gate Array

回答 4）

国内においては，安全保護系のディジタル計算機のうち信号入出力部（IO 部品）等として一部に PLD を採用した実績はありますが，安全保護系としての機能を実現するソフトウェア（ディジタルデータの算術演算，論理演算などの計算を行う装置）に係る部分には採用実績がないため，現行版では PLD を「3.1 ディジタル計算機」の対象範囲としておりません。

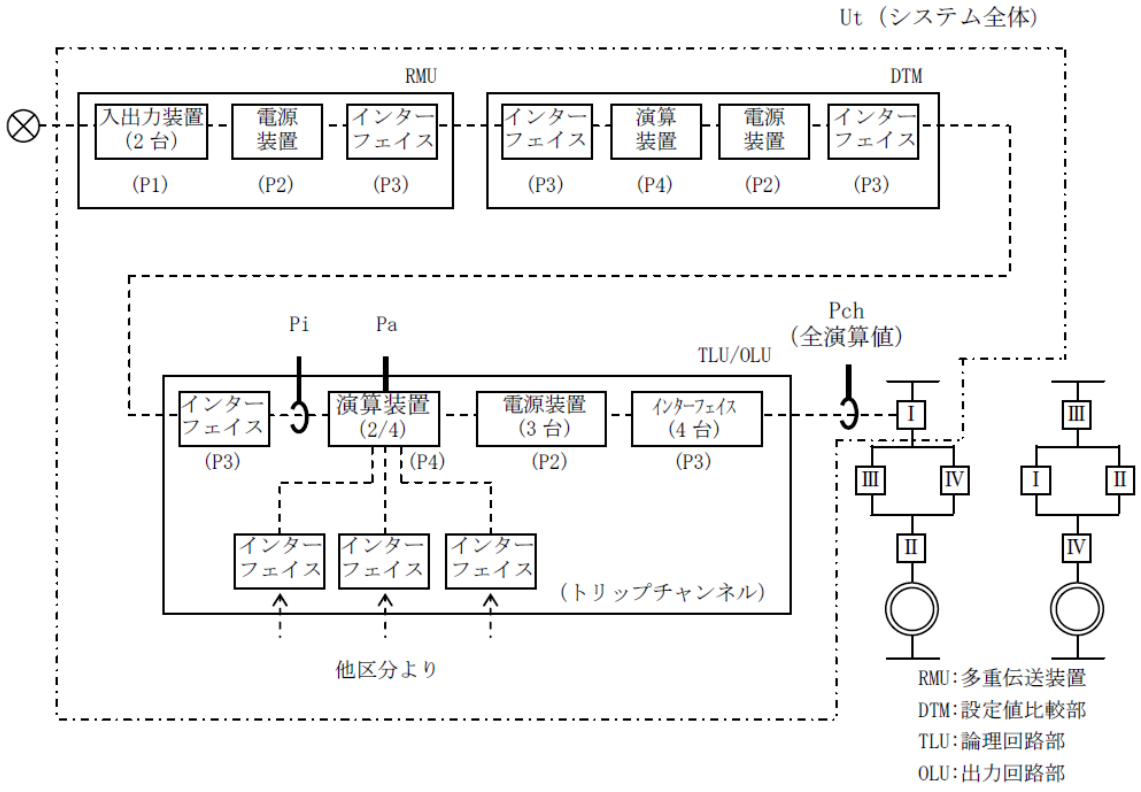
ただし，将来的には安全保護系としての機能を実現するソフトウェアとして PLD が採用される可能性もあり，また，IEEE でも PLD を対象範囲に加えてきていることから，次回以降の改定において，PLD の取り扱いも検討していきたいと考えております。

（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。

回答 5）

ディジタル安全保護系の信頼性に関しては，下記のように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。例として，ABWR の原子炉緊急停止系の信頼性評価モデル（下図）を用いて説明します。

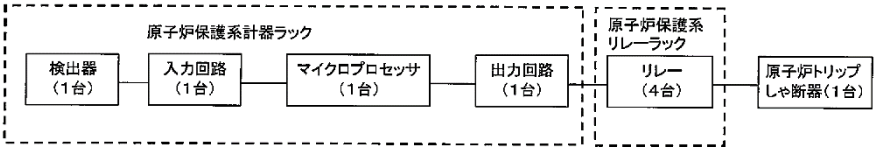
<ABWR の信頼性評価モデル>



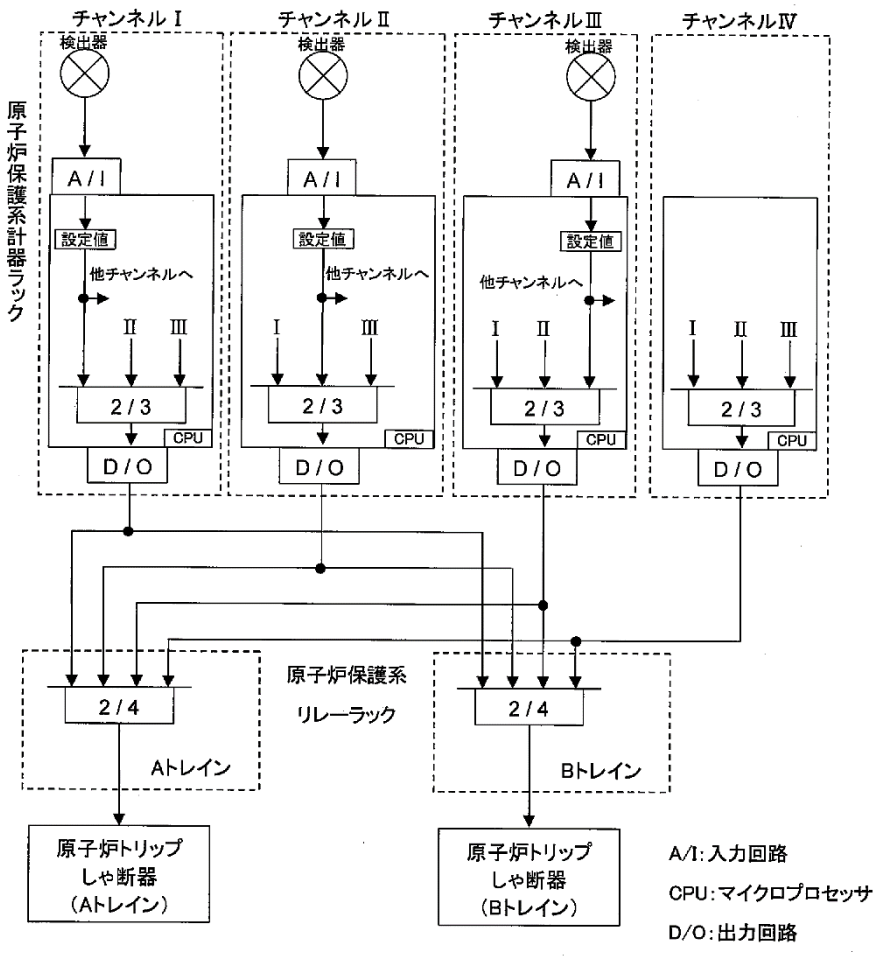
評価対象は，装置の入力からロードドライバ開までのディジタル安全保護系（一点鎖線の範囲）を対象としています。システム全体のアンアベイラビリティを構成要素のアベイラビリティを組み合わせることにより求めます。ここでは，原子炉スクラム要求時にスクラムが失敗する確率として，2 out of 4 システムの 3 重故障を求めます。また，誤動作率については，最初の故障の修理中に 2 番目の故障が生じる 2 重故障で誤スクラムが生じる頻度を求めます。

PWR の場合も同様に，信頼性評価モデルを使用して評価しております。PWR での評価モデルを下図に示します。

〈PWR の信頼性評価モデル〉

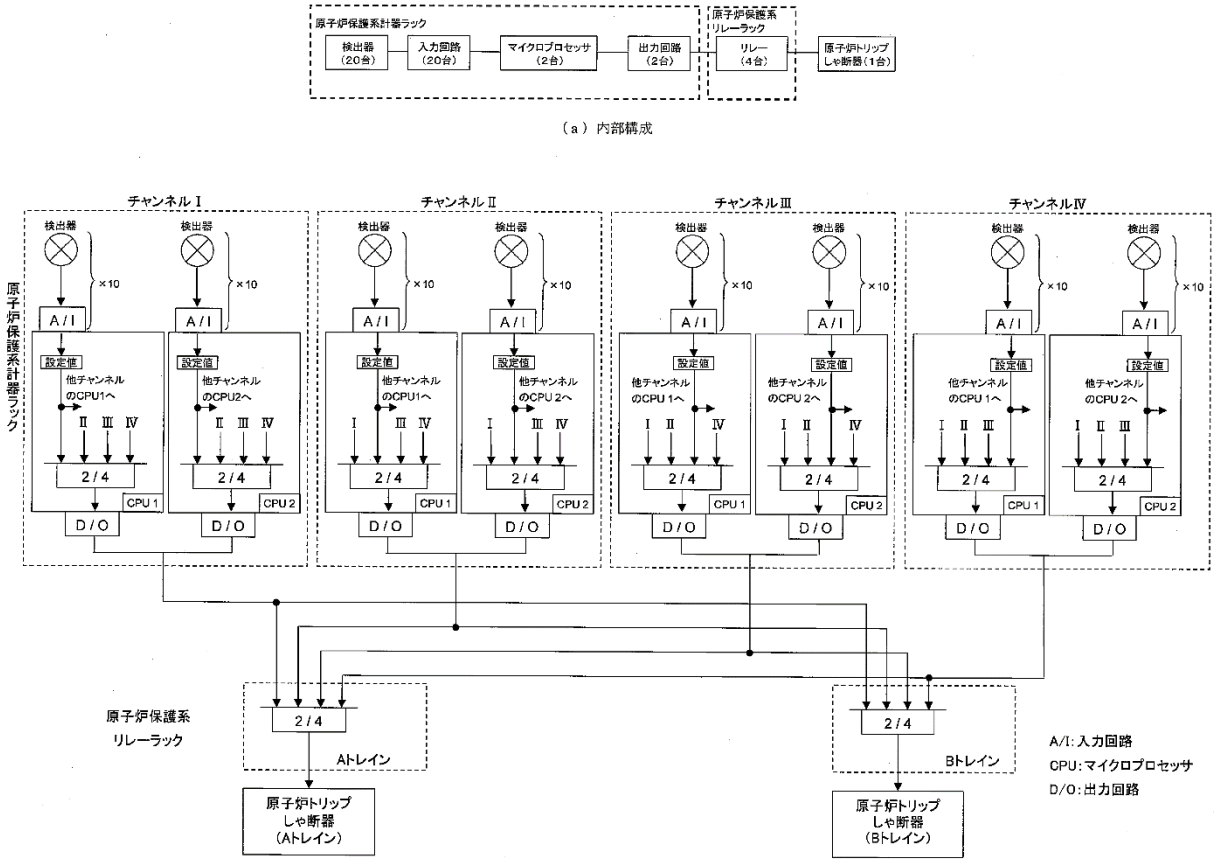


（ａ）内部構成



（ｂ）全体構成

第２図　アンアベイラビリティ評価モデル



第3図　誤動作率評価モデル

また，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しか考慮しておりません。一方で，ディジタル安全保護系は高い信頼性が要求されるため，課題であるソフトウェアの設計製作段階における信頼性確保のための手法として，JEAC4620/JEAG4609 で V&V を実施することを要求しております。

（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。

回答 ６）

ご指摘の通り，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。（解説-4）での記載の趣旨は，”異常の検出”，“検出信号の伝送”等の機能を実現するハードウェア構成要素を，信頼性評価において適切に考慮するよう求めるものです。

実際，（５）で示したモデルにもあるように，安全保護系の機能を実現するソフトウェアの演算処理を行う要素だけでなく，電源や信号伝送（異常検出信号含む）を担うインターフェイス回路などの構成要素についても信頼性評価で考慮することとしています。

（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。

回答 7）

4.6 で計装制御系との分離については「計測制御系で故障が生じてもディジタル安全保護系に影響がない」ものとすることを要求しており，これに対応して機能的な影響の波及を防止する手法として，解説-8 に適用可能な仕様の例を示しています。

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。

ただし，あくまでも例示であり，例示された措置以外の方法によって機能的分離を達成することを妨げるものではありません。

（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。

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

回答 ８）

米国における計測制御系（No-Safety System）との通信の独立性に関する要求事項等は米国の民間規格である IEEE 7-4.3.2 を参考としています。

IEEE 7-4.3.2 の 2003 年版においては，通信の独立性のガイドラインは Annex E に記載されており，2ポートメモリ（バッファメモリ）を用いた例が記載されています。

2010 年版では ISG での検討などを踏まえて，5.6.4 節において，バッファメモリの適用方法の詳細，およびその他通信の実現にあたっての個々の仕様に関する事項などが記載されており，2016 年版でも同様となっています。

JEAC4620 では，要求事項の基本となる「計測制御系で故障が生じてもディジタル安全保護系に影響がない」ものとすることを記載しており，実現方法としての個々の設計仕様に係る要求事項は記載していません。なお，適用可能な設計方針の例としては解説-8 に記載しています。

（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。

[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。

回答 ９）

本規程は安全保護系のディジタル計算機への性能規定を示しており，それを達成する具体的な方法及び数値基準は記載しておりません。各事業者・メーカーは，設置場所の環境等を踏まえて外乱・ノイズへの対応方針や試験内容等を具体化した上で，設計・製作を実施しています。

2008 年版に記載していた JEAG4608 については，「外部からの外乱・ノイズ」に対して JEAG4608 だけを準拠すればよいと誤解されかねないため，2020 年版では削除しました。

（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。

回答 10）

「4.9 外的要因」では，ディジタル安全保護系が，使用時に想定される周辺環境等の外部要因に対して，その安全機能を維持するために考慮すべき項目を示しています。そのうち，「4.9.1 環境条件」および「4.9.2 耐震性」で示す各条件（温度，湿度，放射線量，耐震等）は，ディジタル安全保護系自身がその外部環境に耐え，安全機能を維持することが必要であるため，「4.9.4 設計の確証」において，設計の適格性を確証することを求めています。

一方，「4.9.3 その他の外的要因」で示す火災防護および溢水防護は，ディジタル安全保護系以外のシステム設計等と合わせて対応するものです。例えば火災防護では，安全系の一系統が火災により機能喪失した場合の原子炉冷態停止が求められており，ディジタル安全保護系のうち一系統の火災を仮に想定した上で，対策を講じていきます。このため，本規程においては，火災防護及び溢水防護に係る設計の確証は求めず，それぞれの防護設計・評価において設計の妥当性を確認することとしています。

（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。

回答 11）

安全保護系の動作が行われた場合，その動作した要素が中央制御室に警報として告知されるものとし，1 チャンネルでも動作すれば警報を発するとともに，チャンネルごとに動作状態を表示するものとしています。

ここで，JEAC4620 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」ことを要求しております。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，以下にABWR/PWR それぞれの例を参考として示します。

ABWR では，ディジタル安全保護系の作動要因としている以下の警報項目について，大型表示盤にハードウェア警報窓を設置しています。また，プラント異常の事象把握を支援するものとして，前記警報窓の最上部に大型ファーストヒット表示部を設け，4 大イベント（①MSIV(主蒸気隔離弁)閉，②原子炉スクラム，③タービントリップ，④発電機トリップ）の中で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機能を有しています。

＜ディジタル安全保護系の動作原因（ABWR の例）＞

・原子炉水位低（L-3，L-2，L-1.5，L-1）
・中性子束高高
・ペリオド短短
・D/W 圧力高高
・地震加速度大
・原子炉圧力高高
・MSIV2 弁以上閉
・炉心流量急減
・主蒸気管放射能高高
・CV 急閉
・MSV 閉
・制御棒充填水圧力低
・復水器真空度低
・主蒸気管室温度高
・主蒸気管圧力低
・主蒸気流量高

・原子炉建屋放射能高高
・燃料取替床放射能高高

PWRの総合デジタルプラントでは，第 1 原因の把握として，以下の警報項目について，ファーストアウト警報を設けています。ファーストアウト警報は，運転コンソールに設置された警報VDUに表示されます。また，大型表示装置及び監視操作VDUには，ファーストアウト警報のファーストヒットを監視情報として表示する設計としています。

＜ディジタル安全保護系の動作原因（PWR の例）＞
・中性子束高（SR/IR/PR）
・中性子束変化率高（PR）
・1次冷却材可変温度高（過大温度/過大出力）
・加圧器圧力高
・加圧器圧力低
・1次冷却材流量喪失
・タービントリップ
・蒸気発生器主給水流量低
・蒸気発生器水位異常低
・加圧器水位高
・地震
・加圧器圧力低と加圧器水位低の一致
・加圧器圧力異常低
・主蒸気流量高と主蒸気圧力低の一致
・主蒸気流量高と1次冷却材平均温度異常低の一致
・主蒸気差圧高
・格納容器圧力高
・格納容器圧力異常高

（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。

回答 12）

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を言います。BWR での例を以下に示しますが，これらのいずれかを適用して適切に設計することを考慮しています　。

・外部ネットワークとの直接接続をしない。
・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を設ける。
・安全保護装置の信号を一方向（送信機能のみ）通信に制限し外部からのデータ書き込み機能を設けない。

（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。

回答 13）

規格化にあたっては，技術基準規則の解釈（第三十五条）より引用するとともに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。

設計段階においては言及しておりませんが，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ので，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管理する必要があると考えます。

（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。

回答 14）

JEAC4620 および JEAG4609 では，特定のライフサイクルを指定はしていません。製品・機種などに応じてライフサイクルを予め設定し，これに基づいて品質保証の計画を立てて実行することを要求しています。

JIS X 0160:2021「ソフトウェアライフサイクルプロセス」は，ISO/IEC/IEEE 12207「Software life cycle processes」を国内向けに翻訳したものであり，初版は 2012 年に発行されています。JIS X 0160 は「ソフトウェアシステムのライフサイクルにおける，取得者，供給者及び他の利害関係者の間で円滑に情報伝達を行う場合に必要な定義されたプロセスの集合を提供すること(1.2 目的)」すなわち関係者間の認識統一のための共通の言語の提供を目的としています。

このため，JIS X 0160 も特定のライフサイクル（例えばウォーターフォールモデル）を定義するものではなく，ライフサイクルで実施される様々な活動（プロセス及びこれを構成するアクティビティ及びタスク）を関係者が同じ用語・理解で取り組めるように定義し標準化したものです。なお，JIS X 0160 は，明記はされていませんが，主にソフトウエアハウスが顧客の注文を受けてソフトウェアの開発や導入・運用・保守を行うような業務を想定しているものと考えています。

JIS X 0160 に記載された「プロセス」を次葉に示します。このプロセスの中にはプロジェクトマネジメントや品質保証に係るものも多く含まれていますが，JEAC4620 および JEAG4609 で取り上げている活動と対応するのは主に「テクニカルプロセス」の一部と考えます。
JEAC4620 および JEAG4609 での設計・製作・試験・装荷のプロセスや V&V 活動，構成管理などが対応しており，ほぼ同様な範囲をカバーしていると考えられます。

なお，JEAC4620 および JEAG4609 ではプラントごとの安全保護系の機能を実現するソフトウェアのみを対象としており，それ以外は一般の原子力品質保証活動の対象となります。

JIS X 0160 の記載事項は，様々なプロセスでの実施内容について細分化して定義を明確化・標準化し，実務の計画検討にあたっての関係者間での確認項目として活用できるものであり，所謂「要求事項」を記載したものではありませんが，設計実務に参考になるものであると考えます。

（JIS X 0160 に記載されたプロセス：番号は JIS の章番号）

6.1 合意プロセス
- 6.1.1 取得プロセス
- 6.1.2 供給プロセス

6.2 組織のプロジェクトイネーブリングプロセス
- 6.2.1 ライフサイクルモデル管理プロセス
- 6.2.2 インフラストラクチャ管理プロセス
- 6.2.3 ポートフォリオ管理プロセス
- 6.2.4 人的資源管理プロセス
- 6.2.5 品質管理プロセス
- 6.2.6 知識管理プロセス

6.3 テクニカルマネジメントプロセス
- 6.3.1 プロジェクト計画プロセス
- 6.3.2 プロジェクトアセスメント及び制御プロセス
- 6.3.3 意思決定管理プロセス
- 6.3.4 リスク管理プロセス
- 6.3.5 構成管理プロセス
- 6.3.6 情報管理プロセス
- 6.3.7 測定プロセス
- 6.3.8 品質保証プロセス

6.4 テクニカルプロセス
- 6.4.1 ビジネス又はミッション分析プロセス
  （ビジネス又はミッションにおける問題を定義し可能性をもつソリューションを決定）
- 6.4.2 利害関係者ニーズ及び利害関係者要件（要求事項）定義プロセス
  （利害関係者を識別し，そのニーズを定義）
- 6.4.3 システム及び／又はソフトウェア要件（要求事項）定義プロセス
  （要望されている能力についての利用者主体のビューを，ソリューションについての技術面のビューへ変換）
- 6.4.4 アーキテクチャ定義プロセス
  （システムアーキテクチャの候補及びその代替案を作成し，システム要件を満たす一つ以上の代替案を選定し，アーキテクチャを表現）
- 6.4.5 設計定義プロセス

（アーキテクチャ エンティティとの一貫性をもった実装を可能にするために，システム及びその構成要素に関する十分に詳細なデータ及び情報を提供）

6.4.6 システム分析プロセス

（意思決定を支援するために，技術面の理解のための厳密なデータ及び情報の基盤を提供）

6.4.7 実装プロセス

（指定されたシステム要素を実現）

6.4.8 インテグレーションプロセス

（実現されたシステム（製品又はサービス）へと，システム要素の集合を統合）

6.4.9 検証プロセス

（システム又はシステム要素がその指定された要件及び特性を満たしていることの客観的な証拠を提供）

6.4.10 移行プロセス

（システムが運用環境において，規定されたサービスを供給する能力を確立）

6.4.11 妥当性確認プロセス

（システムが意図された運用環境で意図された用途を達成することで，そのビジネス又はミッションの目標及び利害関係者要件を満たすという客観的証拠を提供）

6.4.12 運用プロセス

（システムを利用してサービスを提供）

6.4.13 保守プロセス

（サービスを提供するシステムの能力を維持）

6.4.14 廃棄プロセス

（システム又はその要素の存在を終了させ，置換又は廃棄される要素を適切に処理）

（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。

回答 15）

3.3 の定義および解説－21 に記載の通り，原子力製品としての一般的な品質保証活動に加えて実施する検証および妥当性確認を「V&V」と定義して 4.19 でこれを実施することを要求しています。この V&V の具体的な実施ガイドは JEAG4609 にまとめています。

JEAG4609 は初版が 1989 年に発行されて以来，様々な安全保護系ディジタル化の設計に適用されてきており，V&V の実施に関する内容については実務に十分浸透していると考えています。

JEAC4620 においては，JEAG4609 に記載された事項の中から，Ｖ＆Ｖの実施にあたって特に重要な要求事項と考えられる，組織的な独立性，文書化，再利用の妥当性の３点を要求事項として記載しました。

JEAG4609 については，従来から利用されてきていることから，今回の改定において基本構成は大きく変更していません。

なお，「検証と妥当性確認」という用語（当時は「検証と健全性確認」としていました）は，JEAG4609 の初版の発行当時は一般的な用語ではありませんでしたが，その後，品質保証活動を記述する用語としての一般的な使用が広がってきました。

このため，JEAC4620 および JEAG4609 では，ディジタル安全保護系に対する従来からの活動は「V&V」と表記することとし，一般的な品質保証活動の用語である「（設計）検証と妥当性確認」とは区別しています。

（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。

回答 16）

JEAC4620 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。「ディジタル安全保護系と動作原理等が異なる追加の設備を設けること」については，ディジタル安全保護系に対する要求事項ではないため，推奨事項としております。

推奨事項であるため，規格として設置することを必須とするものではありませんが，事業者の自主的な取り組みとして，基本的に設置することとしております。

また，「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」の主な目的はソフトウェア共通要因故障対策になりますが，ソフトウェア共通要因故障対策については，ATENA において技術要件書がまとめられ，対策実施に関する取り組みが進められています。ATENA で作成した技術要件書の規格化については，現状のところ，検討の動きはありませんが，今後の動向（検討や対策の実施状況）を踏まえて，必要に応じて検討していくことになると考えます。

（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。

回答 17）

JEAC4620 では耐震性，耐環境性，ソフトウェアの信頼性等，様々な面から共通要因故障が発生しないよう設計上の要求事項を規定しております。

ソフトウェアに対しては，JEAG4609 の目的にも記載したとおり，V&V を実施することでソフトウェアの信頼性を高めております。このため，ソフトウェアに対しても，共通要因故障が発生する可能性は十分に低くなっていると考えられます。

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ますが，JEAC4620 は上記のような設計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。このため，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。

また，JEAC4620 制改定の際に参考としております IEEE Std 7-4.3.2-2016 には「5.16 共通要因故障」としてソフトウェア共通要因故障に関する記載があります。主に以下のような点（抜粋）が記載されておりますが，「動作原理等が異なる追加設備を設けること」を必須としたものではありません。

・PDD（※）の設計エラーがソフトウェア共通要因故障を発生させる可能性がある。
・良好な設計対応が設計エラーを低減している。
・共通要因故障を完全に撲滅することはできないが，シンプルなシステム構成や長年の使用実績がある合理的なコードは適切なレベルまで共通要因故障を低減している。
・潜在的な欠陥が多重化されたシステムに共通に存在する場合に問題となる。
・共通要因故障に対しては，対応より防止と制限に重点をおくべきである。
・共通要因故障対応は多面的なアプローチである。
　－ ソフトウェアの欠陥と共通の要因（トリガー）の防止（システム分割等）
　－ 自己診断（ウォッチドッグタイマー等）
　－ 共通要因故障の影響の制限（エラー状態を押さえるシステム設計等）
　－ 深層防護と多様性による共通要因故障による影響の緩和

上記のような点から，JEAC4620 では，多様性に関する内容である「ディジタル安全保護系と動作原理等が異なる追加の設備を設けること」については推奨事項としております。

※ programmable digital device

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。

回答 1）

国内においては，安全保護系のディジタル計算機のうち信号入出力部（IO 部品）等としてのみ PLD を採用しており，安全保護系としての機能を実現するソフトウェア（ディジタルデータの算術演算，論理演算などの計算を行う装置）ではないため，本指針における V&V 対象外となります。

ただし，将来的には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 PLD が採用される可能性もあり，また，IEEE でも PLD を対象範囲に加えてきていることから，次回以降の改定において，PLD の取り扱いも検討していきたいと考えております。