改正　令和５年１０月１１日　原規技発第 2310116 号　原子力規制委員会決定

令和５年１０月１１日

原子力規制委員会

実用発電用原子炉及びその附属施設の技術基準に関する規則の解釈の一部改正について

実用発電用原子炉及びその附属施設の技術基準に関する規則の解釈（原規技発第 1306194 号）の一部を、別表により改正する。

附　則

この規程は、令和５年１０月１１日から施行する。

別表　実用発電用原子炉及びその附属施設の技術基準に関する規則の解釈　新旧対照表

（下線部分は改正部分）

改　正　後	改　正　前
第３５条（安全保護装置） １～３　（略） ４ デジタル安全保護系の適用に当たっては、次のいずれかの規格によること。この場合において、「日本電気協会「安全保護系へのディジタル計算機の適用に関する規程（JEAC 4620）」等の適用に当たって（別記－１１）」によること。 （１）日本電気協会「安全保護系へのディジタル計算機の適用に関する規程」（JEAC 4620-2008）（以下「デジタル安全保護系規程 2008」という。）及び「ディジタル安全保護系の検証及び妥当性確認に関する指針」（JEAG 4609-2008）（以下「デジタル安全保護系 V&V 指針 2008」という。） （２）日本電気協会「安全保護系へのディジタル計算機の適用に関する規程」（JEAC 4620-2020）（以下「デジタル安全保護系規程 2020」という。）及び「ディジタル安全保護系の検証及び妥当性確認に関する指針」（JEAG 4609-2020）（以下「デジタル安全保護系 V&V 指針 2020」という。）	第３５条（安全保護装置） １～３　（略） ４ デジタル安全保護系の適用に当たっては、日本電気協会「安全保護系へのディジタル計算機の適用に関する規程」（JEAC 4620-2008）（以下「JEAC4620」という。）５．留意事項を除く本文、解説－４から６まで、解説－８及び解説－１１から１８まで並びに「ディジタル安全保護系の検証及び妥当性確認に関する指針」（JEAG 4609-2008）本文及び解説－９に以下の要件を付したものによること。ただし、「ディジタル」は「デジタル」と読み替えること。 （１）JEAC4620 の４．１の適用に当たっては、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。 （２）JEAC4620 の４．１８．３において検証及び妥当性確認の実施に際して作成された文書は、４．１８．２の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。 （３）JEAC4620 の４．８における「想定される電源擾乱、電磁波等の外部からの外乱・ノイズの環境条件を考慮した設計とすること」を「想定される電源擾乱、サージ電圧、電磁波等の外部からの外乱・ノイズの環境条件を考慮して設計し、その設計による対策の妥当性が十分であることを確証すること」と読み替えること。 （４）JEAC4620 の４．５及び解説－６の適用に当たっては、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。試験時に、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よう措置を講ずること。 　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。 （５）JEAC4620 の４．１６の「外部からの影響を防止し得る設計」を「外

	部影響の防止された設備」と読み替えること。 （６）JEAC4620 の４．における安全保護機能に相応した高い信頼性を有するとは、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。また、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。 （７）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。 （「日本電気協会「安全保護系へのディジタル計算機の適用に関する規程（JEAC 4620-2008）」及び「ディジタル安全保護系の検証及び妥当性確認に関する指針（JEAG 4609-2008）」に関する技術評価書」（平成２３年１月原子力安全・保安院、原子力安全基盤機構取りまとめ））
別記　一覧 別記－１～１０　（略） 別記－１１　日本電気協会「安全保護系へのディジタル計算機の適用に関する規程（JEAC 4620）」等の適用に当たって	別記　一覧 別記－１～１０　（略） （新設）

別記－１１

日本電気協会「安全保護系へのディジタル計算機の適用に関する規程（JEAC 4620)」等の適用に当たって

技術基準規則第３５条において、デジタル安全保護系規程 2008 及びデジタル安全保護系 V&V 指針 2008、又はデジタル安全保護系規程 2020 及びデジタル安全保護系 V&V 指針 2020 を適用するに当たっては、次の各表の左欄に掲げる項目ごとに同表の中欄に掲げる記載は、それぞれ同表の右欄のとおりとする。

また、技術基準規則第３５条の規定と、デジタル安全保護系規程 2020 及びデジタル安全保護系 V&V 指針 2020 の規定との対応関係は別表１－１に、デジタル安全保護系規程 2008 及びデジタル安全保護系 V&V 指針 2008 の規定との対応関係は別表１－２に、それぞれ掲げるところによる。

なお、これらの規格の適用に当たっての技術的根拠については、以下を参照のこと。

①「日本電気協会「安全保護系へのディジタル計算機の適用に関する規程（JEAC 4620-2008)」及び「ディジタル安全保護系の検証及び妥当性確認に関する指針（JEAG 4609-2008)」に関する技術評価書」(平成２３年１月原子力安全・保安院、原子力安全基盤機構取りまとめ)

②「日本電気協会「安全保護系へのディジタル計算機の適用に関する規程（JEAC 4620-2020)」及び「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（JEAG 4609-2020)」に関する技術評価書」(原規技発第●号（令和●年●月●日原子力規制委員会決定))

表１　デジタル安全保護系規程2020

(解説-3) 機能を実現するソフトウェア	したがって，本規程におけるソフトウェアとは，特にことわりのない場合，安全保護系としての機能を実現するソフトウェアを示す。	（削る）
4. ディジタル安全保護系に対する要求事項	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。 そのため，ディジタル安全保護系は，以下の要求事項を満足すること。	デジタル計算機（原子炉停止系，工学的安全施設作動系，及び重要度と複雑さがこれらと同程度の安全保護装置のその他の機器(例えば，BWR における核計装・放射線モニタ)に適用される電子計算機をいう。以下同じ。）を適用したデジタル安全保護系（以下「デジタル安全保護系」という。）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。 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。 そのため，デジタル安全保護系は，以下の要求事項を満足すること。
4.1 過渡時及び地震時の機能	ディジタル安全保護系は，運転時の異常な過渡変化が発生する場合又は地震の発生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（原子炉の緊急停止機能）又はその他系統と併せて機能することにより，燃料要素の許容損傷限界を超えないようにできる設計とすること。	デジタル安全保護系は，運転時の異常な過渡変化が発生する場合又は地震の発生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（原子炉の緊急停止機能）又はその他系統と併せて機能することにより，燃料要素の許容損傷限界を超えないようにできる設計とすること。 「燃料要素の許容損傷限界を超えない設計」とは，運転時の異常な過渡変化が発生する場合に，燃料要素の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をいう。
4.3 精度及び応答時間	ディジタル安全保護系は，安全保護上必要な精度及び応答時間（リアルタイム性能を含む。）を計算機システムと関連ハードウェア部を合わせた全体システムとして満足する設計とすること。	デジタル安全保護系は，安全保護上必要な精度及び応答時間（リアルタイム性能を含む。）を計算機システムと関連ハードウェア部を合わせた全体システムとして満足する設計とすること。 リアルタイム性能とは，プロセス信号のサンプリング周期及び処理速度が，プロセスの変化速度に十分追従できる能力のことを言い，応答時間にはサンプリング周期及び処理速度も含まれる。
4.5 独立性	ディジタル安全保護系は，一つのチャンネルの故障によって安全保護機能が喪失しないようにチャンネル相互を電気的，物理的に分離し，チャンネル間の独立性を有する設計とすること。さらに，チャンネル間に通信を用いる場合には機能的にも分離する設計とすること。	デジタル安全保護系は，一つのチャンネルの故障によって安全保護機能が喪失しないようにチャンネル相互を電気的，物理的に分離し，チャンネル間の独立性を有する設計とすること。さらに，チャンネル間に通信を用いる場合には機能的にも分離する設計とすること。 多重化されたチャンネル間の通信の機能的分離の措置は、以下に掲げる手段その他適切な手段を考慮する。 (1)多重化されたチャンネル間の通信は，原則として一方通行の通信路を介して情報伝達を行う。双方向通信が可能な通信路を介して情報伝達を行う場合には，発信側のシステムと受信側のシステ

		ム間の調整，接続の失敗等によって，どちらのシステムも機能的に異常をきたさない設計とする。 (2)デジタル安全保護系のプロセッサと通信コントローラの間にバッファメモリを設置する。
4.6 計測制御系との分離	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。さらに，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。	デ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，その安全保護機能を失わないよう，計測制御系から機能的に分離されたものであること。また，計測制御系で故障が生じてもデ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。 デジタル安全保護系と計測制御系とを部分的に共用する場合には，以下のように設計することにより，電気的に分離することができる。 ・デジタル安全保護系と計測制御系との信号取り合いには，光／電気変換などのアイソレーションデバイスを用いる。この場合アイソレーションデバイスは安全保護系に属する。
4.9.1 環境条件	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。 ・設置される場所における予想温度，湿度，放射線量 ・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	デ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。各環境条件については達成すべき水準を明確にすること。 ・設置される場所における予想温度，湿度，放射線量 ・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
4.16 自己診断機能	ディジタル安全保護系は，各チャンネル独立に適切な周期で実施される自己診断機能を有する設計とすること。また，自己診断機能によりディジタル計算機の異常を検知した場合には，ディジタル計算機の異常を運転員へ告知する設計とすること。	デジタル安全保護系は，各チャンネル独立に適切な周期で実施される自己診断機能を有する設計とすること。また，自己診断機能によりデジタル計算機の異常を検知した場合には，デジタル計算機の異常を運転員へ告知する設計とすること。 自己診断機能は，故障を早期発見することができるため，従来のアナログの安全保護系でも実施されている故障進展後の警報及び定期的な試験による健全性確認に加えて，システムの信頼性を更に向上させるのに有効な一手段である。

		自己診断機能によりデジタル計算機の異常が検出された場合には，運転員が適切な措置をとれるよう，警報等により運転員へ告知する。さらに，自動で，当該チャンネルを動作状態又はバイパス状態にすることもある。 自己診断の例として，ウォッチドッグタイマ，パリティチェック，送受信信号の誤り検出，ソフトウェアによるチェック等がある。
4.17 ソフトウェアの管理外の変更の防止	ディジタル安全保護系に装荷するソフトウェアは，管理外の変更を防止する設計とすること。	デジタル安全保護系のデジタル計算機に装荷するソフトウェアは，管理外の変更を防止する設計とすること。 管理外の変更とは，故意による変更など，承認されていない変更のことをいう。 ソフトウェアの管理外の変更を防止する手段の例としては，以下がある。 (1) ソフトウェアの不揮発化 (2) 鍵付きスイッチの設置 (3) パスワードの登録
4.18 不正アクセス行為等の被害の防止	ディジタル安全保護系は，不正アクセス行為等による以下の被害を防止するために必要な措置を講じる設計とすること。 ・ディジタル計算機に使用目的に沿うべき動作をさせない行為 ・ディジタル計算機に使用目的に反する動作をさせる行為	デジタル安全保護系は，不正アクセス行為等による以下の被害を防止するために必要な措置を講じる設計とすること。 ・電子計算機に使用目的に沿うべき動作をさせない行為 ・電子計算機に使用目的に反する動作をさせる行為 不正アクセス行為等の被害の防止に必要な措置は以下の点を考慮する。 (1) 外部ネットワーク（インターネット等）と遮断することにより，外部ネットワークからの遠隔操作，ウイルスの侵入等の外部影響を防止する。外部ネットワークと遮断するとは，物理的な接続を制限し最小限とすること，前記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，可能な限り外側向けの通信を適用することをいう。 (2) 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，更新，試験，保

		守等で，承認されていない者の操作，ウイルス等の侵入等を防止する。 (3) 鍵付きスイッチの設置及びパスワードの登録は，不正アクセス行為等の被害の防止にも有効である。
4.19 品質保証	ディジタル安全保護系に用いられるディジタル計算機は，以下の手法によりソフトウェアの健全性を確保すること。 ・ソフトウェアライフサイクル及び構成管理手法を含めた，品質保証活動 ・V&V 活動	デジタル安全保護系に用いられる電子計算機は，保安活動の重要度に応じ，以下に掲げる手法その他の適切な手法によりソフトウェアの健全性を確保すること。 ・ソフトウェアライフサイクル及び構成管理手法を含めた，品質保証活動 ・V&V 活動 なお，ソフトウェアの品質を高めるために以下の手法を用いることがある。 ・処理構造の簡素化（定周期，シングルタスク構成等） ・適切な使用言語の適用による処理内容の明確化（可視化言語の適用，ツールによる可視化等） ・ソフトウェア品質保証指標による品質管理（品質指標の例：正確さ，完全性，要求の遵守，性能履歴等） 市販電子計算機，既存開発ソフトウェア又はソフトウェアツールを使用する場合には，目的に応じて適切に品質が確保され，ソフトウェア実行時に，他のソフトウェアに欠陥を招かないよう考慮する。
4.19.1 ソフトウェアライフサイクル	ディジタル安全保護系のソフトウェアに対して，ライフサイクルを通じて品質の管理方法を予め定め，実施するとともに，これを文書化すること。	デジタル安全保護系のソフトウェアに対して，ライフサイクルを通じて品質の管理方法を予め定め，実施するとともに，これを文書化すること。 デジタル安全保護系のソフトウェアの品質を確保するために，ソフトウェアに対してライフサイクルプロセスの考えを基にプロセスごとの管理を実施する。ライフサイクルプロセスの例を以下に示す。 (1) ライフサイクルプロセス デジタル安全保護系に装荷されるソフトウェアに対しては，各プ

		ロジェクトのプロセスを定義し，文書化する。プロセスには，設計，製作，試験，装荷，運転，変更及び廃止がある。 以下に各プロセスの内容を示す。 (a)設計プロセス：製品に対するシステムの要求事項からソフトウェア設計仕様を作成するプロセス (b)製作プロセス：ソフトウェア設計仕様よりソフトウェアを製作するプロセス (c)試験プロセス：製作されたソフトウェアに対して試験を実施するプロセス。ソフトウェア単体に対して行う試験とハードウェアと一体となったシステムとして行う試験がある。 (d)装荷プロセス：実機の最終システムへソフトウェアを実装するプロセス (e)運転プロセス：システムを運転しているプロセス (f)変更プロセス：仕様変更等によりソフトウェアを変更するプロセス (g)廃止プロセス：ソフトウェアを使用不可能とするプロセス (2) 各プロセスで実施すべき品質管理項目 各プロセスで実施すべき品質管理項目に対して計画を作成し，その計画に従って実施した結果を文書化する。なお，計画はプロジェクトの開始段階で一括して作成することでもよい。以下に各プロセスで実施すべき品質管理項目の例を示す。 (a) 設計プロセス ソフトウェアに対する仕様を決定する。また，設計検証手段を決定する。 (b) 製作プロセス 仕様のとおりソフトウェアが製作されていること を確認する。 (c) 試験プロセス 要求仕様を確認するための試験方案を作成し，判定基準内にあることを確認する。試験にはソフトウェア単体で行うものとシステ

		ムとして行うものがある。ソフトウェア単体では確認できない内容はシステムとして確認するなど，その範囲については事前に計画する。 (d) 装荷プロセス 管理されたソフトウェアが正しく実機に実装されることを確認する。ソフトウェアのコンペア等を用いて確認する。 (e) 運転プロセス 運転中はシステムに異常が無いことを確認する。 (f) 変更プロセス ソフトウェアの変更要否について調査する。 ソフトウェアに変更が生じる場合には，変更仕様を決定し変更を実施する。実施内容は設計，製作及び試験におけるそれぞれのプロセスに従う。 (g) 廃止プロセス 廃止することを宣言する。代替手段がある場合にはこれを含むものとする。廃止されたソフトウェアが誤って再使用されることのないよう，例えば，記憶媒体の破壊，図面の使用禁止の識別等の措置を講じる。
4.19.2 ソフトウェア構成管理	ディジタル安全保護系のソフトウェアに対して，構成管理手法を予め定め，実施するとともに，構成管理計画として文書化すること。また，ソフトウェアを構成する管理対象項目は，ソフトウェア構成管理計画に基づき，すべてを文書化すること。	デジタル安全保護系のソフトウェアに対して，構成管理手法を予め定め，実施するとともに，構成管理計画として文書化すること。また，ソフトウェアを構成する管理対象項目は，ソフトウェア構成管理計画に基づき，すべてを文書化すること。 構成管理とは，管理対象要素の特定及び識別，要素の管理方法，並びにソフトウェア構成管理のレビュー又は審査方法を，予め定め，計画に基づき実施することである。 具体的な例を以下に示す。 (1) ソフトウェア及び関連文書を特定し，相互に識別するために，予め構成管理計画を策定し，実行する。 (2) 構成管理計画で，以下の内容を定める。 (a) ソフトウェア及び関連文書に

		ついて，管理対象要素を定める。管理対象要素の例としては以下がある。 ・要求仕様 ・設計仕様 ・製作仕様 ・試験仕様／試験結果 ・設計検証手順／設計検証結果 ・V&V 手順／V&V 結果 ・取扱説明 ・製作したソフトウェア (b)管理対象要素の管理手法を定める。管理する項目の例としては以下がある。 ・改訂番号，改訂日付 ・変更要求有無，他の管理対象要素との整合状況等の状態 ・他の管理対象要素との取り合い (c)ソフトウェアの変更時の管理手法を定める。 (d)ソフトウェア構成管理のレビュー又は審査の方法を定める。 (e)以上の項目を実施するための体制を定める。
4.19.3 V&V	ディジタル安全保護系に対しては，ソフトウェアライフサイクルの設計，製作，試験及び変更の各プロセスに応じて V&V を実施すること。 (1) V&V は，設計，製作及び試験を行う個人又はグループと独立した体制で実施すること。 (2) V&V を実施する上で適切な文書化を行うこと。 (3) ソフトウェアの再利用時においては，既存設計での V&V 結果による代替を可能とする前提として再利用範囲を明確に識別し，再利用の妥当性を示す根拠を文書化すること。	デジタル安全保護系に対しては，デジタル計算機のソフトウェアのうち，ハードウェアと直接結びついて計算機の基本動作のみを制御するソフトウェアを除いたもの（以下単に「ソフトウェア」という。）に対しソフトウェアライフサイクルの設計，製作，試験及び変更の各プロセスに応じて V&V を実施すること。 (1) V&V は，設計，製作及び試験を行う個人又はグループと独立した体制で実施すること。 (2) V&V を実施する上で適切な文書化を行うこと。 (3) ソフトウェアの再利用時においては，既存設計での V&V 結果による代替を可能とする前提として再利用範囲を明確に識別し，再利用の妥当性を示す根拠を文書化すること。 4.19.3.1 V&V（手順） 安全保護系は原子炉の安全確保のために高い信頼性が求められる設備であるため，デジタル安全

		保護系の供給者は，「原子力施設の保安のための業務に係る品質管理に必要な体制の基準に関する規則」が求める保安活動を実施する。 V&V については，「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：JEAG4609-2020」による。具体的には，設計プロセス及び製作プロセスにおいて V&V としての検証を実施し，試験プロセスにおいて V&V としての妥当性確認を実施する。 なお，ソフトウェアライフサイクルプロセスにおいて V&V が必要なプロセスとして，設計，製作，試験及び変更がある。 4.19.3.2 V&V（独立性） ソフトウェアの設計，製作及び試験に対する V&V の実施体制の独立性とは下記をいう。 (1)V&V を実施する個人又はグループは，原設計に携わった者以外の個人又はグループであり，V&V を実施する力量を有することを組織が認めた者である。 (2)V&V を実施する個人又はグループは，設計，製作及び試験に携わった個人又はグループから経済面，工程管理に関する制約を受けない。 4.19.3.3 V&V（文書化） V&V の合格基準，不良結果等に対する措置を決定し文書化する。 V&V の実施に際して作成された文書は，構成管理計画の中にこれらの文書の保存を定め，適切に管理する。

・「(解説-2) 適用範囲（概念図)」は、適用除外とする。
・「3.1 ディジタル計算機」は適用除外とする。
・上記表１に掲げていない項目において「ディジタル」は「デジタル」に読み替える。

表２　デジタル安全保護系 V&V 指針 2020

2.適用範囲	したがって，本指針では，安全保護系設備としての機能を実現するソフトウェア（以下，「ソフトウェア」という。）を適用範囲とする。	削る。

4. V&V	ディジタル安全保護系に装荷するソフトウェアに対しては，V&Vを実施して，安全保護上要求される機能が正しく実現されていることを確認する。 ソフトウェアに関するV&Vは，以下の手法によるものとする。	デジタル安全保護系のデジタル計算機（原子炉停止系，工学的安全施設作動系，及び重要度と複雑さがこれらと同程度の安全保護装置のその他の機器（例えば，BWRにおける核計装・放射線モニタ）に適用される電子計算機をいう。以下同じ。）に装荷するソフトウェア（ハードウェアと直接結びついて計算機の基本動作のみを制御するソフトウェアを除く。以下単に「ソフトウェア」という。）に対しては，V&Vを実施して，安全保護上要求される機能が正しく実現されていることを確認する。 ソフトウェアに関するV&Vは以下の4.1～4.3に示す手法によるものとする。なお，V&Vの対象である設計・製作作業の各ステップの内容を以下に示す。 (1)システム設計要求仕様作成 JEAC4620等のデジタル安全保護系に対する要求事項を基にシステムとしての全体設計を行い，要求仕様を明確に定める。 (2)ハードウェア・ソフトウェア設計要求仕様作成 システム設計要求仕様を基に，以下のハードウェア・ソフトウェア設計要求仕様を明確に定める。 ①ハードウェア・ソフトウェア統合要求仕様 ②ハードウェア設計要求仕様 ③ソフトウェア設計要求仕様 (3)ソフトウェア設計 ソフトウェア設計要求仕様を実現するためのソフトウェアを設計する。このときの設計上の配慮としては，検証を容易に行えるようソフトウェアの機能単位の分割等が望ましい。（例：ソフトウェアロジック図等） (4)ソフトウェア製作 ソフトウェア設計で明らかにされたソフトウェア機能を，デジタル計算機で実現するためのプログラムを作成する。 (5)ハードウェア設計・製作 ハードウェアの機能及び性能をハードウェア設計要求仕様に基づいて明らかにし，ハードウェア

		システムを設計，製作する。(例：盤内配線図等) (6)ハードウェア・ソフトウェア統合 ハードウェアにソフトウェアを装荷し，システムとして組みあげる。
4．2 V&V の実施	ディジタル安全保護系に対しては，設計，製作及び試験の各ステップにおいて，図１に示される V&V 作業を実施する。 V&V 活動は，以下の各項目に従って実施する。 (1)V&V の手順及び内容 検証作業は，図１に示された，設計･製作作業の各ステップにて実施する。妥当性確認作業は，試験プロセスにおいて，必要な検証を経て製作された全体システムに対して行う。V&V では，以下(a)～(g)の各作業を実施する。 (a)V&V 基本計画作成 V&V 作業の開始に当たり，ディジタル安全保護系に対する要求事項及びシステム設計要求仕様に基づき V&V 基本計画を作成する。この基本計画は，以下に示す V&V の各作業，体制及び文書管理について規定する。 ソフトウェアを再利用する場合には，その範囲に応じた V&V の各作業方法等について規定する。 (b)システム設計要求仕様検証（検証 1） 本検証では，JEAC4620 等のディジタル安全保護系に対する要求事項が正しくシステム設計要求仕様に反映されていることを検証する。 (c)ハードウェア・ソフトウェア設計要求仕様検証（検証 2） 本検証では，システム設計要求仕様が正しくハードウェア･ソフトウェア設計要求仕様に反映されていることを検証する。 (d)ソフトウェア設計検証（検証 3） 本検証では，ソフトウェア設計どおりに正しくソフトウェアが製作されていることを検証する。 (e)ソフトウェア製作検証（検証	デジタル安全保護系に対しては，設計，製作及び試験の各ステップにおいて，V&V 作業を実施する。 V&V 活動は，以下の各項目に従って実施する。 (1)V&V の手順及び内容 検証作業は，設計・製作作業の各ステップにて実施する。妥当性確認作業は，試験プロセスにおいて，必要な検証を経て製作された全体システムに対して行う。V&V では，以下(a)～(g)の各作業を実施する。 (a)V&V 基本計画作成 V&V 作業の開始に当たり，デジタル安全保護系に対する要求事項及びシステム設計要求仕様に基づき V&V 基本計画を作成する。この基本計画は，以下に示す V&V の各作業，体制及び文書管理について規定する。 ソフトウェアを再利用する場合には，その範囲に応じた V&V の各作業方法等について規定する。 (b)システム設計要求仕様検証（検証 1） 本検証では，JEAC4620 等のデジタル安全保護系に対する要求事項が正しくシステム設計要求仕様に反映されていることを検証する。 (c)ハードウェア・ソフトウェア設計要求仕様検証（検証 2） 本検証では，システム設計要求仕様が正しくハードウェア･ソフトウェア設計要求仕様に反映されていることを検証する。 (d)ソフトウェア設計検証（検証 3） 本検証では，ソフトウェア設計要求仕様が正しくソフトウェア設計に反映されていることを検証

	4) 本検証では，ソフトウェア設計どおりに正しくソフトウェアが製作されていることを検証する。 (f)ハードウェア・ソフトウェア統合検証（検証 5） 本検証では，ハードウェアとソフトウェアを統合してハードウェア・ソフトウェア設計要求仕様どおりのシステムとなっていることを検証する。 (g)妥当性確認 妥当性確認では，ハードウェアとソフトウェアを統合して検証されたシステムが，JEAC4620 等のディジタル安全保護系に対する要求事項を満たしていることを確認する。 (2)体制 ソフトウェアの設計，製作及び試験に対する V&V を実施する体制は，V&V 基本計画作成時に決定される。また，以下に示すとおり，V&V 作業は，設計・製作及び試験に携わった組織から独立した者が行う。 (a)V&V を実施する個人又はグループは，原設計に携わった者以外の個人又はグループとし，V&V を実施する力量を有することを組織が認めた者とする。 (b)V&V を実施する個人又はグループは，設計，製作及び試験に携わった組織から経済面，工程管理に関する制約を受けないものとする。 (3)文書管理 V&V を実施する上で以下の文書化を行う。 (a)設計，製作作業の文書化 図 1 に示されるステップごとに必要な設計，製作に関わる内容を明確にし，文書化する。 (b)V&V の文書化 V&V 作業の開始に当たり，V&V 基本計画を文書として作成する。また，V&V の各作業実施に当たっては 4.2(1)の内容を明確にし，作業内容，合格基準，不良結果等に対する措置の文書化を行い，作業ごとに結果を文書化する。	する。 (e)ソフトウェア製作検証（検証 4） 本検証では，ソフトウェア設計どおりに正しくソフトウェアが製作されていることを検証する。 (f)ハードウェア・ソフトウェア統合検証（検証 5） 本検証では，ハードウェアとソフトウェアを統合してハードウェア・ソフトウェア設計要求仕様どおりのシステムとなっていることを検証する。 (g)妥当性確認 妥当性確認では，ハードウェアとソフトウェアを統合して検証されたシステムが，JEAC4620 等のデジタル安全保護系に対する要求事項を満たしていることを確認する。 (2)体制 ソフトウェアの設計，製作及び試験に対する V&V を実施する体制は，V&V 基本計画作成時に決定される。また，以下に示すとおり，V&V 作業は，設計・製作及び試験に携わった組織から独立した者が行う。 (a)V&V を実施する個人又はグループは，原設計に携わった者以外の個人又はグループとし，V&V を実施する力量を有することを組織が認めた者とする。 (b)V&V を実施する個人又はグループは，設計，製作及び試験に携わった組織から経済面，工程管理に関する制約を受けないものとする。 (3)文書管理 V&V を実施する上で以下の文書化を行う。 (a)設計，製作作業の文書化 各ステップごとに必要な設計，製作に関わる内容を明確にし，文書化する。 (b)V&V の文書化 V&V 作業の開始に当たり，V&V 基本計画を文書として作成する。また，V&V の各作業実施に当たっては 4.2(1)の内容を明確にし，作

	(4) ソフトウェアツールの管理 ソフトウェアツールを使用する際には，目的に応じて適切に品質管理されたツールを使用する。 なお，ソフトウェアツールとは，以下をいう。 ・ソフトウェアを設計，製作及び試験する上で使用するツール（コンパイラ等） ・V&V を実施する上で使用するツール	業内容，合格基準，不良結果等に対する措置の文書化を行い，作業ごとに結果を文書化する。 (4) ソフトウェアツールの管理 ソフトウェアツールを使用する際には，目的に応じて適切に品質管理されたツールを使用する。 ソフトウェアツールの品質の確保とは，「原子力施設の保安のための業務に係る品質管理に必要な体制の基準に関する規則」が求める保安活動の結果として確保することである。 なお，ソフトウェアツールとは，以下をいう。 ・ソフトウェアを設計，製作及び試験する上で使用するツール（コンパイラ等） ・V&V を実施する上で使用するツール

・ 「(解説-3) 適用範囲（概念図)」は適用除外とする。
・ 「3.1 ディジタル計算機」は適用除外とする。
・ 上記表２に掲げていない項目において「ディジタル」は「デジタル」に読み替える。

表３　デジタル安全保護系規程 2008

4. ディジタル安全保護系に対する要求事項	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。 そのため，ディジタル安全保護系は，以下の要求事項を満足すること。	デ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。 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。 そのため，デジタル安全保護系は，以下の要求事項を満足すること。
4.1 過渡時，事故時及び地震時の機能	ディジタル安全保護系は，運転時の異常な過渡変化時，事故時及び地震の発生により原子炉の運転に支障が生じる場合において，原子炉停止系及び必要な工学的安全施設の作動を自動的に開始させる機能を果たす設計とすること。	デジタル安全保護系は，運転時の異常な過渡変化時，事故時及び地震の発生により原子炉の運転に支障が生じる場合において，原子炉停止系及び必要な工学的安全施設の作動を自動的に開始させる機能を果たす設計とすること。 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。
4.2 精度・応答時間	ディジタル安全保護系は，安全保護上必要な精度，応答時間（リアルタイム性能を含む）を計算機システムと関連ハードウェア部を合わせた全体システムとして満足する設計とすること。	デジタル安全保護系は，安全保護上必要な精度，応答時間（リアルタイム性能を含む）を計算機システムと関連ハードウェア部を合わせた全体システムとして満足する設計とすること。 リアルタイム性能とは，プロセス信号のサンプリング周期及び処理速度が，プロセスの変化速度に十分追従できる能力のことを言い，応答時間にはサンプリング周期及び処理速度を含めるものとする。
4.4 独立性	ディジタル安全保護系は，一つのチャンネルの故障によって安全保護機能が喪失しないようにチャンネル相互を電気的，物理的に分離し，チャンネル間の独立性を有する設計とすること。	デジタル安全保護系は，一つのチャンネルの故障によって安全保護機能が喪失しないようにチャンネル相互を電気的，物理的に分離し，チャンネル間の独立性を有する設計とすること。 多重化されたチャンネル間の通信の機能的分離は具体的には以下を考慮する。 ・多重化されたチャンネル間の通信は，原則として一方通行の通信路を介して情報伝達を行う。双方向通信が可能な通信路を介して情報伝達を行う場合には，発信側のシステムと受信側のシステム間の調整あるいは接続の失敗等によって，どちらのシステムも機能的に異常をきたさない設計とする。 ・通信接続の制御は，受信側の異常が発信側に影響しない設計とする。
4.5 計測制御系との分離	ディジタル安全保護系と計測制御系とを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，ディジタル安全保護系と計測制御系を電気的に分離する設計とすること。更に，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。	デジタル安全保護系と計測制御系とを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ジタル安全保護系に影響のないよう，デジタル安全保護系と計測制御系を電気的に分離する設計とすること。更に，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。 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。試験時に，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よう措置を講ずること。 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。 デジタル安全保護系と計測制御系とを部分的に共用する場合には，以下のように設計することにより，電気的に分離することができる。 ・安全保護系と計測制御系との信号取り合いは，光／電気変換などのアイソレーションデバイスを用いて電気的に分離する。
4.8 環境条件	ディジタル安全保護系は，期待される安全機能に応じて必要な耐震性，耐サージ性を有するとともに，火災防護上の措置，設置される場所における予想温度，湿度，放射線量，想定される電源擾乱，電磁波等の外部からの外乱・ノイズの環境条件を考慮した設計とすること。	デジタル安全保護系は，期待される安全機能に応じて必要な耐震性，耐サージ性を有するとともに，火災防護上の措置，設置される場所における予想温度，湿度，放射線量，想定される電源擾乱，サージ電圧，電磁波等の外部からの外乱・ノイズの環境条件を考慮して設計し，その設計による対策の妥当性が十分であることを確証すること。
4.15 自己診断機能	ディジタル安全保護系は，各チャンネル独立に適切な周期で実施される自己診断機能を有する設計とすること。 また，自己診断機能によりディジタル計算機の異常を検知した場合には，ディジタル計算機の異常を運転員へ告知する設計とすること。	デジタル安全保護系は，各チャンネル独立に適切な周期で実施される自己診断機能を有する設計とすること。 また，自己診断機能によりデジタル計算機の異常を検知した場合には，デジタル計算機の異常を運転員へ告知する設計とすること。 自己診断機能は，故障を早期発見することができるため，従来のアナログの安全保護系でも実施されている故障進展後の警報及び定期的な試験による健全性確認に加えて，システムの信頼性を更に向上させるのに有効な一手段である。自己診断機能によりデジタル計算機の異常が検出された場合には，運転員が適切な措置をとれるよう，警報等により運転員

		へ告知する。更に，自動で，当該チャンネルを動作状態又はバイパス状態にすることもある。 自己診断の例として，ウォッチドッグタイマ，パリティチェック，送受信信号の誤り検出，ソフトウェアによるチェック等がある。
4.16 外部ネットワークとの遮断	ディジタル安全保護系は，外部ネットワークと遮断することにより外部からの影響を防止し得る設計とすること。	デジタル安全保護系は，外部ネットワークと遮断することにより外部影響の防止された設備とすること。
4.17 ソフトウェアの管理外の変更に対する防護措置	ディジタル安全保護系に装荷するソフトウェアは，管理外の変更に対して適切な防護措置を講じ得る設計とすること。	デジタル安全保護系に装荷するソフトウェアは，管理外の変更に対して適切な防護措置を講じ得る設計とすること。 管理外の変更とは，故意による変更など，承認されていない変更のことをいう。 ソフトウェアの管理外の変更に対する防護措置の例としては，以下がある。 (1) ソフトウェアの不揮発化 (2) 鍵付きスイッチの設置 (3) パスワードの登録
4.18 品質管理	安全保護系に用いられるディジタル計算機は，以下の手法によりソフトウェアの健全性を確保すること。 ・ソフトウェアライフサイクル及び構成管理手法を含めた，品質保証活動 ・検証及び妥当性確認活動	安全保護系に用いられるデジタル計算機は，以下の手法によりソフトウェアの健全性を確保すること。 ・ソフトウェアライフサイクル及び構成管理手法を含めた，品質保証活動 ・検証及び妥当性確認活動 市販デジタル計算機，既存開発ソフトウェア又はソフトウェアツールを使用する場合には，目的に応じて適切に品質が確保され，ソフトウェア実行時に，他のソフトウェアに欠陥を招かないよう考慮する。 なお，ソフトウェアの品質を高めるために以下の手法を用いることがある。 ・処理構造の簡素化（定周期・シングルタスク構成等） ・適切な使用言語の適用による処理内容の明確化（可視化言語の適用，ツールによる可視化等） ・ソフトウェア品質保証指標による品質管理（品質指標の例：正確さ，完全性，要求の遵守，

		性能履歴等)
4.18.1 ソフトウェアライフサイクル	ディジタル安全保護系のソフトウェアに対して，ライフサイクルを通じて品質の管理方法を予め定め，実施するとともに，これを文書化すること。	デジタル安全保護系のソフトウェアに対して，ライフサイクルを通じて品質の管理方法を予め定め，実施するとともに，これを文書化すること。 デジタル安全保護系のソフトウェアの品質を確保するために，ソフトウェアに対してライフサイクルプロセスの考えを基にプロセスごとの管理を実施する。 (1) ライフサイクルプロセス デジタル安全保護系に装荷されるソフトウェアに対しては，各プロジェクトのプロセスを定義し，文書化する。プロセスには，設計，製作，試験，装荷，運転，変更及び廃止がある。 以下に各プロセスの内容を示す。 設計プロセス：製品に対するシステムの要求事項からソフトウェア設計仕様を作成するプロセス。 製作プロセス：ソフトウェア設計仕様よりソフトウェアを製作するプロセス。 試験プロセス：製作されたソフトウェアに対して試験を実施するプロセス。ソフトウェア単体に対して行う試験とハードウェアと一体となったシステムとして行う試験がある。 装荷プロセス：実機の最終システムへソフトウェアを実装するプロセス。 運転プロセス：システムを運転しているプロセス。 変更プロセス：仕様変更等によりソフトウェアを変更するプロセス。 廃止プロセス：ソフトウェアを使用不可能とするプロセス。 ソフトウェアライフサイクルプロセスには，以下の理由により，開発及び保守プロセスを定義していない。 (2) 各プロセスで実施すべき品質管理項目 各プロセスで実施すべき品質管理項目に対して計画を作成し，その計画に従って実施した結果を文書化する。

		なお，計画はプロジェクトの開始段階で一括して作成することでもよい。以下に各プロセスで実施すべき品質管理項目の例を示す。 1）設計プロセス ソフトウェアに対する仕様を決定する。 また，検証手段を決定する。 2）製作プロセス 仕様のとおりソフトウェアが製作されていることを確認する。 3）試験プロセス 要求仕様を確認するための試験方案を作成し，判定基準内にあることを確認する。試験にはソフトウェア単体で行うものとシステムとして行うものがあり，ソフトウェア単体では確認できない内容はシステムとして確認することでよい。 4）装荷プロセス 管理されたソフトウェアが正しく実機に実装されることを確認する。ソフトウェアのコンペア等を用いて確認する。 5）運転プロセス 運転中はシステムに異常が無いことを確認する。 6）変更プロセス ソフトウェアの変更要否について調査する。 ソフトウェアに変更が生じる場合には，変更仕様を決定し変更を実施する。実施内容は設計・製作及び試験におけるそれぞれのプロセスに従う。 7）廃止プロセス 廃止することを宣言する。代替手段がある場合にはこれを含むものとする。
4.18.2 ソフトウェア構成管理	ディジタル安全保護系のソフトウェアに対して，構成管理手法を予め定め，実施するとともに，構成管理計画として文書化すること。また，ソフトウェアを構成する管理対象項目は，ソフトウェア構成管理計画に基づき，すべてが文書化されること。	デジタル安全保護系のソフトウェアに対して，構成管理手法を予め定め，実施するとともに，構成管理計画として文書化すること。 また，ソフトウェアを構成する管理対象項目は，ソフトウェア構成管理計画に基づき，すべてを文書化すること。 構成管理とは，管理対象要素の特定・識別と，要素の管理方法，及びソフトウェア供給者に対する

		監査あるいは審査方法を予め定め，計画に基づき，実施することである。 具体的には以下に示す。 (1) ソフトウェア及び関連文書を特定し，相互に識別するために，予め構成管理計画を策定し，実行する。 (2) 構成管理計画で，以下の内容を定める。 ①ソフトウェア及び関連文書について，管理対象要素を定める。管理対象要素の例としては以下がある。 ・要求仕様 ・設計仕様 ・製作仕様 ・試験仕様／試験結果 ・検証手順／検証結果 ・取扱説明 ・製作したソフトウェア ②管理対象要素の管理手法を定める。管理する項目の例としては以下がある。 ・改訂番号，改訂日付 ・変更要求有無，他の管理対象要素との整合状況などの状態 ・他の管理対象要素との取り合い ③ソフトウェアの変更手法を定める。 ④ソフトウェア供給者への監査あるいは審査方法を定める。 ⑤以上の項目を実施するための体制を定める。
4.18.3 検証及び妥当性確認	ディジタル安全保護系は，設計，製作，試験，変更のソフトウェアライフサイクルのプロセスで検証及び妥当性確認を実施すること。 (1) 検証及び妥当性確認は，技術及び管理において設計，製作及び試験を行う組織と独立した組織が実施すること。 (2) 検証及び妥当性確認を実施する上で適切な文書化が行われていること。 (3) ソフトウェアの再利用時においては，既存設計での検証結果による代替を可能とする前提として再利用範囲が明確に識別さ	デジタル安全保護系は，設計，製作，試験，変更のソフトウェアライフサイクルのプロセスで検証及び妥当性確認を実施すること。 (1) 検証及び妥当性確認は，技術及び管理において設計，製作及び試験を行う組織と独立した組織が実施すること。検証及び妥当性確認の実施体制の独立性とは下記をいう。 (a)ソフトウェアの設計，製作及び試験に対する検証及び妥当性確認を実施する人間又はグループは，原設計に携わった人間以外の人間又はグループであること。 (b)検証及び妥当性確認の実施を

	れ，再利用の妥当性を示す根拠が文書化されていること。	管理する組織は，設計，製作，試験及び工程管理に携わった組織以外の組織であること。 (2) 検証及び妥当性確認を実施する上で適切な文書化が行われていること。検証及び妥当性確認の実施に際して作成された文書は，4.18.2 の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。検証及び妥当性確認の合格基準及び不良結果等に対する措置を決定し文書化すること。 (3) ソフトウェアの再利用時においては，既存設計での検証結果による代替を可能とする前提として再利用範囲が明確に識別され，再利用の妥当性を示す根拠が文書化されていること。

・ 上記表３に掲げていない項目において「ディジタル」は「デジタル」に読み替える。

表４　デジタル安全保護系 V&V 指針 2008

4．2 検証及び妥当性確認の実施	ディジタル安全保護系に対しては，設計・製作・試験の各段階において，図１に示される検証及び妥当性確認作業を実施する。 (図１は略) 検証及び妥当性確認活動は，以下の各項目に従って実施する。 (1) 検証及び妥当性確認の手順及び内容 検証作業は，図１に示された，設計・製作の各プロセスにて実施する。妥当性確認は，試験プロセスにおいて，必要な検証を経て製作された全体システムに対して行う。検証及び妥当性確認では，下記(a)～(g)の各作業を実施する。 (a) 検証・妥当性確認基本計画作成 検証・妥当性確認作業の開始に当たり，ディジタル安全保護系システム要求事項及びシステム設計要求仕様に基づき検証・妥当性確認基本計画を作成する。この基本計画は，以下に示す検証及び妥当性確認の各作業，体制及び文書管理について規定する。 また，ソフトウェアを再利用する場合には，その範囲に応じた検証及び妥当性確認の各作業方法等	デジタル安全保護系に対しては，設計・製作・試験の各段階において，検証及び妥当性確認作業を実施する。 検証及び妥当性確認活動は，以下の各項目に従って実施する。 (1)検証及び妥当性確認の手順及び内容 検証作業は，設計・製作の各プロセスにて実施する。妥当性確認は，試験プロセスにおいて，必要な検証を経て製作された全体システムに対して行う。検証及び妥当性確認では，下記(a)～(g)の各作業を実施する。 (a)検証・妥当性確認基本計画作成 検証・妥当性確認作業の開始に当たり，デジタル安全保護系システム要求事項及びシステム設計要求仕様に基づき検証・妥当性確認基本計画を作成する。この基本計画は，以下に示す検証及び妥当性確認の各作業，体制及び文書管理について規定する。 また，ソフトウェアを再利用する場合には，その範囲に応じた検証及び妥当性確認の各作業方法等

	について規定する。 (b) システム設計要求仕様検証（検証 1） 本検証では，JEAC 4620 のディジタル安全保護系システム要求事項が正しくシステム設計要求仕様に反映されていることを検証する。 (c)ハードウェア・ソフトウェア設計要求仕様検証（検証 2） 本検証では，システム設計要求仕様が正しくハードウェア・ソフトウェア設計要求仕様に反映されていることを検証する。 (d) ソフトウェア設計検証（検証 3） 本検証では，ソフトウェア設計要求仕様が正しくソフトウェア設計に反映されていることを検証する。 (e)　ソフトウェア製作検証（検証 4） 本検証では，ソフトウェア設計通りに正しくソフトウェアが製作されていることを検証する。 (f)ハードウェア・ソフトウェア統合検証（検証 5） 本検証では，ハードウェアとソフトウェアを統合してハードウェア・ソフトウェア設計要求仕様通りのシステムとなっていることを検証する。 (g)妥当性確認 妥当性確認では，ハードウェアとソフトウェアを統合して検証されたシステムが，JEAC 4620 のディジタル安全保護系システム要求事項を満たしていることを確認する。 (2)体制 検証及び妥当性確認を実施する体制は，検証・妥当性確認基本計画作成作業時に決定されるべきである。 また，以下に示すとおり，設計・製作作業とその検証及び妥当性確認作業は，別の人間が行う。 (a)ソフトウェアの設計，製作及び試験に対する検証及び妥当性確認を実施する人間又はグループは，原設計に携わった人間以外	について規定する。 (b) システム設計要求仕様検証（検証 1） 本検証では，JEAC 4620 のデジタル安全保護系システム要求事項が正しくシステム設計要求仕様に反映されていることを検証する。 (c)ハードウェア・ソフトウェア設計要求仕様検証（検証 2） 本検証では，システム設計要求仕様が正しくハードウェア・ソフトウェア設計要求仕様に反映されていることを検証する。 (d) ソフトウェア設計検証（検証 3） 本検証では，ソフトウェア設計要求仕様が正しくソフトウェア設計に反映されていることを検証する。 (e) ソフトウェア製作検証（検証 4） 本検証では，ソフトウェア設計通りに正しくソフトウェアが製作されていることを検証する。 (f)ハードウェア・ソフトウェア統合検証（検証 5） 本検証では，ハードウェアとソフトウェアを統合してハードウェア・ソフトウェア設計要求仕様通りのシステムとなっていることを検証する。 (g)妥当性確認 妥当性確認では，ハードウェアとソフトウェアを統合して検証されたシステムが，JEAC 4620 のデジタル安全保護系システム要求事項を満たしていることを確認する。 (2)体制 検証及び妥当性確認を実施する体制は，検証・妥当性確認基本計画作成作業時に決定されるべきである。 また，以下に示すとおり，設計・製作作業とその検証及び妥当性確認作業は，別の人間が行う。 (a)ソフトウェアの設計，製作及び試験に対する検証及び妥当性確認を実施する人間又はグループは，原設計に携わった人間以外

	の人間又はグループであること。 (b)検証及び妥当性確認の実施を管理する組織は，設計，製作，試験及び工程管理に携わった組織以外の組織であること。この組織は，管理面で独立していれば同一部署内でも構わない。(解説-8) なお，設計・製作者はシステム設計要求仕様の作成，ハードウェア・ソフトウェア設計要求仕様の作成，ソフトウェア設計，ソフトウェア製作，ハードウェア・ソフトウェア統合の各作業を行い，検証者は検証・妥当性確認基本計画立案，システム設計要求仕様検証，ハードウェア・ソフトウェア設計要求検証，ソフトウェア設計検証，ソフトウェア製作検証，ハードウェア・ソフトウェア統合検証及び妥当性確認の各作業を行う。 (3)文書管理 検証及び妥当性確認を実施する上で以下の文書化を行う。 (a)設計の文書化 図１に示される各ステップごとに必要な設計・製作に係わる内容を明確にし文書化する。 (b)　検証及び妥当性確認作業の文書化 検証及び妥当性確認作業の開始に当たり，検証・妥当性確認基本計画を文書として作成する。 また，検証及び妥当性確認の各作業実施に当たっては 4.2(1)の内容を明確にし，作業内容，合格基準及び不良結果等に対する措置の文書化を行い，各作業ごとに結果を文書化する。 (4)　ソフトウェアツールの管理 ソフトウェアツールを使用する際には，目的に応じて適切に品質管理されたツールを使用する。 なお，ソフトウェアツールとは，以下をいう。 ・ソフトウェアを設計・製作・試験する上で使用するツール(コンパイラ等) ・検証及び妥当性確認を実施する上で使用するツール	の人間又はグループであること。 (b)検証及び妥当性確認の実施を管理する組織は，設計，製作，試験及び工程管理に携わった組織以外の組織であること。この組織は，管理面で独立していれば同一部署内でも構わない。 なお，設計・製作者はシステム設計要求仕様の作成，ハードウェア・ソフトウェア設計要求仕様の作成，ソフトウェア設計，ソフトウェア製作，ハードウェア・ソフトウェア統合の各作業を行い，検証者は検証・妥当性確認基本計画立案，システム設計要求仕様検証，ハードウェア・ソフトウェア設計要求検証，ソフトウェア設計検証，ソフトウェア製作検証，ハードウェア・ソフトウェア統合検証及び妥当性確認の各作業を行う。 (3)文書管理 検証及び妥当性確認を実施する上で以下の文書化を行う。 (a)設計の文書化 ステップごとに必要な設計・製作に係わる内容を明確にし文書化する。 (b)検証及び妥当性確認作業の文書化 検証及び妥当性確認作業の開始に当たり，検証・妥当性確認基本計画を文書として作成する。 また，検証及び妥当性確認の各作業実施に当たっては 4.2(1)の内容を明確にし，作業内容，合格基準及び不良結果等に対する措置の文書化を行い，各作業ごとに結果を文書化する。 (4)ソフトウェアツールの管理 ソフトウェアツールを使用する際には，目的に応じて適切に品質管理されたツールを使用する。 なお，ソフトウェアツールとは，以下をいう。 ・ソフトウェアを設計・製作・試験する上で使用するツール(コンパイラ等) ・検証及び妥当性確認を実施する上で使用するツール

・ 上記表４に掲げていない項目において「ディジタル」は「デジタル」に読み替える。

別表１－１　技術基準規則の規定とデジタル安全保護系規程2020及びデジタル安全保護系V&V指針2020の規定との対応関係

注記
対応規格箇条は、原則として第１階層の箇条で分類。最下位の箇条まで適用される。

技術基準規則	規格
（安全保護装置） 第三十五条 発電用原子炉施設には、安全保護装置を次に定めるところにより施設しなければならない。 一 運転時の異常な過渡変化が発生する場合又は地震の発生により発電用原子炉の運転に支障が生ずる場合において、原子炉停止系統その他系統と併せて機能することにより、燃料要素の許容損傷限界を超えないようにできるものであること。 二 系統を構成する機械若しくは器具又はチャンネルは、単一故障が起きた場合又は使用状態からの単一の取り外しを行った場合において、安全保護機能を失わないよう、多重性を確保すること。 三 系統を構成するチャンネルは、それぞれ互いに分離し、それぞれのチャンネル間において安全保護機能を失わないように独立性を確保すること。 四 駆動源の喪失、系統の遮断その他の不利な状況が生じた場合においても、発電用原子炉施設をより安全な状態に移行するか、又は当該状態を維持することにより、発電用原子炉施設の安全上支障がない状態を維持できること。 五 不正アクセス行為その他の電子計算機に使用目的に沿うべき動作をさせず、又は使用目的に反する動作をさせる行為による被害を防止するために必要な措置が講じられているものであること。 六 計測制御系の一部を安全保護装置と共用する場合には、その安全保護機能を失わないよう、計測制御系から機能的に分離されたものであること。 七 発電用原子炉の運転中に、その能力を確認するための必要な試験ができるものであること。 八 運転条件に応じて作動設定値を変更できるものであること。	デジタル安全保護系規程2020 4. デジタル安全保護系V&V指針2020 4. 5.

別表１－２　技術基準規則の規定とデジタル安全保護系規程 2008 及びデジタル安全保護系 V&V 指針 2008 の規定との対応関係

注記
対応規格箇条は、原則として第１階層の箇条で分類。最下位の箇条まで適用される。

技術基準規則	規格
（安全保護装置） 第三十五条 発電用原子炉施設には、安全保護装置を次に定めるところにより施設しなければならない。 一 運転時の異常な過渡変化が発生する場合又は地震の発生により発電用原子炉の運転に支障が生ずる場合において、原子炉停止系統その他系統と併せて機能することにより、燃料要素の許容損傷限界を	デジタル安全保護系規程 2008 4. デジタル安全保護系 V&V 指針

超えないようにできるものであること。 二 系統を構成する機械若しくは器具又はチャンネルは、単一故障が起きた場合又は使用状態からの単一の取り外しを行った場合において、安全保護機能を失わないよう、多重性を確保すること。 三 系統を構成するチャンネルは、それぞれ互いに分離し、それぞれのチャンネル間において安全保護機能を失わないように独立性を確保すること。 四 駆動源の喪失、系統の遮断その他の不利な状況が生じた場合においても、発電用原子炉施設をより安全な状態に移行するか、又は当該状態を維持することにより、発電用原子炉施設の安全上支障がない状態を維持できること。 五 不正アクセス行為その他の電子計算機に使用目的に沿うべき動作をさせず、又は使用目的に反する動作をさせる行為による被害を防止するために必要な措置が講じられているものであること。 六 計測制御系の一部を安全保護装置と共用する場合には、その安全保護機能を失わないよう、計測制御系から機能的に分離されたものであること。 七 発電用原子炉の運転中に、その能力を確認するための必要な試験ができるものであること。 八 運転条件に応じて作動設定値を変更できるものであること。	2008 4. 5.