資料４－２

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）並びに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（案）

目次

１．はじめに

「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」（平成２５年原子力規制委員会規則第６号。以下「技術基準規則」という。）は、実用発電用原子炉及びその附属施設が満たすべき技術基準を機能要求又は性能水準要求として規定しており、これを満たす具体的仕様として「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」（平成２５年６月１９日　原規技発第 1306194 号。以下「技術基準規則解釈」という。）において、技術評価した民間規格を引用している。

原子力規制委員会は、平成３０年に民間規格の活用について見直しを行い「原子力規制委員会における民間規格の活用について」（平成３０年６月６日　原子力規制委員会）としてとりまとめている。この中で、技術評価は、３学協会[1]の意見を参考に規則解釈等の改訂が必要となるものの存否を原子力規制庁において検討し、被規制者から意見（技術評価を希望する３学協会規格）を聴取することとされた。

これを踏まえ、令和３年に公開の会合[2]において、被規制者から技術評価を希望する３学協会規格を、３学協会から技術評価を行うに際しての参考意見を聴取するとともに、規制執行部局の意向を確認した結果、令和３年度の技術評価の対象として、「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。）並びに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）」（以下「デジタル安全保護系 V&V 指針 2020」という。）を選定し、これらの技術評価を行うことについて原子力規制委員会の了承を得た[3]。

本書は、原子力規制委員会が上記規格の技術評価について取りまとめたものである。

２．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 の技術評価に当たって

２．１　技術評価における視点

「原子力規制委員会における民間規格の活用について」（平成３０年６月６日原子力規制委員会）及び「民間規格の技術評価の実施に係る計画」（令和３年５月１２日原子力規制委員会）を踏まえ、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 の技術評価を、以下の点を確認すること等により実施する。

①　技術基準規則やその他の法令又はそれに基づく文書で要求される性能との項目及び範囲において対応していること。

②　技術基準規則で要求される性能を達成するための必要な技術的事項について、具体的な手法や仕様が示されていること。その他の法令又は法令に基づく文書で要求される事項を達成するための必要な技術的事項については、具体的な手法、仕様、方法及び活動が示されていること。

③　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 に示される具体的な手法、仕様、方法及び活動について、その技術的妥当性が証明あるいはその根拠が記載されていること。なお、海外規格がデジタル安全保護系規程 2020 及びデ

[1] 日本原子力学会、日本電気協会及び日本機械学会
[2] 第１５回新規制要件に関する事業者意見の聴取に係る会合（令和３年１月２２日）
[3] 令和３年度第７回原子力規制委員会（令和３年５月１２日）

ジタル安全保護系V&V指針2020に取り込まれたものについては、上記の条件に加え、海外規格との相違点（変更点）及び我が国の規制基準で要求する性能との関係も検討する。

④　規制当局が過去に追加要件を課している事項については、技術の進歩、運転等における経験などの知見を考慮し、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への反映が行われていること。

２．２　技術評価の範囲と手順

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の技術評価は以下に示す範囲と手順により行う。

①　技術評価は、既に「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」（以下「技術基準規則解釈」という。）に引用されている「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。）からデジタル安全保護系規程2020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）」（以下「デジタル安全保護系V&V指針2008」という。）からデジタル安全保護系V&V指針2020への変更点を対象とする。なお、過去に技術評価されたものであっても最新知見の蓄積や技術の進歩等により再度確認が必要と判断した場合には、再評価を行う。

②　解説は、原則として技術評価の対象外であるが、記載内容を精査し、規格本文における規定内容の技術基準規則への充足性に関係する場合には、技術評価の対象とする。

③　検討に当たっては、原子力規制委員会委員及び原子力規制庁職員から構成される「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」（備考参照）を設置して検討を行い、技術評価を行う。

（備考）

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構成員名簿

原子力規制委員会

田中 知	原子力規制委員会委員

原子力規制庁

佐藤 暁	技術基盤グループ長
遠山 眞	技術基盤グループ 技術基盤課長
佐々木 晴子	技術基盤グループ 技術基盤課 企画調整官
今瀬 正博	技術基盤グループ 技術基盤課 原子力規制専門職
濱口 義兼	技術基盤グループ シビアアクシデント研究部門 主任技術研究調査官
瀧田 雅美	技術基盤グループ システム安全研究部門 安全技術専門職
酒井 宏隆	技術基盤グループ 核燃料廃棄物研究部門 上席技術研究調査官
皆川 武史	技術基盤グループ システム安全研究部門 技術研究調査官
藤澤 博美	技術参与

（令和４年１月２５日時点）

２．３　技術基準規則との対応

（１）　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 について

安全保護装置については、技術基準規則第 2 条第 2 項第 9 号にその定義が、第３５条にその性能要求が規定され、その具体的仕様の例示基準は、技術基準規則解釈で定めている。技術基準規則解釈は、第３５条第４号において「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。」と規定している。ここでの「本文」とは要求事項のことである。

技術基準規則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 については、「表 2.3-1 技術基準規則第３５条及び解釈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 との対応関係」に示すように、技術基準規則の要求事項と対応している。なお、同表では、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 で規定の内容が変更されている部分（技術的変更でない軽微な変更は除く。）に下線を付してある。

なお、技術評価は「性能規定化された規制要求に対する容認可能な実施方法」について行うものであることから、これに該当しない場合は「技術評価の対象外」とし、技術評価の結果、適用すべきでないと判断したものは「適用除外」としている。ただし、これは実施を妨げるものではなく、技術的根拠があれば個別に説明を行うことにより用いることができる。この考え方は、技術基準規則解釈の前文に次のように規定されている。

○　技術基準規則に定める技術的要件を満足する技術的内容は、本解釈に限定されるものではなく、技術基準規則に照らして十分な保安水準の確保が達成できる技術的根拠があれば、技術基準規則に適合するものと判断する。

表 2.3-1　技術基準規則及び解釈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階層の細分箇条で分類。上位の箇条（細分箇条でないもの）は適用される。

技術基準規則	技術基準規則解釈	規格
（定義） 第二条（略） ２　この規則において、次に掲げる用語の意義は、それぞれ当該各号に定めるところによる。 九　「安全設備」とは、設計基準事故時及び設計基準事故に至るまでの間に想定される環境条件において、その損壊又は故障その他の異常により公衆に放射線障害を及ぼすおそれを直接又は間接に生じさせる設備であって次に掲げるものをいう。 ハ　安全保護装置（運転時の異常な過渡変化が発生する場合、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及び一次冷却材喪失その他の設計基準事故時に原子炉停止系統を自動的に作動させ、かつ、発電用原子炉内の燃料体の破損又は発電用原子炉の炉心（以下単に「炉心」という。）の損傷による多量の放射性物質の放出のおそれがある場合に、工学的安全施設を自動的に作動させる装置をいう。以下同じ。）、非常用炉心冷却設備（原子炉圧力容器内において発生した熱を通常運転時において除去する発電用原子炉施設が設計基準事故時及び設計基準事故に至るまでの間にその機能を失った場合に原子炉圧力容器内において発生した熱を除去する設備をいう。以下同じ。）その他非常時に発電用原子炉の安全性を確保するた		

めに必要な設備及びそれらの附属設備 （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	第３５条（安全保護装置） １ 第１号の安全保護装置の機能の確認については、設置許可申請書の添付書類八の設備仕様及び設置許可申請書において評価した運転時の異常な過渡変化の評価の条件に非保守的な変更がないことを確認すること。 ２ 第３号に規定する「独立性を確保すること」とは、チャンネル間の距離、バリア、電気的隔離装置等により、相互を分離することをいう。 ３ 第５号に規定する「必要な措置が講じられているものであること」とは、外部ネットワークと物理的な分離又は機能的な分離を行うこと、有線又は無線による外部ネットワークからの遠隔操作及びウイルス等の侵入を防止すること、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及びウイルス等の侵入を防止すること等の措置を講ずることをいう。なお、ソフトウェアの内部管理を強化するために、ウイルス等によるシステムの異常動作を検出させる場合には以下の機能を有すること。 （１）ウイルス等によるシステムの異常動作を検出する機能を設ける場合には、ウイルス等を検知した場合に運転員等へ告知すること。 （２）ウイルス等によるシステムの異常動作を検出する機能は、安全保護装置の機能に悪影響を及ぼさないこと。 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-	デジタル安全保護系規程 2008 4.1 4.2 4.3 4.4 4.5 4.6 4.7 4.8 4.9 4.10 4.11 4.12 4.13 4.14 4.15 4.16 4.17 4.18 (解説-4) (解説-5) (解説-6) (解説-8) (解説-11) (解説-12) (解説-13) (解説-14) (解説-15) (解説-16)

こと。	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	(解説-17) (解説-18) デジタル安全保護系 V&V 指針 2008 4.1 4.2 4.3 5. (解説-9)

	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)	

３．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 の技術的妥当性の確認方法

３．１　規格の変更点

３．１．１　デジタル安全保護系規程 2020 のデジタル安全保護系規程 2008 からの変更点

デジタル安全保護系規程 2020 のデジタル安全保護系規程 2008 からの変更点（「添付資料－１　変更点一覧」 の「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 4620-2020 における同 JEAC 4620-2008 からの変更点一覧」参照）は 68 件あり、各々の変更点について、「表 3.1-1 変更点に関する分類」に基づいて整理した。

表 3.1-1 変更点に関する分類

根拠の分類		具体的内容
①	記載の適正化のための変更	・用語の統一 ・表現の明確化 ・題目の修正 ・条項番号の変更 ・単位換算の見直し ・記号の変更
②	関連規格の引用年版等の変更	・関連規格の年版改正の反映 ・新たな関連規格の反映
③	国内外の知見の反映等	・国内外における試験研究成果の反映等
④	技術評価の対象外	・技術評価の対象機器以外の機器に係る変更

３．１．２　デジタル安全保護系 V&V 指針 2020 のデジタル安全保護系 V&V 指針 2008 からの変更点

デジタル安全保護系 V&V 指針 2020 のデジタル安全保護系 V&V 指針 2008 からの変更点（「添付資料－１　変更点一覧」の「２．日本電気協会　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 における同 JEAG 4609-2008 からの変更点一覧」参照）は 23 件あり、各々の変更点について、「表 3.1-1　変更点に関する分類」の分類に基づいて整理した。

３．２　技術評価の対象となる規定の選定

デジタル安全保護系規程 2020 のデジタル安全保護系規程 2008 からの変更点（技術評価の対象となる「表 2.3-1　技術基準規則及び解釈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」に掲げる規定に関するもの）のうち、表 3.1-1 の①に分類される項目については、技術的要求事項の変更がないことを確認した。また、②に分類される項目の検討結果については３．２．１に、③に分類される項目の検討結果については４．１に示す。

同様に、デジタル安全保護系 V&V 指針 2020 のデジタル安全保護系 V&V 指針 2008 からの変更点（技術評価の対象となる「表 2.3-1　技術基準規則及び解釈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」に掲げる規定に関するもの）のうち、①に分類される項目については、技術的要求事項の変更がないこと

を確認し、②に分類される項目の検討結果については３．２．２に、③に分類される項目の検討結果については４．２に示す。

なお、過去に技術評価されたものであっても、最新知見の蓄積や技術の進歩等により再度評価の確認が必要と判断した場合には、当該部分を技術評価の対象とした。

３．２．１　デジタル安全保護系規程 2020

（１）　引用規格の引用年版等の変更

デジタル安全保護系規程 2008 から変更又は追加された引用規格を「添付資料－２　引用規格の変更に関する確認結果」の「１．デジタル安全保護系規程 2020 における関連規格のデジタル安全保護系規程 2008 からの変更に関する確認結果」に示す。年版を最新のものに変更したものは 5 件である。これらの変更内容のうち、「表 3.2.1-1　引用規格の年版等の変更に該当する事項」の 3 件名が技術評価の対象となることを確認した。

この技術評価については、次項で述べるデジタル安全保護系規程 2020 の国内外の知見の反映等に係る技術評価の結果と併せて評価を行う。

表 3.2.1-1　引用規格の年版等の変更に該当する事項

No	件名	主な変更内容	記載箇所
1	JEAC 4111-2013 原子力安全のためのマネジメントシステム規程 JEAG 4121-2015[2018 年追補版] 原子力安全のためのマネジメントシステム規程（JEAC 4111-2013）の適用指針	・「原子力発電所における安全のための品質保証規程」→「原子力安全のためのマネジメントシステム規程」と名称変更し、年版を 2003 年版→2013 年版に変更 ・「原子力発電所における安全のための品質保証規程（JEAC 4111-2003）の適用指針 －原子力発電所の運転段階－」→「原子力安全のためのマネジメントシステム規程（JEAC 4111-2013）の適用指針」と名称変更し、年版を 2005[2007 年追補版]→2015[2018 年追補版]に変更	（解説-18）品質保証活動
2	「原子力発電所耐震設計技術規程：JEAC4601-2015」	・「原子力発電所耐震設計技術指針[重要度分類・許容応力編]：JEAG4601・補-1984」から「原子力発電所耐震設計技術規程：JEAC4601-2015」に名称及び年版変更	（解説-10）外的要因（関連規格・指針）
3	JEAC 4626-2010 原子力発電所の火災防護規程 JEAG 4607-2010 原子力発電所の火災防護指針	・1999 年版から 2010 年版に変更	（解説-10）外的要因（関連規格・指針）

（２）　国内外の知見の反映等

デジタル安全保護系規程 2008 からデジタル安全保護系規程 2020 への変更点について、国内外の知見の反映等によると判断した事項及び変更点以外で確認を行った事項は「表 3.2.1-2　国内外の知見の反映等に該当する変更事項」に示すとおりであり、事項ごとに技術的妥当性を検討した。

表 3.2.1-2　国内外の知見の反映等に該当する変更事項

No.	件名	主な変更内容又は確認の内容	記載箇所
1	過渡時、事故時及び地震時の機能	・過渡時及び地震時の機能と事故時の機能に分割し、前者は「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」、後者は「異常な状態を検知し，原子炉停止系（原子炉の緊急停止機能）及び必要な工学的安全施設を自動的に作動させる設計」に明確化 ・用語の定義「3.1 ディジタル計算機」の範囲について確認 ・用語の定義「3.2 安全保護系」の範囲について確認 ・動作に失敗する確率及び誤動作率について再確認	4.1 過渡時及び地震時の機能 4.2 事故時の機能 3.1 ディジタル計算機 3.2 安全保護系 4. ディジタル安全保護系に対する要求事項
2	独立性の確保と試験可能性	・チャンネル間に通信を用いる場合の機能的分離を追加 ・多重化されたチャンネル間の通信の機能的分離の措置を考慮事項から例示事項に変更 ・多重化されたチャンネル間の通信を「通信接続の制御を受信側の異常が発信側に影響しない設計」から「ディ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」に変更 ・試験可能性の規定見直しについて確認	4.5 独立性 （解説-7）多重化されたチャンネル間の通信 4.8 試験可能性
3	故障時の機能要求、中央制御室の表示	・駆動源の喪失を安全保護系の駆動源喪失と明確化し、フェイルセーフの記載のほかにフェイルアズイズを追加 ・中央制御室に表示する動作原因について確認	4.7 故障時の機能 4.15 動作及びバイパスの表示
4	駆動源の喪失等に対する措置	・外部電源系が喪失した場合あるいは短時間の全交流動力電源喪失の場合でも安全保護機能を果たすことが可能なようにする規定を削除し、非常用所内電源系からの給電を明確化	4.10 非常用電源の使用
5	不正アクセス行為等の被害防止措置	・外部ネットワークとの遮断規定を削除し、不正アクセス行為等による被害を防止するために必要な措置を講じる設計とする規定を追加	4.18 不正アクセス行為等の被害の防止
6	計測制御系からの機能的分離	・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の措置を考慮事項から例示に変更し、計測制御系からの情報受け制限と試験時及び保守時の例外扱いを追加 ・アイソレーションデバイスは安全保護系に属する旨を追記 ・ディ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例示	（解説-8）計測制御系との分離

		を追加	
7	設定値の変更	・作動設定値を変更する必要がある場合に、手動による変更ができる設計から適切な変更が可能な設計に修正	4.11 設定値の変更
8	ライフサイクルを通じた品質の管理方法	・ソフトウェア単体では確認できない内容をシステムとして確認する範囲については、事前に計画することを規定 ・廃止されたソフトウェアの誤使用防止措置を講じる規定を追加	（解説-19）ソフトウェアライフサイクル
9	検証及び妥当性確認(V&V)と品質保証	・V&V を行う体制を「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」から「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」に変更 ・ディジタル安全保護系の供給者に対する品質保証活動を要求 ・V&V としての検証は設計プロセス及び製作プロセス、V&V としての妥当性確認は試験プロセスと明確化 ・V&V を実施する個人又はグループの力量及び経済面、工程管理に関する制約を受けないことを追加 ・V&V に係る文書は構成管理計画の中で保存及び管理を追加 ・品質保証について再確認	4.19.3 V&V （解説-21） V&V（手順） （解説-22） V&V（独立性） （解説-23） V&V（文書化） 4.19 品質保証 （解説-18）品質保証活動
10	ソフトウェアの構成管理	・構成管理の対象に V&V 手順及び V&V 結果を追加し、ソフトウェア供給者に対する監査又は審査をソフトウェア構成管理のレビュー又は審査に変更 ・ソフトウェア及び関連文書について、管理対象要素の例に「V&V 手順／V&V 結果」を追加	（解説-20）ソフトウェアの構成管理
11	環境条件の考慮	・溢水防護上の措置をその他の外的要因に追加し、当該規格として「原子力発電所の内部溢水影響評価ガイド:平成 25 年 6 月 19 日原子力規制委員会決定」を追加 ・外的要因に対する設計の確証規定を追加 ・耐サージ性に関する「原子力発電所の耐雷指針：JEAG4608-2007」を削除 ・「原子力発電所耐震設計技術指針[重要度分類・許容応力編]：JEAG4601・補-1984」から「原子力発電所耐震設計技術規程：JEAC4601-2015」に変更 ・火災防護の規格に「原子力発電所の火災防護規程：JEAC4626-2010」及び審査基準を追加	4.9 外的要因 （解説-10）外的要因（関連規格・指針）
12	健全性を実証できない場合の原理の	・「ディジタル安全保護系は，「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,共通要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考えられる」との記載を追加	5.留意事項

	異なる手段の設置	し、「ハードウェア設備」を「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」に変更 ・IEEE 規格、IEC 規格から本規程に反映した事項について確認	

３．２．２　デジタル安全保護系 V&V 指針 2020

（１）　引用規格の引用年版等の変更

デジタル安全保護系 V&V 指針 2008 から変更又は追加された引用規格を「添付資料－２ 引用規格の変更に関する確認結果」 の「２．デジタル安全保護系 V&V 指針 2020 における関連規格のデジタル安全保護系 V&V 指針 2008 からの変更に関する確認結果」に示す。年版を最新のものに変更したものは 2 件である。これらの変更内容のうち、「表 3.2.2-1　引用規格の年版等の変更に該当する事項」の 1 件名が技術評価の対象となることを確認した。

この技術評価については、次項で述べるデジタル安全保護系 V&V 指針 2020 の国内外の知見の反映等に係る技術評価の結果と併せて評価を行う。

表 3.2.2-1　引用規格の年版等の変更に該当する事項

No	件名	主な変更内容又は再確認の内容	記載箇所
1	JEAG 4121-2015[2018 年追補版]原子力安全のためのマネジメントシステム規程（JEAC 4111-2013）の適用指針	「原子力発電所における安全のための品質保証規程（JEAC 4111-2003）の適用指針 －原子力発電所の運転段階－」→「原子力安全のためのマネジメントシステム規程（JEAC 4111-2013）の適用指針」と名称変更し、年版を 2005[2007 年追補版]→2015[2018 年追補版]に変更	3.3 V&V（解説-10）ソフトウェアツール

（２）　国内外の知見の反映等

デジタル安全保護系 V&V 指針 2008 からデジタル安全保護系 V&V 指針 2020 への変更点について、国内外の知見の反映等によると判断した事項及び変更点以外で再度確認を行った事項は「表 3.2.2-2　国内外の知見の反映等に該当する変更事項」に示すとおりであり、事項ごとに技術的妥当性を検討した。

表 3.2.2-2　国内外の知見の反映等に該当する変更事項

No.	件名	主な変更内容又は確認の内容	記載箇所
1	検証及び妥当性確認（V&V）	・V&V の対象規格を JEAC4620 から JEAC4620 等に変更し、V&V 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ことを追加	4．1 V&V の目的と概要
		・V&V を実施する個人又はグループの力量及び経済面、工程管理に関する制約を受けないことを追加 ・なお書きで規定していた設計・製作者の各作業項目及び検証者の各作業項目を削除 ・図１の設計・製作作業の範囲を示す一点鎖線の範囲の各ステップに設計検証を追加 ・ソフトウェアの品質確保に適用する品質保	4．2 V&V の実施 （解説-10）ソフトウェ

		証仕様書の項番号を「7.6 監視機器及び測定機器の管理」から「7.1.5 監視及び測定のための資源」に変更 ・用語の定義「3.2 安全保護系」の範囲と V&V の対象範囲について確認	アツール

４．技術評価の内容

４．１　デジタル安全保護系規程 2020

４．１．１　過渡時、事故時及び地震時の機能

本規程は過渡時、事故時及び地震時の機能について、「4.1 過渡時及び地震時の機能」及び「4.2 事故時の機能」に詳細を規定している。

（１）　変更の内容（「表 4.1.1-1　過渡時、事故時及び地震時の機能に関する規定内容の変更点」参照）

① 過渡時及び地震時の機能と事故時の機能に分割し、前者は「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」、後者は「異常な状態を検知し，原子炉停止系（原子炉の緊急停止機能）及び必要な工学的安全施設を自動的に作動させる設計」に対応することを明確化した。

表 4.1.1-1　過渡時、事故時及び地震時の機能に関する規定内容の変更点

デジタル安全保護系規程 2020	デジタル安全保護系規程 2008
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。 4.2 事故時の機能 ディジタル安全保護系は，設計基準事故が発生する場合において，その異常な状態を検知し，原子炉停止系（原子炉の緊急停止機能）及び必要な工学的安全施設を自動的に作動させる設計とすること。	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。

（２）　日本電気協会による変更の理由

① 「JEAC 4604-2009 原子力発電所安全保護系の設計規程」に合わせ、「原子炉停止系」を「原子炉停止系（原子炉の緊急停止機能）」とした。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（JEAC4620-2008）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（JEAG4609-2008）」に関する技術評価書（以下「デジタル安全保護系規程 2008 等技術評価書」という。）の 5.1(1)「①過渡時，

事故時及び地震時の機能」の適用条件を反映。過渡時と事故時とで機能要求が異なるため、それぞれ別の項目として記載した。文章は技術基準規則に合わせた。

（３）　検討の結果

①　「4.1 過渡時及び地震時の機能」の規定内容は、技術基準規則第３５条第１号の規定と同等であり、デジタル安全保護系規程 2008 等技術評価書の 5.1(1)デジタル安全保護系規程「①過渡時、事故時及び地震時の機能」の適用に当たっての条件は下記としている。

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。

これを受けて、技術基準規則解釈 第３５条第４号（１）には、以下のように規定されている（表 2.3-1 より再掲)。

（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。

「4.1 過渡時及び地震時の機能」は上記を反映したものであり、妥当と判断する。

デジタル安全保護系規程 2020 には「(解説-5) 過渡時及び地震時の機能」が追加された。

(解説-5) 過渡時及び地震時の機能 ここで規定する「地震」は基準地震動を指している。原子炉を自動停止する地震加速度設定値は，基準地震動による応答加速度以下とすることができる。 「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。

技術基準規則第３５条第１号は「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。」と規定しており、第二段落の文章はそのための方法を具体的に規定した内容である。

したがって、「4.1 過渡時及び地震時の機能」の末尾に「「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。」を加える。

「4.2 事故時の機能」の規定内容は、デジタル安全保護系規程 2008 の規定内容をほぼ踏襲したものであり、「実用発電用原子炉及びその附属施設の位置、構造及び設備の基準に関する規則」（以下、「設置許可基準規則」という。）第２４条第２号に規定する「設計基準事故が発生する場合において、その異常な状態を検知し、原子炉停止系統及び工学的安全施設を自動的に作動させるものとすること」と整合しており、妥当と判断する。

（４）　変更点以外の評価

①　安全保護系の定義と適用範囲

用語の定義は技術評価の対象ではないが、用語の定義に「3.2 安全保護系」が追加され、設備の範囲として検出器から動作装置入力端子までとし、検出器が含まれることが明記された[4]。

> 3.2 安全保護系
> 原子炉施設の異常状態を検知し，必要な場合，原子炉停止系（原子炉の緊急停止機能），工学的安全施設の作動を直接開始させるよう設計された設備であり，検出器から動作装置入力端子までをいう。

技術基準規則には「安全保護系」という用語は使用されておらず、技術基準規則解釈第３５条第４号（１）及び（７）にはデジタル安全保護系規程 2008 を適用するに当たっての要件において使用されている[5]（「表 2.3-1　技術基準規則及び解釈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」参照）。「安全保護系」の定義は、「発電用軽水型原子炉施設に関する安全設計審査指針」（平成２年８月 30 日原子力安全委員会決定）の「Ⅲ．用語の定義」において、「原子炉施設の異常状態を検知し、必要な場合、原子炉停止系、工学的安全施設等の作動を直接開始させるよう設計された設備をいう。」とされており、日本電気協会は、安全保護系の設備の範囲として「検出器から動作装置入力端子まで」と定義している。

「ディジタル安全保護系」及び「ディジタル計算機」の範囲について、日本電気協会は次のように説明している[6]。

○ディジタル安全保護系とは

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

○「ディジタル計算機」とは

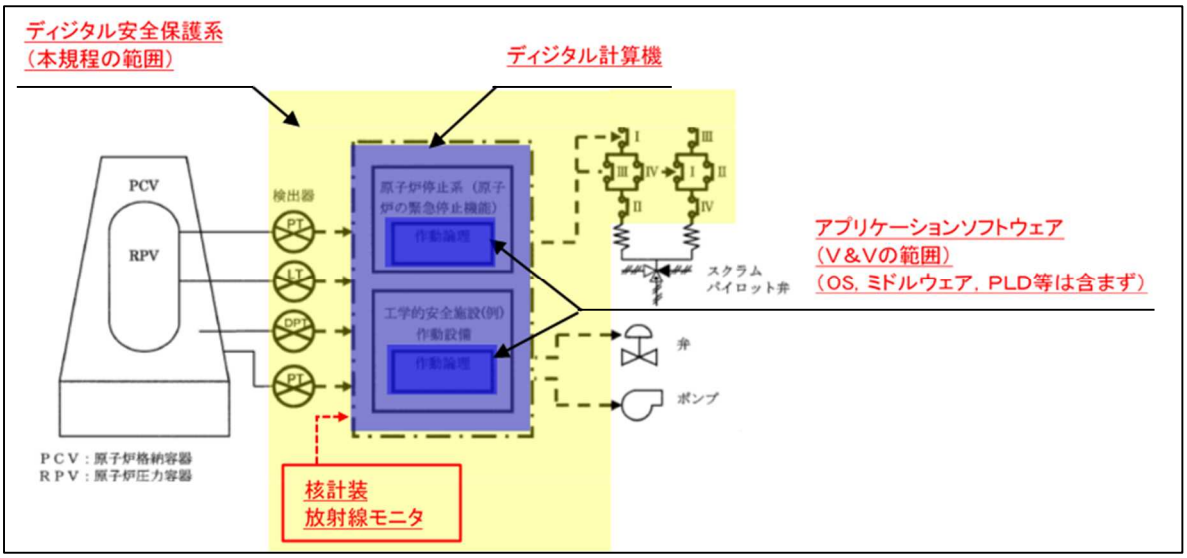
本規程におけるディジタル計算機とは，安全保護系としての機能を実現するソフトウェアが実装されたディジタル計算機（下図の青色ハッチング）を指しています。

---

[4] 用語の定義については、要求事項でないことから技術評価対象外と分類し、規定本文の要求事項との関係において技術評価することにしている（「添付資料－１　変更点一覧」の「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 4620-2020 における同 JEAC 4620-2008 からの変更点一覧」№.２参照）。用語「安全保護系」は「1.目的」に使用されているが、同箇条の変更内容は「記載の適正化のための変更」に分類（同№.１参照）され、技術評価の対象から除外されることから、変更点以外の評価とした。

[5] 「デジタル安全保護系」という用語は除く。

[6] 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　資料３－２　回答 1.3)



上記をまとめると以下のようになる。

○　デジタル安全保護系とは、デジタル計算機を有する原子炉停止系及び工学的安全施設作動系の演算・論理回路を有する安全保護系をいう。

○　デジタル計算機とは、原子炉停止系及び工学的安全施設作動系の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設備をいう。

安全保護系に属するデジタル化された核計装や放射線計装などの装置に関する論理・演算処理部は、本規程の「ディジタル計算機」に含まれるのかについて、日本電気協会は次のように説明している[7]。

本規程の対象は，ディジタル計算機に「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」を実装したディジタル安全保護系（検出器～動作装置入力端子まで）です。ここで，核計装や放射線計装は，演算部分を含め検出器として扱っており，本規程におけるディジタル計算機（ソフトウェア）としては要求範囲外です。

また、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について次のように説明している[8]。

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

[7] 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　資料３－１　回答 1. 3)

[8] 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　資料４－１　回答 2. 1)

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。

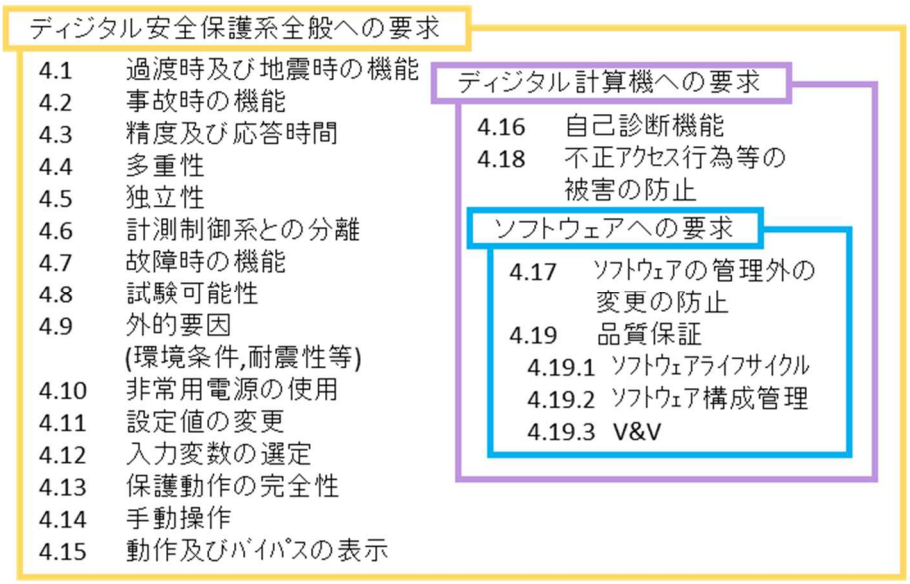
上記のような点から，JEAC4620 では 2008 年の制定時から核計装，放射線モニタを「ディジタル計算機」の対象とはしておらず， 2020 年の改定においてもその考え方は変更しておりません。

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。

日本電気協会は、核計装・放射線計装の論理・演算処理部は、原子炉停止系及び工学的安全施設作動系の演算・論理回路ではないため、本規程でいうデジタル計算機ではないとしている。また、規定ごとの適用範囲について、次のように説明している[9]。

▼JEAC4620-2020 ４章における各要求事項との関係

[9] 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　資料４－１　回答 1. 1)



日本電気協会の説明によれば、核計装・放射線計装の論理・演算処理部には「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」、「4.17 ソフトウェアの管理外の変更の防止」及び「4.19 品質保証」は適用されないということになる。

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、適用範囲の詳細を日本電気協会は次のように説明している[10]。

○「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

[10] 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　資料４－１　回答 1. 2)

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。

また、「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しているが、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ある。同規程では適用対象外とした理由について、日本電気協会は次のように説明している[11]。

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（資料４－１の回答２．１)）。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。

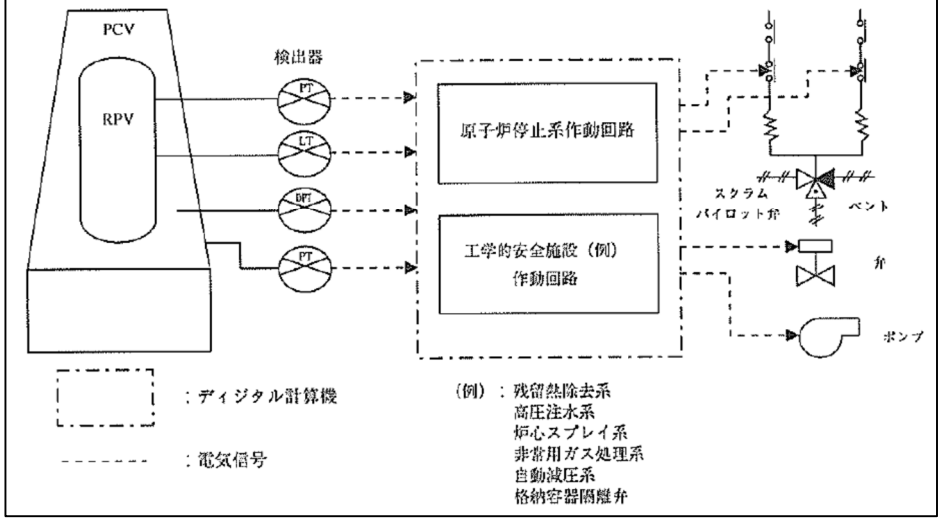
但し，これは核計装・放射線モニタについて，技術基準規則 35 条で要求されている事項を満足しなくて良いという意味ではありません。

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。

[11] 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　資料４－１　回答 2.2)

「発電用原子力設備に関する技術基準を定める省令の解釈」の別記－７「ディジタル安全保護系を適用するに当たっての要求事項」を策定した経緯を調べると、「原子炉制御室における誤操作防止のための設備面への要求事項及びディジタル計算機の安全保護系への適用に当たっての要求事項について」(平成 17 年 12 月、原子力安全・保安院、独立行政法人 原子力安全基盤機構) において、デジタル安全保護系規程 2020 及びデジタル安全保護系規程 2008 の前身である「安全保護系へのディジタル計算機の適用に関する指針」JEAG 4609-1999 が参考規格として記載されている。同指針の適用範囲は「原子力発電所の計測制御装置のうち，安全保護系に適用するディジタル計算機を対象」とされ、1999 年当時には検出器の演算・論理処理部にデジタル（CPU 等）が使われたプラントも存在していた実態を考慮すれば、明示されてはいないものの、検出器のデジタル化された演算・論理処理部は、下記の「参考図１ ディジタル計算機を適用した安全保護系の設備概念図 (BWR)」に示すディジタル計算機の四角枠の中に含まれていたと考えるのが自然である。

参考図１　ディジタル計算機を適用した安全保護系の設備概念図（BWR）



その後の技術の進歩により、核計装・放射線計装のデジタル化が進んだものの、「ディジタル計算機」の範囲は見直されることなく、現在に至ったと思われる。

日本電気協会の説明によれば、デジタル安全保護系規程 2020 の規定のうち「4.16 自己診断機能」から「4.19 品質保証」までは核計装・放射線計装の論理・演算処理部には適用されないが、仮にこれらの規定をデジタル化された核計装・放射線計装の演算・論理処理部に適用した場合の適用性について、日本電気協会は、次のように説明している[12]。

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

[12] 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　資料４－１　回答 2.3)

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。

ディジタル制御を適用した核計装，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。

デジタル安全保護系に属する核計装・放射線計装の論理・演算処理部は、原子炉停止系・工学的安全施設作動系と同等の設計管理が行われるべきものであり、日本電気協会は、デジタル安全保護系規程を核計装・放射線計装の論理・演算処理部に適用することに問題はないとしている。また、技術基準規則第３５条は、「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。」とし、第５号において「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。」としており、安全保護系に対する要求事項となっている。これらから、デジタル安全保護系規程の適用範囲は妥当ではない。

したがって、今後は、デジタル安全保護系規程 2020 及びデジタル安全保護系規程 2008 の適用範囲は、日本電気協会の説明によらず、核計装・放射線計装を含む検出器側のデジタル化された演算・論理処理部についても含むこととし、同規程における「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）に対する要求事項を「デジタル安全保護系のデジタル化された演算・論理処理部」（核計装・放射線計装も含む安全保護系全体）に適用することとし、同規程（解説を含む。）における「ディジタル計算機」は、「デジタル安全保護系のデジタル化された演算・論理処理部」と読み替える。

なお、「4.18 不正アクセス行為等の被害の防止」その他の評価については４．１．５項において述べる。「4.19 品質保証」及び「4.17 ソフトウェアの管理外の変更の防止」

については４．１．９項において述べる。「4.16 自己診断機能」については、技術基準規則解釈において、デジタル安全保護系の適用に当たってデジタル安全保護系規程 2008 の自己診断機能に関する「(解説-11)」を引用していることから、デジタル安全保護系規程 2008 の「(解説-11)」は「4.15 自己診断機能」に、ディジタル安全保護系規程 2020 の「(解説-15) 自己診断機能」は「4.16 自己診断機能」に加える。

また、「1.目的」は技術評価の対象ではないが、ディジタル安全保護系規程 2020 の「1.目的」の「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」は「原子力発電所の安全保護系においてデジタル化された演算・論理処理部を有するもの」に読み替える。また、「(解説-2) 適用範囲 (概念図)」は、デジタル計算機に核計装・放射線計装が入らないことが示されていることから、適用除外とする。

日本電気協会には、「(解説-2)」の「参考図 1 ディジタル安全保護系の概念図 (BWR)」及び「参考図 2 ディジタル安全保護系の概念図 (PWR)」の「デジタル計算機」の示す範囲並びに同図の凡例の記載を整理することを要望する。

② ソフトウェアの範囲と PLD

(a) ソフトウェアの範囲

ディジタル安全保護系規程 2020 に「ソフトウェア」の定義はないが、「(解説-3) 機能を実現するソフトウェア」には「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。」と記載されている。

「安全保護系としての機能を実現するソフトウェア」の意味について、日本電気協会は次のように説明している[13]。

○安全保護系としての機能を実現するソフトウェアとは

「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。

すなわち、ディジタル安全保護系規程 2020 における「ソフトウェア」とは、デジタル安全保護系の全てのソフトウェアではないとのことである。

技術基準規則解釈第３５条第３号においては、電子計算機に対する不正アクセス行為等による被害の防止措置としてソフトウェアの内部管理の強化を求めており、「4.18 不正アクセス行為等の被害の防止」において、対象を「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」に限定することは妥当ではない。

したがって、「(解説-3) 機能を実現するソフトウェア」の「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。」は削り、「ソフトウェア」の範囲は「安全保護系としての機能を実現するソフトウェア」に限定しないこととする。

[13] 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　資料３－１　回答 1.3)

(b) PLD の取扱い等

「3.1 ディジタル計算機」は「内蔵されたプログラムによって制御され，人手の介入なしにディジタルデータの算術演算,論理演算等の計算を行う装置」と定義されている。核計装や放射線計装のデジタル化においては、当初 CPU ベースでのソフトウェアが適用されていたが、電子機器技術の発展により近年では PLD[14]（FPGA[15]等）が適用される場合がある。「3.1 ディジタル計算機」には PLD が適用される場合を含むのか、含む場合に PLD は「内蔵されたプログラム」又は「ディ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のかについて、日本電気協会は次のように説明している[16]。

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（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ソフトウェア）に係る部分には採用実績がないため，現行版では PLD に実装されるプログラムを安全保護系としての機能を実現するソフトウェア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。

米国の IEEE Std 603[17]及び IEEE Std 7-4.3.2[18]の適用範囲とデジタル安全保護系規程 2020 の適用範囲の比較において、日本電気協会は次のように説明している[19]。

JEAC4620 と IEEE7-4.3.2 対象とする範囲の比較を以下に示します。

	JEAC4620	*IEEE 7-4.3.2*
対象システム	*安全保護系*	*安全系（safety system）※*
ディジタルデバイス	*ディジタル計算機（CPU ベース）*	*プログラマブル・ディジタル・デバイス（PLD や FPGA を含む）*
ソフトウェアに対する要件の範囲	*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（核計装・放射線モニタは検出器とみなし対象範囲外）*	*検出器から駆動装置入口まで,及びそれらの電源のうち,ディジタル化された設備*

※：safety system については，IEEE 603 で対象範囲が定義されている

[14] Programmable Logic Device
[15] Field Programmable Gate Array
[16] 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　資料３－１　回答 1.4)
[17] IEEE 603-2018 IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations
[18] IEEE 7-4.3.2-2016 IEEE Standard Criteria for Programmable Digital Devices in Safety Systems of Nu-clear Power Generating Stations
[19] 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　資料２－１　回答 1.3)③

日本電気協会は、「現行版ではPLDに実装されるプログラムを安全保護系としての機能を実現するソフトウェアの対象範囲としていない」としているが、PLDの中には計算機の基本動作を制御することに相当する機能及び安全保護系としての論理演算を行う機能の双方を実行する、ソフトウェアに相当するデジタル論理演算処理が含まれる場合がある。この処理は、ハードウェア記述言語によりその処理内容が記述され、設計ツールを用いて論理合成という変換により基本的な論理回路の組合せに展開した上で、配置配線という変換により集積回路上の配線情報を求めた上で、PLD素子内の集積回路にその配線情報として実装されることから、本規程の「ソフトウェア」の対象となりうる。

日本電気協会は、「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、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」としている。安全保護系のデジタル化された演算・論理処理部に装荷するソフトウェアとして採用されるPLDの取扱いについては、国内外の動向を踏まえ、明確にすることを要望する。

デジタル計算機を適用していない従来型の安全保護系とデジタル計算機を適用したデジタル安全保護系とを組み合わせた場合について、本文規定には該当する記述は見当たらないが、「(解説-1)目的」の末尾に「一部にディジタル計算機を適用する場合には，ディジタル計算機がシステムに影響を及ぼす範囲において，本規程に従うものとする。」と記載されている。

上記解説の記載は、日本電気協会の説明によれば、「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」の一部をソフトウェアで実装するデジタル計算機を適用したデジタル安全保護系と同回路の残部をアナログ型とした従来型の安全保護系との組合せを想定させる記載であり、複雑化して分かりにくい。「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」のデジタル計算機だけでなく、検出器側のデジタル部分を含むデジタル安全保護系のデジタル化された演算・論理処理部を対象として、従来型の安全保護系とを組み合わせた場合の要求事項を本文に規定することを要望する。その際に、「ディジタル計算機がシステムに影響を及ぼす範囲」とは「デジタル安全保護系のデジタル化された演算・論理処理部が担う検出器から動作装置入力端子まで」のことであると明確にすることを要望する。

③　アンアベイラビリティと誤動作率

「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，その安全保護機能に相応した高い信頼性を有すること」と規定している。また、デジタル安全保護系規程2008等技術評価書の5.1(1)デジタル安全保護系規程「⑥アンアベイラビリティ及び誤動作率の評価」の適用に当たっての条件は下記としている。

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。

これを受けて、技術基準規則解釈 第３５条第４号（６）には、以下のように規定

されている。

（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。

これに対応して「(解説-4) アンアベイラビリティ及び誤動作率の評価」（後述）が追加されている。上記適用に当たっての条件は、アンアベイラビリティ及び誤動作率の評価結果が「従来型のものと比較して同等以下」とされているが、デジタル安全保護系規程 2020 はデジタル安全保護系規程 2008 の規定内容から変更されておらず、「その安全保護機能に相応した高い信頼性を有すること」とされている。その理由について、日本電気協会は次のように説明している[20]。

アンアベイラビリティ及び誤動作率の評価については，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。信頼度の算出には構成要素のアベイラビリティを使用しますが，その値は導入時期や構成要素の種類，基となるデータベースの構築方法等によって異なる部分があり，従来型とディジタル型を比較評価しても，同じ条件での評価にはなりません。また，従来型とディジタル型では構成要素の点以外にも，自己診断機能の有無，信号処理方法，回路構成，システム構成の相違等，機能面，構成面における相違があり，これらも同じ条件での評価を阻害する要因となる可能性があります。このため，従来型とディジタル型のアンアベイラビリティ及び誤動作率をその数値だけで単純に比較することは，技術的に妥当な評価とならない可能性があるものと考えます。

また，従来型の定義もアナログ型を示しているのか，現状のディジタル型を示しているのか明確になっておりません。

ディジタル安全保護系の信頼性は，様々な要求事項を満足することで確保されるものです。アンアベイラビリティ及び誤動作率はその評価方法の一つであり，これだけを満足していれば信頼性を確保できるというものではありません。つまり，アンアベイラビリティ及び誤動作率の評価は，耐震性や耐環境性，品質保証，ソフトウェアの信頼性等を確保した上で，システムを構築し，そのシステムが非常時の動作やプラントの通常運転に大きな影響を与えない構成であることを確認することが主な目的であり，ある一定の数値を満足するから信頼性が十分であると判断できるものではないと考えております。

このような点から，設計を行う上で従来型と比較することは，一つの指標となりえますが，適用するシステムに合った信頼性を評価，確保することが重要と考えており，その数値自体が設計の要求事項になるものではないと考えております。このため，JEAC4620 では「アンアベイラビリティ及び誤動作率について，従来型と比較して同等以下であること」を要求事項としてはおりません。

[20] 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　資料２－１　回答　1. 1)

なお，海外の規格等でもこのような従来型と比較するような基準を適用しているケースは確認されておりません。

安全系システムの定量的な信頼性評価に関して、米国では以下の経緯がある。

- IEEE Std 603-1991 の 4.9 項には、安全システム設計の信頼性が各安全システム設計およびシステム設計に課せられる可能性のある定性的または定量的信頼性目標に適切であるかどうかを判断するために使用される方法を文書化する旨が規定されている。
- これに関して NRC は、標準審査要領[21]において、定量的信頼性目標の概念は単一の手法としてはこれを認めず[22]、信頼性評価は決定論的手法によることとしてる[23]。

これは、一般的にシステムを構成する部位ごとの故障率を用いた信頼性評価はシステムの構成品が増えるほど不利な評価値となる傾向があり、システム分析（ハザード分析等）を踏まえた総合的なシステム信頼性向上対策（設備増加を伴う場合がある）を制限し、かえって信頼性の低下をもたらす可能性があるためと考えられる。

また、NRC は定量的な信頼性評価を適用しない理由として、ソフトウエアとハードウエアの総合的な信頼性の観点から以下を記載している。

- デジタルコンピュータを含む安全システムの場合、ハードウェアとソフトウェアの両方の信頼性を考慮する必要があり、ハードウェア障害の結果ではないソフトウェア障害は設計エラーが原因であるため、ハードウェア信頼性評価に使用されるランダムな障害動作には従わない。その結果、ハードウェアとソフトウェアによってもたらされる非信頼度（アンアベイラビリティ）を評価するためには、さまざまな方法論を使用する必要がある。

一方、国内においては、技術基準規則解釈第３５条（６）において、以下のとおり規定している。

- 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
- 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。

これは、新規にデジタル設備を適用する場合に、同一の構成でアナログ設備をデジタル設備に置き換えることは信頼性の観点から適切ではなく、必要な多重化構成、自己診断等の対策を要求する必要があることが背景にあったことによる。

---

[21] Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants:LWR Edition - Instrumentation and Controls-Introduction (NUREG-0800,Appendix7.1-C (rev.4, 1997))

[22] ハザード分析等と併せて適用する場合は適用が認められる。

[23] NRC は PRA におけるデジタル I&C の取り扱いについては、Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition - Probabilistic Risk Assessment and Severe Accident Evaluation for New Reactors (NUREG-0800, 19.0 (Rev.3, 2015)の中で取り扱っている。

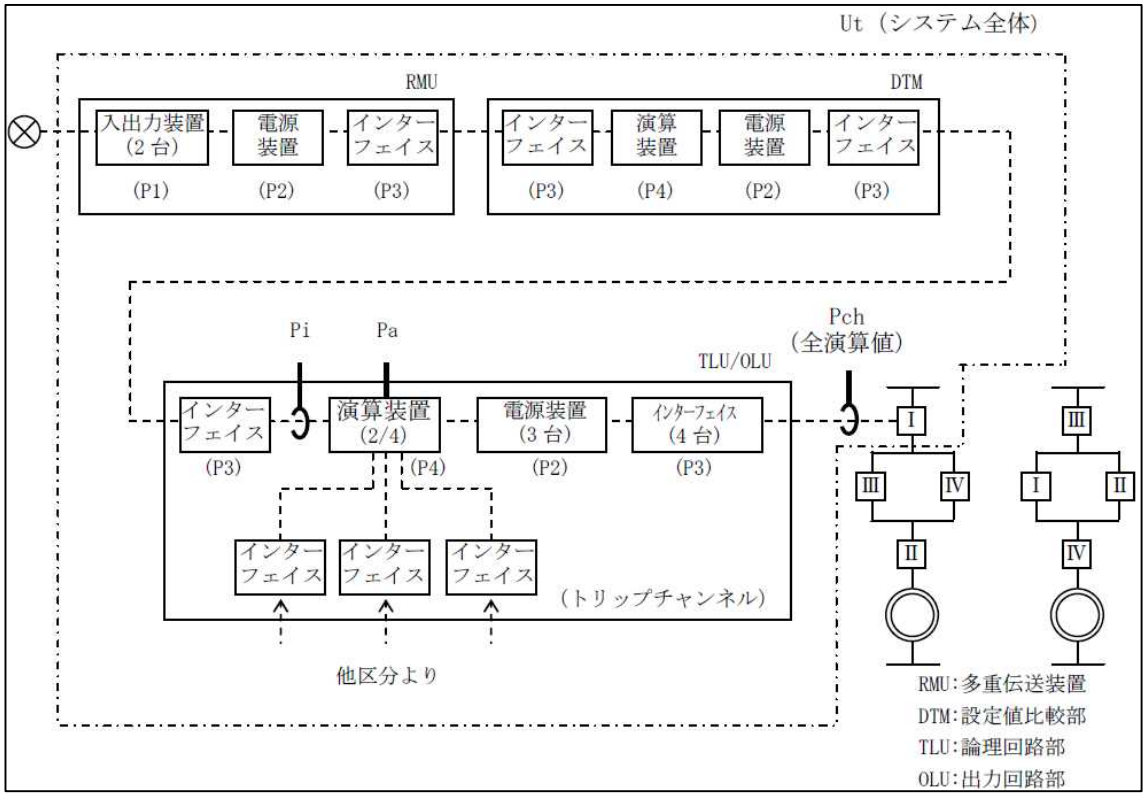
日本電気協会は､「アンアベイラビリティ及び誤動作率の評価は,耐震性や耐環境性,品質保証，ソフトウェアの信頼性等を確保した上で，システムを構築し，そのシステムが非常時の動作やプラントの通常運転に大きな影響を与えない構成であることを確認することが主な目的」としており、定量評価の取り扱いに関してはNRCの考え方と整合している。したがって、「安全保護機能に相応した高い信頼性を有すること」としたことは妥当と判断する。

日本電気協会の説明には、ハザード分析等の総合的なシステム信頼性向上対策には触れられていない。これまでのデジタルシステムの適用実績、国際的な動向等を踏まえれば、定量的な信頼性評価を絶対視しない考え方に移行すべき段階にあると考えられるため、ハザード分析等の総合的な信頼性向上対策と、これとあわせて実施すべき定量的なシステム信頼性評価の観点から、記載を充実することを要望する。

アンアベイラビリティ及び誤動作率をどのように考慮するのか、また、アンアベイラビリティや誤動作率の評価には、ソフトウェアも一つの構成要素になるのかについて日本電気協会は次のように説明している[24]。

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〉

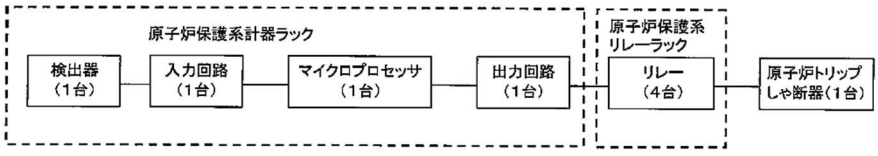


[24] デジタル安全保護系に関する日本電気協会規格の技術評価に関する検討チーム　資料１－２　回答 1.5)

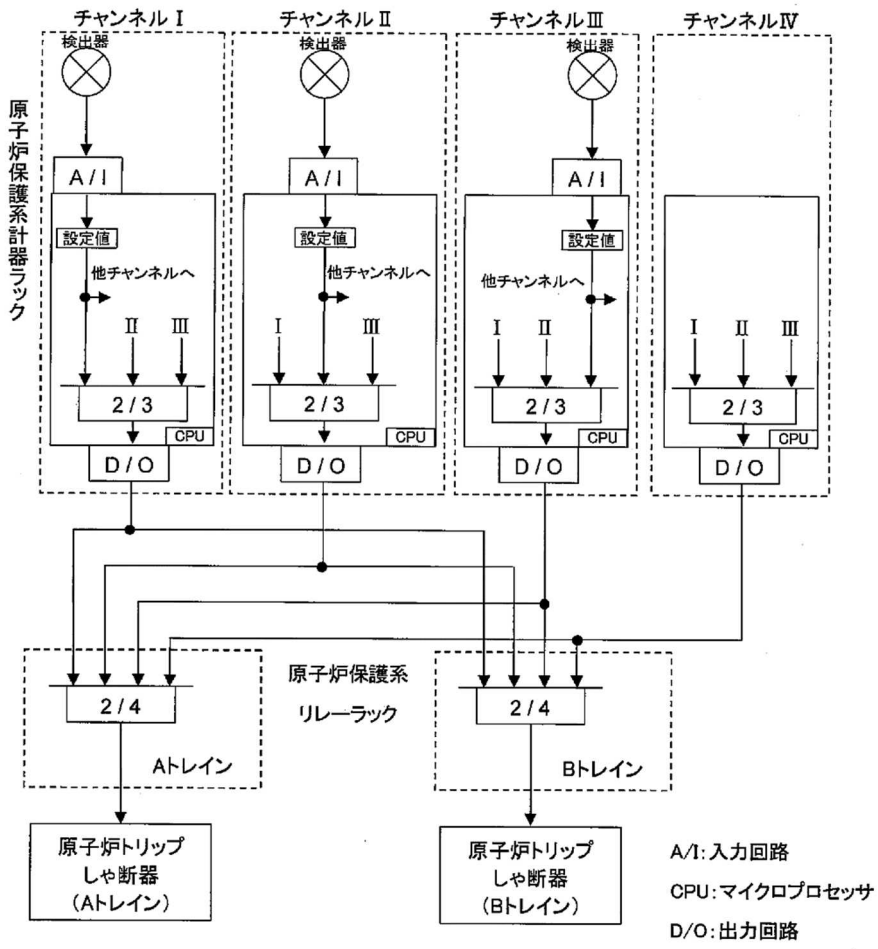
評価対象は，装置の入力からロードドライバ開までのディジタル安全保護系（一点鎖線の範囲）を対象としています。システム全体のアンアベイラビリティを構成要素のアベイラビリティを組み合わせることにより求めます。ここでは，原子炉スクラム要求時にスクラムが失敗する確率として，2 out of 4 システムの 3 重故障を求めます。また，誤動作率については，最初の故障の修理中に 2 番目の故障が生じる 2 重故障で誤スクラムが生じる頻度を求めます。

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〉

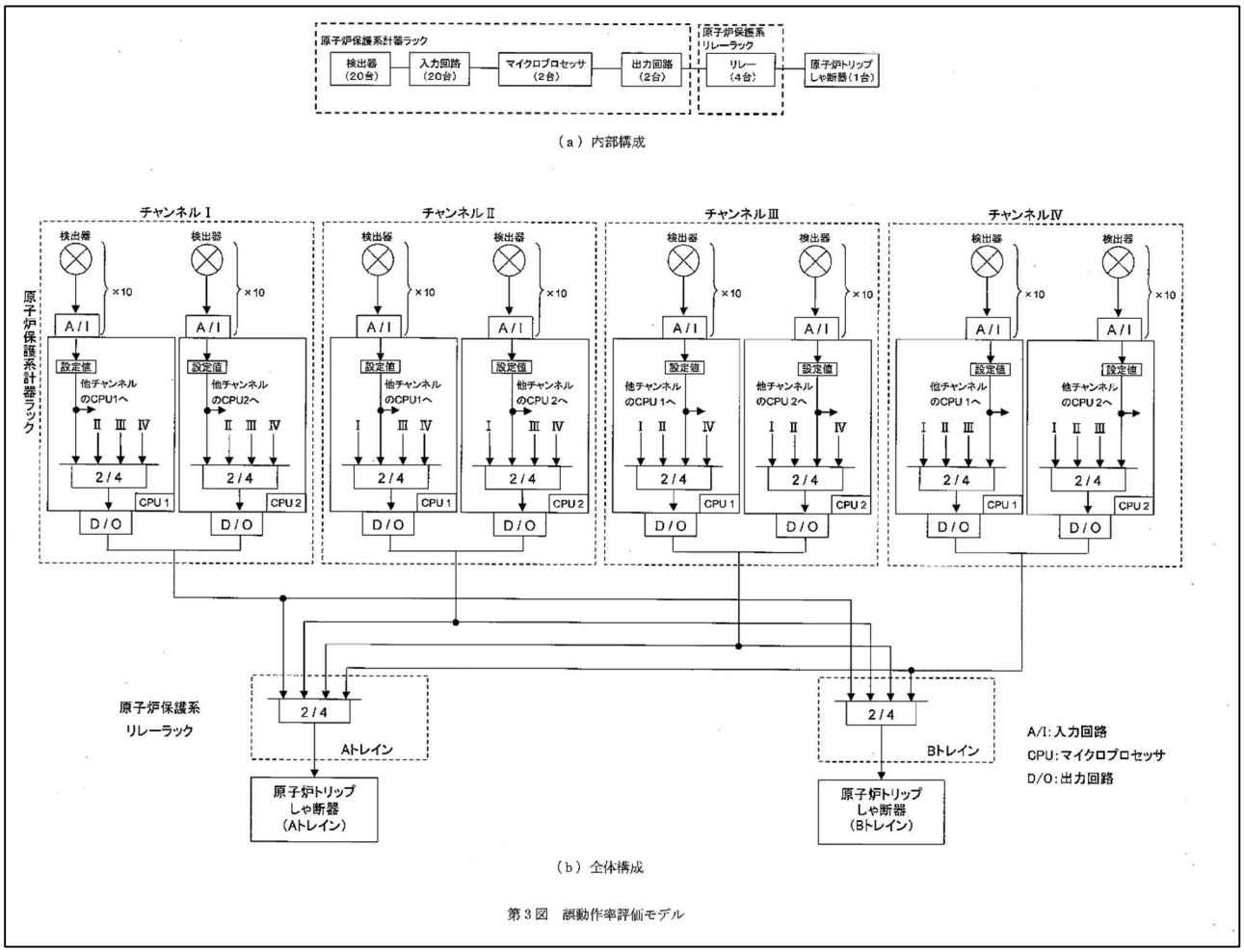


（ａ）内部構成



（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。

また､デジタル安全保護系規程 2008 等技術評価書の適用に当たっての条件を参考に、「(解説-4) アンアベイラビリティ及び誤動作率の評価」が追加された。

(解説-4) アンアベイラビリティ及び誤動作率の評価 アンアベイラビリティ及び誤動作率の評価に際して考慮するハードウェア構成要素としては，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，トリップの作動等が含まれる。

異常の検出等デジタル安全保護系の機能が記載され、当該機能がハードウェア構成要素の一部に扱われている。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あるが、機能を記載している理由について、日本

電気協会は次のように説明している[25]。

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，資料１－２の回答 1. 5)で示した信頼性評価モデル（前出の図）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。

日本電気協会は、「(解説-4) アンアベイラビリティ及び誤動作率の評価」の記載の趣旨は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としていることから、妥当と判断する。

日本電気協会の回答において検出部とみなすとされた核計装や放射線モニタのようにその内部処理として、燃料の許容限界を超えないようにするための安全に係る設定値に対する原子力特有のトリップ信号判定処理等にデジタル化された演算・論理処理が使われている場合、ハードウェア構成要素としてだけではなく、そのソフトウェア構成要素としてどのように考慮されるのか説明を求めたところ、日本電気協会は次のように回答している[26]。

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のみ考慮しております。この考え方は，内部処理の内容によらず，同様となります。

一方で，ソフトウェアに関しては，品質保証活動の中で信頼性を担保しております。ここで，本規定の適用範囲については資料１－２の回答１．３）で記載の通り，核計装や放射線モニタを検出器として取り扱っており，本規程におけるディジタル計算機としての要求範囲外としておりますので，核計装や放射線モニタにソフトウェアが適用される場合，そのソフトウェアに関しては JEAC4111/JEAG4121 で規定されている原子力の通常の品質保証活動の中で信頼性を担保することとなります。一方で，資料２－１の回答１．３）で記載した「原子炉停止系及び工学的安全施設作動系の演算・論理回路を実装するソフトウェア」に対しては，原子力の通常の品質保証活動に加えて，本規定で V&V の実施を要求しております。

近年、技術の発展に伴うデジタル処理の適用範囲の拡大及び機器更新時の部分的なデジタル処理の導入など、安全保護系へのデジタル技術は適用範囲が拡大されている。ある装置に技術基準規則第３５条第１項の「運転時の異常な過渡変化が発生する場合

[25] 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　資料１－２　回答 1. 6)

[26] 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　資料３－２　回答 1. 3) ①

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」ためのデジタル化された演算・論理処理が適用されているのであれば、これに必要な全ての要素を含めて評価するよう見直すことを要望する。また、「(解説-4) アンアベイラビリティ及び誤動作率の評価」 は、 ハードウェア構成要素にソフトウェア構成要素を加味するような表現になっていることから見直すことを要望する。

（5） 適用に当たっての条件

変更点

①

読み替える規定	読み替えられる字句	読み替える字句
4.1 過渡時及び地震時の機能	(末尾に追加)	「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。

変更点以外

①

読み替える規定	読み替えられる字句	読み替える字句
1.目的	本規程は、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（以下，ディジタル安全保護系という。）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するものである。	本規程は、原子力発電所の安全保護系においてデジタル化された論理・演算処理部を有するもの（以下，デジタル安全保護系という。）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するものである。
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。 （解説-15）自己診断機能 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	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安全保護系のデジタル化された論理・演算処理部の異常を検知した場合には、当該処理部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ィ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。	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安全保護系のデジタル化された演算・論理処理部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。
（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）

○「(解説-2) 適用範囲（概念図)」は適用除外とする。

② なし

③

読み替える規定	読み替えられる字句	読み替える字句
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。 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。 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。
（解説－4）アンアベイラビリティ及び誤動作率の評価	アンアベイラビリティ及び誤動作率の評価に際して考慮するハードウェア構成要素としては，異常の検出，検出信号の伝送，入出力信号の処理，演算処理，	（適用除外）

	トリップ信号の伝送，トリップの作動等が含まれる。	

（6） 要望事項

○ 「(解説-2)」の「参考図 1 ディジタル安全保護系の概念図 (BWR)」及び「参考図 2 ディジタル安全保護系の概念図 (PWR)」の「デジタル計算機」の示す範囲並びに同図の凡例の記載を整理し、検出器から動作装置入力端子までを含むデジタル安全保護系全体を広く包含して規定した規格とすることを要望する。

○ 安全保護系のデジタル化された演算・論理処理部に装荷するソフトウェアとして採用される PLD の取扱いについては、国内外の動向を踏まえ、明確にすることを要望する。

○ 解説-1 のまた書きは、「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」のデジタル計算機だけでなく、検出器側のデジタル部分を含むデジタル安全保護系のデジタル化された演算・論理処理部を対象として、従来型の安全保護系とを組み合わせた場合の要求事項を本文に規定することを要望する。その際に、「ディジタル計算機がシステムに影響を及ぼす範囲」とは、「デジタル安全保護系のデジタル化された演算・論理処理部が担う検出器から動作装置入力端子まで」のことであると明確にすることを要望する。

○ これまでのデジタルシステムの適用実績、国際的な動向等を踏まえれば、定量的な信頼性評価を絶対視しない考え方に移行すべき段階にあると考えられるため、ハザード分析等の総合的な信頼性向上対策と、これとあわせて実施すべき定量的なシステム信頼性評価の観点から、記載を充実することを要望する。

○ ある装置に技術基準規則第３５条第１項の「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」ためのデジタル化された演算・論理処理が適用されているのであれば、これに必要な全ての要素を含めて評価するよう見直すことを要望する。

○ 「(解説-4) アンアベイラビリティ及び誤動作率の評価」 は、 ハードウェア構成要素にソフトウェア構成要素を加味するような表現になっていることから見直すことを要望する。

４．１．２ 独立性の確保等

安全保護系の独立性については、「4.5 独立性」及び「(解説-7) 多重化されたチャンネル間の通信」に規定している。

（1） 変更の内容（「表 4.1.2 -1 独立性に関する規定内容の変更点」参照）

① チャンネル間に通信を用いる場合の機能的分離を追加した。

② 多重化されたチャンネル間の通信の機能的分離の措置を考慮事項から例示事項に変更した。

③　多重化されたチャンネル間の通信例を「通信接続の制御を受信側の異常が発信側に影響しない設計」から「ディ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」に変更した。

表 4.1.2 -1　独立性に関する規定内容の変更点

デジタル安全保護系規程 2020	デジタル安全保護系規程 2008
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。 （解説-7）多重化されたチャンネル間の通信 多重化されたチャンネル間の通信の機能的分離の措置の例としては以下がある。 (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)ディ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。	4.4 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。 （解説-5） 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。

（2）　日本電気協会による変更の理由

①　チャンネル間の通信における機能的分離を、「4.6 計測制御系との分離」と同様に本文要求事項とした。

②　解説では、通信における機能的分離に関して、独立性の確保を実現する手段を例として挙げる形とした。

③　デジタル安全保護系規程 2008 は解説の２つの具体例が同様の内容の記載であったため別の例を示すこととし、バッファメモリの設置を追記した。

（3）　検討の結果

①　「4.6 計測制御系との分離」においては、デジタル安全保護系規程 2008 から通信を共用する場合の機能的分離を規定している。「4.5 独立性」における追記は、これと整合を図ったものであり、妥当と判断する。

②③　デジタル安全保護系規程 2008 の（解説-5）は多重化されたチャンネル間の通信の機能的分離についての考慮事項を記載しており技術評価において本文規定と同様に

要求事項としていたが、デジタル安全保護系規程 2020 の「(解説-7) 多重化されたチャンネル間の通信」は例示に留めている。

「(解説-7) 多重化されたチャンネル間の通信」には、独立性の要件として「(1) 片方向通信」と「(2) バッファメモリ」の２項目が記載されている。これらは同時に適用するのか、それとも何れか一方でもよいのか、及びその理由について、日本電気協会は次のように説明している[27]。

解説-7 で示した適用の例は，同時に適用することを要求するものではありません。

資料２－１の回答 1. 12)を参照いただきたいですが，本解説についても，省令 62 号・別記７の「具体的仕様の例」を参考に例を選定しており，これにバッファメモリの適用を加えています。

デジタル通信が介在する場合の独立性の要件の国際的な動向としては、IEEE Std 7-4.3.2、DI&C-ISG-04 Rev.1 等で規定されている例がある。これらを比較した結果を「添付資料－３ 機能的分離（通信の独立性）に関する海外動向との比較」に示す。両規格の記載内容は具体的な仕様規定であるが、デジタル安全保護系規程 2020 の規定は、必ずしもこれらの内容が十分に反映されているとはいえない。また、「(解説-7) 多重化されたチャンネル間の通信」に記載の事項は、独立性を確保するための個別の手段の例示であるが、(1)に記載した複数の方法及び(2)の方法をどのように組み合わせるか明確でなく、また、国際的な動向と比較しても独立性を確保するための要件として不十分であり、妥当ではない。

技術基準規則解釈において、デジタル安全保護系規程 2008 の「(解説-5)」は同規格の適用に当たっての条件とされていたことから、デジタル安全保護系規程 2008 の「(解説-5)」は「4.4 独立性」に加え、デジタル安全保護系規程 2020 の「(解説-7)多重化されたチャンネル間の通信」の「多重化されたチャンネル間の通信の機能的分離の措置の例としては以下がある。」は「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を含む複数の手段の適切な組合せを考慮する。」と読み替え、読替え後の「(解説-7) 多重化されたチャンネル間の通信」の内容を「4.5 独立性」に加える。

（４） 変更点以外の評価

① 技術評価の対象となる変更点ではない[28]が「4.8 試験可能性」の変更内容を「表 4.1.2-2 試験可能性に関する規定内容の変更点」に示す。変更内容は記載の適正化であるが、規定の読み方によっては、デジタル安全保護系規程 2008 の「試験ができる機能」を有する設計とは、例えば、試験を開始するための操作スイッチを有する設計を要求しているとも読めることから念のため確認することとした。

表 4.1.2 -2 試験可能性に関する規定内容の変更点

[27] 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 資料２－１ 回答 1. 12)

[28] 「添付資料－１ 変更点一覧」に示すように変更内容は記載の適正化であり技術的変更には分類されていない。

デジタル安全保護系規程 2020	デジタル安全保護系規程 2008
4.8 試験可能性 ディジタル安全保護系は，安全保護機能の健全性及び多重性の維持が確認できるように，原子炉運転中でも各チャンネルが独立に試験ができる設計とすること。	4.7 試験可能性 ディジタル安全保護系は，安全保護機能の健全性及び多重性の維持が確認できるように原子炉運転中でも試験ができる機能を有する設計とすること。

日本電気協会は、「試験ができる機能を有する設計」を「試験ができる設計」に変更した理由について次のように説明している[29]。

「試験ができる設計」と「試験ができる機能を有する設計」に要求上の差異はなく，言葉の重複を避けたものです。つまり「○○できる」ということは，「○○の機能を有する」と同義であると考えています。

また，参考としている基準類や IEEE においても，文章の根幹だけを抜き出すと「試験ができる設計（もの）とする」あるいは「Capability of testing shall be provided（試験可能性を有すること）」となります。

なお，試験のための切り替えスイッチや試験端子を設けることは，試験できる設計を実装する際の技術的な選択枝のひとつですが，試験を行うためには安全保護系以外の装置（信号発生器やテスターなど）も必要であることから，安全保護系の中に試験が実施できる機能をすべて持たせるものではありません。

日本電気協会によると、変更内容は同義の範囲内で記載の適正化が行われたものであることから、妥当と判断する。

（5） 適用に当たっての条件

変更点

① なし

②③

読み替える規定	読み替えられる字句	読み替える字句
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。 （解説-7）多重化されたチャンネル間の通信 多重化されたチャンネル間の通信の機能的分離の措置の例としては以下がある。	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を含む複数の手段の適切な

[29] 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　資料３－３　回答 1)

	(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)ディ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。	組合せを考慮する。 (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。

変更点以外

① なし

４．１．３　故障時の機能要求、中央制御室の表示

安全保護系の故障時の機能要求、中央制御室の表示については、「4.7 故障時の機能」に規定している。

（1）　変更の内容（「表 4.1.3-1　故障時の機能に関する規定内容の変更点」参照）

① 駆動源の喪失を安全保護系の駆動源喪失と明確化し、フェイルセーフの記載のほかにフェイルアズイズを追加した。

表 4.1.3-1　故障時の機能に関する規定内容の変更点

デジタル安全保護系規程 2020	デジタル安全保護系規程 2008
4.7 故障時の機能 ディジタル安全保護系は，その駆動源の喪失，系の遮断及びその他の不利な状況になっても，最終的に原子炉施設を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，原子炉施設の安全上支障がない状態を維持できる設計とすること。	4.6 故障時の機能 ディジタル安全保護系は，駆動源の喪失，系の遮断及びその他の不利な状況になっても最終的に原子炉施設が安全な状態に落ち着く設計とすること。

（2）　日本電気協会による変更の理由

① 設置許可基準規則第２４条第５号の規定を反映した。2008 年版はフェイルセーフの記載のみであるが、フェイルアズイズについても記載した。なお、設置許可基準規則の「安全保護回路」は「安全保護系」と変更した。また、フェイルセーフの表現にフェイルアズイズの表現を追加し、本項での故障が安全保護系の故障であることが分かるように「その」を追記した。

（３）　検討の結果

①　「4.7 故障時の機能」の内容は、技術基準規則第３５条第４号の規定と整合しており妥当と判断する。

（４）　変更点以外の評価

①　変更点ではないが、「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」と規定されている。どのような情報（例えば第一原因）を「動作原因」とするのか説明を求めたところ、日本電気協会は次のように回答している[30]。

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*
- *D/W 圧力高高*
- *原子炉圧力高高*
- *炉心流量急減*
- *CV 急閉*
- *制御棒充填水圧力低*
- *主蒸気管室温度高*
- *主蒸気流量高*
- *燃料取替床放射能高高*
- *ペリオド短短*
- *地震加速度大*
- *MSIV2 弁以上閉*
- *主蒸気管放射能高高*
- *MSV 閉*
- *復水器真空度低*
- *主蒸気管圧力低*
- *原子炉建屋放射能高高*

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

[30] 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　資料１－２　回答 1.11）

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*

上記を一般化すると、以下の２つを満足することで要件を満たすと考えられる。

- 安全保護系が１チャンネルでも動作すれば警報を発し個々の動作状態を表示する。
- 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。

これについて、日本電気協会は次のように回答している[31]。

4.15 項の要求事項はディジタル安全保護系の動作原因が中央制御室に表示されることであり，このうち安全保護系に対する設計要件としては，動作原因を中央制御室で表示できるように，警報装置等のヒューマンマシンインターフェイスに情報を提供する（信号を出力する）ことまでと考えております。表示する情報や表示の具体的な実現手段については，プラントごとの監視/操作設計で考慮すべき事項であり，安全保護系に対する要求として規定するものではないと考えております。

なお，安全保護系の動作・状態を表示する実例については前出の通りです。また，ファーストヒット/ファーストアウトに関しては，安全保護系以外の要素（タービントリップや発電機トリップの動作原因）も含んでいることを補足致します。

設置許可基準規則第 10 条第１項及び同解釈は次のように規定している。

設置許可基準規則	設置許可基準規則解釈
（誤操作の防止） 第十条 設計基準対象施設は、誤操作を防止するための措置を講じたものでなければならない。	第１０条（誤操作の防止） １ 第１項に規定する「誤操作を防止するための措置を講じたもの」とは、人間工学上の諸因子を考慮して、盤の配置及び操作器具並びに弁等の操作性に留意すること、計器表示及び警報表示において発電用原子炉施設の状態が正確かつ迅速に把握できるよう留意すること並びに保守点検において誤りを生じにくいよう留意すること等の措置

[31] 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　資料２－１　回答 1.7)

	を講じた設計であることをいう。また、運転時の異常な過渡変化又は設計基準事故の発生後、ある時間までは、運転員の操作を期待しなくても必要な安全機能が確保される設計であることをいう。

ここで求められる警報表示を実現するためには、安全保護装置の動作原因についても適切な情報を生成し技術基準規則第４７条に規定する警報装置へ出力する必要がある。

上記動作原因の表示に関し、日本電気協会は、「安全保護系の動作が行われた場合、その動作した要素が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。」とするとともに、これに加えてプラントごとの監視操作設計の考え方に基づき原子炉スクラム等のイベントの動作原因をファーストヒット情報等で表示する設計を例示している。

安全保護装置の動作原因は多数決論理が成立し実際に安全保護動作が行われた時点をもって判別する必要があり、迅速にこれを把握するためには類似の信号（例えば原子炉停止に伴い二次的に発生するトリップ信号）との識別を適切に行う必要がある。日本電気協会の説明は、１チャンネルでも動作すればそれを出力するとともに、原子炉スクラム等のイベントの動作原因を表示するとしていることから、これらに照らして技術的に妥当と判断するが、動作原因をファーストヒット情報等で表示する設計については例示による回答に留まっている。

このため、安全保護系の動作原因について、その詳細な情報としてのチャンネルごとの動作原因に加え、安全保護系の動作原因（多数決論理が成立した原因）を、正確に識別して表示することが望ましく、そのための要件を具体化することを検討するよう要望する。この際、表示に関する記載は原子炉制御室に関する規程・ガイド等との関係も考慮し、適切な範囲の記載とすることに留意が必要である。

（５）　適用に当たっての条件

変更点

①　なし

変更点以外

①　なし

（６）　要望事項

○　安全保護系の動作原因について、その詳細な情報としてのチャンネルごとの動作原因に加え、安全保護系の動作原因（多数決論理が成立した原因）を、正確に識別して表示することが望ましく、そのための要件を具体化することを検討するよう要望する。

４．１．４　駆動源の喪失等に対する措置

駆動源の喪失等に対する措置については、「4.10 非常用電源の使用」に規定している。

（1） 変更の内容（「表 4.1.4 -1 駆動源の喪失等に対する措置に関する規定内容の変更点」参照）

① 外部電源系が喪失した場合あるいは短時間の全交流動力電源喪失の場合でも安全保護機能を果たすことが可能なようにするとの規定を削除し、非常用所内電源系からの給電を明確化した。

表 4.1.4 -1 駆動源の喪失等に対する措置に関する規定内容の変更点

デジタル安全保護系規程 2020	デジタル安全保護系規程 2008
4.10 非常用電源の使用 ディジタル安全保護系は，非常用所内電源系より給電される設計とすること。	4.9 非常用電源の使用 ディジタル安全保護系は，外部電源系が喪失した場合あるいは短時間の全交流動力電源喪失の場合でも安全保護機能を果たすことが可能なように，非常用所内電源系より給電される設計とすること。

（2） 日本電気協会による変更の理由

① 「短時間の全交流動力電源喪失」とは、安全設計審査指針を参照したものであり、デジタル安全保護系規程 2008 制定時において、「短時間」とは 30 分程度と解釈されており、さらに「長時間」SBO[32]は「考慮する必要はない」とされていた。しかし、この解釈は新規制基準では成立しない。新規制では、SBO 対策は安全保護系とは別に重大事故等対処設備にて対応することとなっており、安全保護系は非常用電源から給電されることのみを要求とした。

（3） 検討の結果

① 短時間の全交流動力電源喪失に関する規定を削除し、非常用所内電源系からの給電を明確化したものであり妥当と判断する。

（4） 適用に当たっての条件

① なし

４．１．５ 不正アクセス行為等の被害防止措置

不正アクセス行為等の被害防止措置については、「4.18 不正アクセス行為等の被害の防止」に規定している。

（1） 変更の内容（「表 4.1.5-1 不正アクセス行為等の被害防止措置に関する規定内容の変更点」参照）

① 外部ネットワークとの遮断規定を削除（解説に移行）し、不正アクセス行為等による被害を防止するために必要な措置を講じる設計とする規定を追加した。

[32] Station Black Out（全交流電源喪失）の略

表 4.1.5-1　不正アクセス行為等の被害防止措置に関する規定内容の変更点

デジタル安全保護系規程 2020	デジタル安全保護系規程 2008
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 （解説-17）不正アクセス行為等の被害の防止 不正アクセス行為等の被害の防止に必要な措置の例としては，以下がある。 (1) 外部ネットワーク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。 (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) 解説-16 の(2)鍵付きスイッチの設置及び(3)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。	4.16 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。

（２）　日本電気協会による変更の理由

①　技術基準規則第３５条第５号の規定を反映して、表現は分かりやすいように見直した。解説は技術基準規則解釈第３５条第３号の規定に合わせた。また、デジタル安全保護系規程 2008「4.16 外部ネットワークとの遮断」をデジタル安全保護系規程 2020「(解説-17) 不正アクセス行為等の被害の防止」の(1)に移行した。「(解説-16) ソフトウェアの管理外の変更の防止[33]」のうち不正アクセスの防止にも有効な項目を同 (解説-17) の(3)で参照した。また、デジタル安全保護系規程 2008 等技術評価書の 5.1(1)「⑤外部ネットワークとの遮断」の適用条件「外部影響の防止された設備とすること。」を反映した。

（３）　検討の結果

①　「4.18 不正アクセス行為等の被害の防止」は、技術基準規則第３５条第５号の規定に整合する内容に変更したものであり妥当と判断する。

「(解説-17) 不正アクセス行為等の被害の防止」については、デジタル安全保護系規程 2008 等技術評価書の 5.1(1)デジタル安全保護系規程「⑤外部ネットワークとの遮

[33] 「添付資料－１　変更点一覧」の「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 4620-2020 における同 JEAC 4620-2008 からの変更点一覧」№18 参照

断」の適用に当たっての条件は下記としている。

④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。

これを受けて、技術基準規則解釈 第３５条第４号（５）には、以下のように規定されている。

（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。

「(解説-17) 不正アクセス行為等の被害の防止」の(1)は上記及び技術基準規則解釈第３５条第3号の内容の一部を反映したものである。

「(解説-17) 不正アクセス行為等の被害の防止」の(1)において、「外部ネットワークと遮断」とあるが、ここでの「遮断」の定義について、日本電気協会は次のように説明している[34]。

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。

「遮断」を満足する具体的な要件は、実例を一般化すると以下と捉えられる。

- 「外部ネットワークとの直接接続をしない。」は、物理的な接続を制限し最小限とすることをいう。
- 「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」は、前項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をいう。
- 「信号を一方向（送信機能のみ）通信に制限」は、上記において可能な限り外側向けの通信を適用することをいう。

これについて、日本電気協会は次のように回答している[35]。

「遮断」については、定義を規定するのではなく，ディジタル計算機に対し影響を与えない状態を作るための手段として記載しております。

これは遮断を実現するための方法（制御方式，通信方式，回路構成など）は多種多様であると共に，セキュリティ関連の技術革新に伴って新技術が導入されていくことが考えられ、具体的な要件を設定して限定することは、設計の柔軟性を損なったり、新たな技術の導入に際し障害になってしまう可能性があることから，解説-17 では不正アクセス行為等の被害の防止に必要な措置の例として挙げ，手段とし

[34] 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　資料１－２　回答 1.12)

[35] 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　資料２－１　回答 1.8)

ての記載としています。

「外部ネットワークとの直接接続をしない。」とは、物理的な接続を制限し最小限とすることであり、「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」、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、「安全保護装置の信号を一方向（送信機能のみ）通信に制限」とは、これらにおいて可能な限り外側向けの通信を適用することと考えられる。したがって、分かりやすさの観点から、「(解説-17) 不正アクセス行為等の被害の防止」の (1) に「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。」を加える。

「(解説-17) 不正アクセス行為等の被害の防止」は、「4.18 不正アクセス行為等の被害の防止」の措置を行う際に考慮すべき内容であることから、同解説の内容は、「4.18 不正アクセス行為等の被害の防止」加える。その際、「外部ネットワーク」の意味を明確にするために、デジタル安全保護系規程 2020 の「3.用語の定義」の「3.5 外部ネットワーク」を参考に、「外部ネットワーク」は、「外部ネットワーク (インターネット等)」と読み替える。また、同解説の「不正アクセス行為等の被害の防止に必要な措置の例としては，以下がある。」は「不正アクセス行為等の被害の防止に必要な措置については，以下を考慮する。」と読み替える。

「(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。」とあるが、対象を設計開発段階からではなく、据付以降に限定している理由について、日本電気協会は次のように説明している[36]。

> *規格化にあたっては，技術基準規則の解釈（第３５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。*

また、フルライフサイクル管理の考え方を適用しない理由について、日本電気協会は、次のように説明している[37]。

> *今回の改定に際して，当該の記載については技術基準規則の解釈（第三十五条）より引用したため、現地に限定した記載となっていますが，フルライフサイクル管理の必要性は認識しており，設計段階において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。*

---

[36] 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　資料１－２　回答 1.13)

[37] 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　資料３－２　回答 1.9)

設計段階における規格への反映については今後のセキュリティ関連規格の動向とともに反映する方向で検討したいと考えます。

「(解説-17) 不正アクセス行為等の被害の防止」の(2)の規定は技術基準規則解釈第３５条第３号の規定を引用したもので、同規定は「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及びウイルス等の侵入を防止する」としていることから、妥当と判断する。

設置許可基準規則は同解釈第２４条第６号において「システムの導入段階、更新段階又は試験段階でコンピュータウイルスが混入することを防止する」と規定していることを踏まえ、設計開発段階を含むフルライフサイクルにおいてウイルスの侵入等を防止するよう規定することを要望する。

（４） 変更点以外の評価

４．１．１（４）で述べたたように、デジタル安全保護系規程 2020 の「４．ディジタル安全保護系に対する要求事項」及び解説において、「ディジタル計算機」は、「デジタル安全保護系のデジタル化された演算・論理処理部」と読み替えることとしている。したがって、「4.18 不正アクセス行為等の被害の防止」において、「・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」とあるのは「・デジタル化された演算・論理処理部に使用目的に沿うべき動作をさせない行為」と、「・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」とあるのは、「・デジタル化された演算・論理処理部に使用目的に反する動作をさせる行為」と読み替える。

（５） 適用に当たっての条件

変更点①及び変更点以外①

読み替える規定	読み替えられる字句	読み替える字句
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 (解説-17) 不正アクセス行為等の被害の防止 不正アクセス行為等の被害の防止に必要な措置の例としては，以下がある。 (1) 外部ネットワーク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	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。 ・デジタル化された演算・論理処理部に使用目的に沿うべき動作をさせない行為 ・デジタル化された演算・論理処理部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

	ルスの侵入等の外部影響を防止する。	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) 解説-16 の(2)鍵付きスイッチの設置及び(3)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。	(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。

（6） 要望事項

○「(解説-17) 不正アクセス行為等の被害の防止」(2)の物理的及び電気的アクセスの制限については、設計開発段階を含むフルライフサイクルにおいてウイルスの侵入等を防止するよう規定することを要望する。

４．１．６ 計測制御系からの機能的分離

計測制御系からの機能的分離については、「4.6 計測制御系との分離」に規定している。

（1） 変更の内容（「表 4.1.6-1 計測制御系からの機能的分離に関する規定内容の変更点」参照）

① 解説にアイソレーションデバイスは安全保護系に属する旨を追記

② 解説の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の措置を考慮事項から例示に変更し、計測制御系からの情報受け制限と試験時及び保守時の例外扱いを追加

③ ディ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例示を追加

表 4.1.6-1 計測制御系からの機能的分離に関する規定内容の変更点

デジタル安全保護系規程 2020	デジタル安全保護系規程 2008
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	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

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。 （解説-8）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，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。 ・ディ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。 また，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は以下がある。 (1)試験時又は保守時を除き，計測制御系からの情報を受けない設計とする。 (2)試験時又は保守時に計測制御系からの情報を受ける場合には，当該チャンネルをバイパス又はトリップとする。 (3)ディジタル安全保護系から計測制御系への通信は，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。 (4)ディ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。	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。 （解説-6） 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，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。また，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は具体的には（解説-5）の事項を考慮する。 ＜参考＞ （解説-5） 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。

（２）　日本電気協会による変更の理由

①　IAEA SSR-2/1 の Requirement 64 に合わせ、アイソレーションデバイスの属性を明確にした。

②③　デジタル安全保護系規程 2008 等技術評価書の 5.1(1)「④計測制御系との分離」の適用条件を反映した。なお、同技術評価書の「試験時」は「試験時又は保守時」に変更した。デジタル安全保護系規程 2008 は解説-5 を参照していたが、参照することはやめ、同様な内容であっても例示を記載することとし、解説-7 の内容を追記した。

（３）　検討の結果

① アイソレーションデバイス[38]の属性規定については、「IAEA SSR-2/1(Rev.1) Safety of Nuclear Power Plants: Design」の「Requirement 64: Separation of protection systems and control systems」の規定に基づき、デジタル安全保護系と計測制御系との信号取合に用いる光／電気変換などのアイソレーションデバイスは安全保護系に属する旨を明確化したものであり妥当と判断する。

②③ デジタル安全保護系規程 2008 等技術評価書の 5.1(1)デジタル安全保護系規程「④計測制御系との分離」の適用に当たっての条件は下記としている。

> 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。

これを受けて、技術基準規則解釈 第３５条第４号（４）には、以下のように規定されている。

> （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。

日本電気協会は、上記の「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」は、分離手段として根拠が不十分であるため、反映しないこととした[39]としている。

また、技術基準規則解釈制定時に任意でのパブリックコメントの募集を実施した結果において、計測制御系との分離について下記の意見と回答が示され[40]、これを踏まえて技術基準規則解釈第３５条第４号（４）が規定された経緯がある。

> ＜意見＞
> 【安全保護系へのデジタル計算機の適用について】
> 「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。」とあるが、一般に多様化設備は非安全系で構成し、安全保護系に接続されることから、この表現では多様化設備の導入を阻害する恐れがあり、安全保護系と計測制御系とのインタフェースは機能的に分離することを要求すれば十分である。
> ＜回答＞
> 計測制御系からの誤った情報により安全性が損なわれる事態を防止するための要求です。試験時以外に、多様化設備により安全保護系を操作するシステムについては、技術の進展や第 3 条の特殊な設計による施設の認可などの状況を踏まえて、解釈の改訂に反映することとします。

[38] 通信相互間における電流の流れを防止しながらデータを送受信するために電気的に絶縁分離する装置
[39] 2019 年 12 月 25 日、第 73 回原子力規格委員会資料 73-4-2-2「JEAC 4620-20XX「安全保護系へのディジタル計算機の適用に関する規程」改定案 新旧比較表」7 頁
[40] 平成 25 年 6 月 19 日、第 11 回原子力規制委員会配付資料 別添 3 別紙「原子力規制委員会設置法の一部の施行に伴う関係規則の整備等に関する規則（案）等に対するご意見への考え方」197 頁

「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。」と規定されている。この「通信」の定義と，機能的分離が適用される範囲について日本電気協会は次のように説明している[41]。

「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。）

「解説-8 計測制御系との分離」には、デ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例が記載されている。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について、日本電気協会は次のように説明している[42]。

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。

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、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の説明を求めたところ、日本電気協会は次のように回答している[43]。

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

[41] 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　資料４－１　回答 3. 1)

[42] 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　資料１－２　回答 1. 7)

[43] 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　資料４－１　回答 3. 2)

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。

機能的分離のためには通信の独立性、及び信号の優先処理の考慮が必要と考えられるが、日本電気協会の説明によれば、一般的な機能的分離は安全保護系全般に適用されるとしたうえで、通信の独立性については、ネットワーク伝送やデータリンクへ適用されること、優先処理回路についても適用範囲としていることから妥当と判断する。また、優先処理回路がFPGA等による場合についても、ハードウエアの開発・設計として必要な品質保証活動を実施するとしていることから妥当と判断する。また、「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る（例えば、DI&C-ISG-04[44]に記載の項目）が、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、日本電気協会はその理由を次のように説明している[45]。

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。

いずれも「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。」との回答であるが、これによれば、バッファメモリさえ用いれば他に制限はないとも読める。この場合、通信方

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

[45] 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　資料１－２　回答 1.8)

向に関する制限はなくなり、非安全系との通信がある場合にそれからの影響を排除できなくなる。この課題に関して、国際的な動向としては、以下のように整理されている。

- 通信を行う場合の一般的な制限事項
- 通信の方向性に関する制限事項（例えば低位から高位への通信は安全を支援、又は強化する場合のみ許可）
- 非安全系からの信号により安全機能が損なわれないための考慮事項（優先度処理、及び共通原因故障としての考慮事項を含む）

これらを反映しなかった理由について、日本電気協会は次のように説明している[46]。

解説-8 に記載している具体例は，本文要求事項を満足するために採用する設計方針の例であり，このいずれかを必ず適用しなければならないというものではありません。また，逆に例に記載された一文が設計のすべてを説明しているものでもなく，例に記載された設計方針を採用した場合でも，本文要求事項を満足するように詳細な設計検討が行われます。

計測制御系全般に言えることではありますが，特にこのような通信機能については，これを実現する接続構成・回路構成・適用素子・適用ソフトウエアなどはきわめて多種多様であり，特定の設計仕様を前提とした詳細設計例を要件として記載することは，かえって設計の柔軟性を損なったり，新たな技術の導入の障害になってしまう可能性があります。したがって，本文においては，最終的に満たすべき要求のみを記載し，個々の設計の選択枝については解説に例を載せることとしています。

記載されている例は，当時の省令 62 号・別記 7 に示された「具体的仕様の例」を参考に，実際に適用する可能性のあるものを記載するとともに，IEEE 7-4.3.2 などでも検討されていたバッファメモリの利用についても記載しました。なお，省令 62 号の別記 7 に記載された「具体的仕様の例」については，これらを必ず適用するという性格のものではありませんでしたが，設計に際して有用な事例であると考え，JEAC4620 に反映しました。なお，その後の技術評価や技術基準規則の解釈では，この「具体的仕様の例」で示されていた内容の一部が，例であるか否かを明示されない形で記載されておりますが，技術基準規則本文で要求される事項の本質は特段変化していないと認識していることから，本規程では「具体的仕様の例」として扱っています。

ご参考ですが，特定の設計を前提として仕様を制限するような要件の記載方法については，米国でも解消する方向で検討が進んでおり，現行の IEEE 7-4.3.2 に記載されている仕様を限定する要求の多くは，次回改定時に本文から削除する方向で検討が進んでいます。この中には安全上の利点を条件とする要求も含まれています。

「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

[46] 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　資料２－１　回答 1.6)

ないよう措置を講ずること。」については、U.S.NRC[47]「SRP-7.1 Instrumentation and Controls - Introduction (1997)」[48]の「II. Acceptance Criteria」の「Supplemental Guidance for Digital Computer-Based Safety Systems」「5. Communications independence」(2)の記載に基づき規定されたものであるが、その後の技術の進歩により、2007 年以降の文書からは削除されている。また、「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」の規定は、米国で発行された暫定審査ガイド（DI&C-ISG-04、Highly-Integrated Control Rooms - Communications Issues (HICRc)）でハンドシェイク通信[49]が禁止されたこと、多様性を有する多区分型ディスプレイ適用にあたって本ガイドが参考となること等の技術の進展状況から、「(解説-8)計測制御系との分離」の(4)に他の有効な手段として「ディ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」と記載しており、妥当と判断する。

技術基準規則解釈において、デジタル安全保護系規程 2008 の「(解説-6)」は同規格の適用に当たっての条件とされていたことから、デジタル安全保護系規程 2008 の「(解説-5)」は「4.4 独立性」に加え、デジタル安全保護系規程 2020 の「(解説-8) 計測制御系との分離」の「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，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。・ディ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。」は「4.6 計測制御系との分離」に加える。

「試験時又は保守時を除き，計測制御系からの情報を受けない設計とする」の記載については、国際的な最新動向を踏まえ、「安全性を支援又は向上させる場合（試験時又は保守時に必要な場合を含む）を除き、計測制御系からの情報を受けない設計とする。」等の表現に見直すことを要望する。

「(解説-8) 計測制御系との分離」の「また、」以降の例示(1)及び(2)は上記理由により、また、(3)及び(4)は「4.5 独立性」の「(解説-7)多重化されたチャンネル間の通信」に記載する例示(1)及び(2)の内容と重複している（「4.1.2 独立性の確保等」参照）ことから、「4.6 計測制御系との分離」には加えないこととする。

また、国際的な動向としては、「添付資料-3 機能的分離（通信の独立性）に関する海外動向との比較」に示すように、米国では通信の独立性及び優先回路に多くの要件があり、デジタル安全保護系規程 2020 の記載は、必ずしもこれらの内容が十分に反映されているとはいえない。

このため、計測制御系との分離については、通信の独立性に関する要件及び低位から高位への信号伝送を許容する場合の条件、さらにこれに該当する通信がある場合の信号の優先処理の観点等から、IEEE Std 7-4.3.2、DI&C-ISG-04 Rev.1 等の国際的な動向を踏まえ、記載内容を整理し、この例示としてバッファメモリの適用等を記載すること

---

[47] United States Nuclear Regulatory Commission

[48] Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants:LWR Edition - Instrumentation and Controls-Introduction (NUREG-0800,Chapter 7.1 (rev.4, 1997))

[49] 通信を確実にするために、送信側の信号が受信側に届いたことを確認してから送信側が次のデータ信号を送信する通信方式

を要望する。

（4） 適用に当たっての条件

① なし

②③

読み替える規定	読み替えられる字句	読み替える字句
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。 （解説-8）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，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。 ・ディ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。 また，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は以下がある。 (1)試験時又は保守時を除き，計測制御系からの情報を受けない設計とする。 (2)試験時又は保守時に計測制御系からの情報を受ける場合には，当該チャンネルをバイパス又はトリップとする。 (3)ディジタル安全保護系から計測制御系への通信は，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	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，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。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。

	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。 (4)ディ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。	

（５） 要望事項

○「試験時又は保守時を除き，計測制御系からの情報を受けない設計とする」の記載については、国際的な最新動向を踏まえ、「安全性を支援又は向上させる場合（試験時又は保守時に必要な場合を含む）を除き、計測制御系からの情報を受けない設計とする。」等の表現に見直すことを要望する。

○計測制御系との分離については、通信の独立性に関する要件及び低位から高位への信号伝送を許容する場合の条件、さらにこれに該当する通信がある場合の信号の優先処理の観点等から、IEEE Std 7-4.3.2、DI&C-ISG-04 Rev.1 等の国際的な動向を踏まえ、記載内容を整理し、この例示としてバッファメモリの適用等を記載することを要望する。

４．１．７ 設定値の変更

設定値の変更については、「4.11 設定値の変更」に規定している。

（１） 変更の内容（「表 4.1.7-1 4.11 設定値の変更に関する規定内容の変更点」参照）

① 作動設定値を変更する必要がある場合に、手動による変更ができる設計から適切な変更が可能な設計に修正した。

表 4.1.7-1 4.11 設定値の変更に関する規定内容の変更点

デジタル安全保護系規程 2020	デジタル安全保護系規程 2008
4.11 設定値の変更 ディジタル安全保護系は，運転条件に応じた適切な保護を行うために設定値を変更する必要がある場合には，適切な設定変更が可能な設計とすること。	4.10 設定値の変更 ディジタル安全保護系は，運転条件に応じた適切な保護を行うために設定値を変更する必要がある場合には，手動にて作動設定値を変更できる設計とすること。

（２） 日本電気協会による変更の理由

① 運転条件に応じた設定値変更とは、設定値を書き替える手段の要求よりも、運転条件に応じて（自動的に）設定値が切り替わることの要求とした方が適切であるため、JEAC4604 の記載に合わせて本文を見直すとともに、解説を追加した。

（３） 検討の結果

① 技術基準規則第３５条第８号は設定値の変更について「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」と規定しており、その手段・方法は特に制限していない。手動による設定値変更に拘る必要性はないので、変更は妥当と判断する。

（４） 適用に当たっての条件

①なし

４．１．８ ライフサイクルを通じた品質の管理方法

ライフサイクルを通じた品質の管理方法については、「4.19.1 ソフトウェアライフサイクル」及び「(解説-19) ソフトウェアライフサイクル」に規定している。

（１） 変更の内容（「表 4.1.8-1 ライフサイクルを通じた品質の管理方法に関する規定内容の変更点」参照）

① 「(解説-19)」の「(2)各プロセスで実施すべき品質管理項目」における「(c)試験プロセス」において、ソフトウェア単体では確認できない内容をシステムとして確認する範囲については、事前に計画することを規定した。②同「(g)廃止プロセス」において、廃止されたソフトウェアの誤使用防止措置を講じる規定を追加した。

表 4.1.8-1 ライフサイクルを通じた品質の管理方法に関する規定内容の変更点

デジタル安全保護系規程 2020	デジタル安全保護系規程 2008
4.19.1 ソフトウェアライフサイクル （略） （解説-19）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 ディ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：（略） (b)製作プロセス：（略） (c)試験プロセス：（略） (d)装荷プロセス：（略） (e)運転プロセス：（略） (f)変更プロセス：（略） (g)廃止プロセス：（略） 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。	4.18.1 ソフトウェアライフサイクル （略） （解説-14） ディ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 ディ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，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：（略） 製作プロセス：（略） 試験プロセス：（略） 装荷プロセス：（略） 運転プロセス：（略） 変更プロセス：（略） 廃止プロセス：（略） ソフトウェアライフサイクルプロセスには，下記の理由により，開発，保守プロセスを定義していない。

(h)開発プロセス：（略） (i)保守プロセス：（略） (2) 各プロセスで実施すべき品質管理項目 （略） (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 （略） (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 （略） (e) 運転プロセス （略） (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。 以上のプロセスの状態を参考図３に示す。 （図は略）	開発プロセス：（略） 保守プロセス：（略） (2) 各プロセスで実施すべき品質管理項目 （略） 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 （略） 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 （略） 5) 運転プロセス （略） 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・試験のプロセスに従う。 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。 以上のプロセスの状態を参考図３に示す。 （図は略）

（２）　日本電気協会による変更の理由

① 単体試験又はシステム試験のどちらかを実施すればよいように読めるため、記載を見直した。

② デジタル安全保護系規程 2008 等技術評価書の 5.2(1)「③「4.18.1 ソフトウェアライフサイクル」の要望事項を反映した。

（３）　検討の結果

① 試験プロセスにおいて、ソフトウェア単体では確認できない内容をシステムとして確認する範囲について事前に計画することは品質保証活動として当然のことであり妥

当と判断する。

「(解説-19) ソフトウェアライフサイクル」の「(2)各プロセスで実施すべき品質管理項目　(a)設計プロセス」において、「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。」と規定しているが、技術基準規則解釈第３５条第１号に規定する「安全保護装置の機能の確認については、設置許可申請書の添付書類八の設備仕様及び設置許可申請書において評価した運転時の異常な過渡変化の評価の条件に非保守的な変更がないことを確認する」に対応する規定を明確にすることを要望する。

② デジタル安全保護系規程 2008 等技術評価書において、「廃止プロセスの品質管理項目は、「ソフトウェアが廃止され、誤って再使用されることのない措置をとる」ことと考える」と評価し、「廃止プロセスを分かりやすく定義すること」を要望している。デジタル安全保護系規程 2020 の規定内容は、誤って再使用されることのない措置について具体化したものであり、妥当と判断する。

技術基準規則解釈において、デジタル安全保護系規程 2008 の「(解説-14)」は同規格の適用に当たっての条件とされていたことから、デジタル安全保護系規程 2008 の「(解説-14)」は「4.18.1 ソフトウエアライフサイクル」に加え、デジタル安全保護系規程 2020 の「(解説-19) ソフトウェアライフサイクル」(参考図３を除く。) は「4. 19.1 ソフトウエアライフサイクル」に加える。

（４） 適用に当たっての条件

①なし

②

読み替える規定	読み替えられる字句	読み替える字句
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。 （解説-19）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 ディ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。	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。

	(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 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。 (h)開発プロセス：製品を製作する前の研究，試作等であり，製品設計とは直結しないプロセスである。 (i)保守プロセス：ソフトウェアの保守としては実施する内容がない。なお，システムの保守としては定期検査時の試験がある。 (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。	(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 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。 (h)開発プロセス：製品を製作する前の研究，試作等であり，製品設計とは直結しないプロセスである。 (i)保守プロセス：ソフトウェアの保守としては実施する内容がない。なお，システムの保守としては定期検査時の試験がある。 (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。 以上のプロセスの状態を参考図３に示す。 （図は略）	(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。 （削る）

（５） 要望事項

○「(解説-19) ソフトウェアライフサイクル」の「(2)各プロセスで実施すべき品質管理項目 (a)設計プロセス」において、「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。」と規定しているが、技術基準規則解釈第３５条第１号に規定する「安全保護装置の機能の確認については、設置許可申請書の添付書類

八の設備仕様及び設置許可申請書において評価した運転時の異常な過渡変化の評価の条件に非保守的な変更がないことを確認する」に対応する規定を明確にすることを要望する。

４．１．９　検証及び妥当性確認（V&V）と品質保証

検証及び妥当性確認（V&V）については、「4.19.3 V&V」、「(解説-21) V&V（手順)」、「(解説-22) V&V（独立性)」及び「(解説-23) V&V（文書化)」に規定している。品質保証については「4.19 品質保証」及び「(解説-18) 品質保証活動」に規定している。

（１）　変更の内容（「表 4.1.9 -1　検証及び妥当性確認（V&V）に関する規定内容の変更点」参照）

① V&V を行う体制を「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」から「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」に変更した。(4.19.3 V&V)

② ディジタル安全保護系の供給者に対する品質保証活動を要求した。((解説-21) V&V（手順))

③ V&V としての検証は設計プロセス及び製作プロセス、V&V としての妥当性確認は試験プロセスと明確化した。((解説-21) V&V（手順))

④ V&V を実施する個人又はグループの力量及び経済面、工程管理に関する制約を受けないことを追加した。((解説-22) V&V（独立性))

⑤ V&V に係る文書は構成管理計画の中で保存及び管理することを追加した。((解説-23) V&V（文書化))

表 4.1.9 -1　検証及び妥当性確認（V&V）に関する規定内容の変更点

デジタル安全保護系規程 2020	デジタル安全保護系規程 2008
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。 (解説-21) 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，	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れ，再利用の妥当性を示す根拠が文書化されていること。 (解説-16)

ディジタル安全保護系の供給者は，「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]」に従った一般の品質保証活動を実施した上で，ディジタル安全保護系のソフトウェアに対しV&V 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」を参照する。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，参考図３に示す設計，製作，試験及び変更がある。 （解説-22）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。 （解説-23）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。	検証及び妥当性確認については，「ディジタル安全保護系の検証及び妥当性確認に関する指針：JEAG 4609-2008」を参照する。新規設計や変更により検証及び妥当性確認が必要なプロセスとして，設計，製作，試験，変更を対象とする。 なお，ソフトウェアライフサイクルプロセスにおける検証及び妥当性確認の対象を参考図３に示す。 （解説-17） 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。 (1)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。 (2)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。 （解説-18） 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。

（２）　日本電気協会による変更の理由

① JEAC4111／JEAG4121 の一般の品質保証における「検証と妥当性確認」と区別するために、JEAG4609 に示す「検証と妥当性確認」は「V&V」と表記した。「検証」と「妥当性確認」は、各プロセスに応じて実施することが分かるように本文及び解説を見直した。「組織」を「個人又はグループ」に変更した。

② 一般の品質保証活動と V&V との関係を追記した。

③ デジタル安全保護系規程 2008 の記載では、すべてのプロセスにおいて、「検証」と「妥当性確認」の両方の実施が必要であるように解釈されかねないため、デジタル安全

保護系規程 2020 ではそれぞれをどのプロセスで実施すべきかを明記した[50]。

④　デジタル安全保護系規程 2008 の(1)の V&V を実施する組織と(2)の V&V の実施を管理する組織とが別でなければならないようにも読めるため、「V&V を実施する個人又はグループ」に表現を統一した。また、(1)は技術的な独立性を有すること、(2)は経済面や工程管理面の制約を受けないことを明記した。

⑤　デジタル安全保護系規程 2008 等技術評価書の 5.1(1)「②検証及び妥当性確認」の適用条件を反映した。

（３）　検討の結果

①　「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る。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」が発行されている（制定：1996 年、改訂 2007 年、2012 年)。同規格の規定との違いについて、日本電気協会は次のように説明している[51]。

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，

[50] 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　資料２－１　回答 1.13)

[51] 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　資料１－２　回答 1.14)

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）

日本電気協会は、ソフトウェアの品質保証活動を行うに当たり「JIS X 0160:2021 ソフトウェアライフサイクルプロセス」を参考にすることができるとしている。ソフトウェアの品質保証に関する JIS 規格は国際規格との整合性をとったものである。JIS 規格の利用を前提として、デジタル安全保護系のソフトウェアの品質保証への適用に当たり必要な規定の追加及び不都合な規定の除外をする方法も考えられる。

また、「4.19.3 V&V」には、V&V に関する要件として(1)～(3)に実施体制の独立性、文書化、再利用が規定されているが、V&V として何を実施すれば十分とみなせるか、基本的な事項が規定されていない理由について、日本電気協会は次のように説明している[52]。

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

[52] 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　資料１－２　回答 1.15)

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。

また、V&V について、デジタル安全保護系 V&V 指針 2020 によることと規定しなかった理由について、日本電気協会は、次のように説明している[53]。

JEAC4620 では，基本的な品質保証活動に加えて V&V 活動を実施することを要求しています。

この V&V の実施方法は，ガイドラインである JEAG4609 の趣旨に沿った形で，また，実際の V&V 対象の仕様等を踏まえて個別に具体化することを想定しています。

実際に，V&V の対象となる設備の種類や設計・制作にあたる組織の構成などによって設計の手順や関連する図書の構成などが異なってくることから，JEAG4609 では典型的な設計のステップを例示して V&V の内容を解説しています。

したがって，V&V の実施にあたっては，JEAG4609 を参照しながら具体的な V&V 計画を適切に立案し実行することになります。

技術基準規則解釈第３５条第４号は「「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。」として、デジタル安全保護系V&V指針2008によるV&Vの実施を求めている。これは、デジタル安全保護系規程2008にV&Vに関する基本的な要件の記載がないため、技術基準規則解釈に直接引用したものである。

デジタル安全保護系規程2020においても、本文にV&Vの実施を求める記載はあるが、V&V として実施すべき事項（内容）は網羅されておらず、解説においてデジタル安全保護系 V&V 指針 2020 を参照するとの記載に留まっている。

したがって、デジタル安全保護系規程 2020 を用いる際には、デジタル安全保護系 V&V 指針 2020 により V&V を実施されるよう、「4.19.3 V&V」に「V&V は、JEAG4609-2020 による。」を加える。

---

[53] 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　資料２－１　回答 1.10）

デジタル安全保護系規程 2008 では、「(解説-16)」において「新規設計や変更により検証及び妥当性確認が必要なプロセスとして，設計，製作，試験，変更を対象」としていたが、デジタル安全保護系規程 2020 では、「(解説-21) V&V（手順)」において、V&V としての検証は設計プロセス及び製作プロセス、V&V としての妥当性確認は試験プロセスと、検証と妥当性確認が区別されている。その理由について、日本電気協会は、上記（２）③に記載のとおり全てのプロセスにおいて、「検証」と「妥当性確認」の両方の実施が必要であるように解釈されかねないためとしている。

また、「設計，製作，試験，変更」のうちの「変更」はデジタル安全保護系規程2020では、検証と妥当性確認のどちらに区分されるのか、また、「(解説-19) ソフトウェアライフサイクル」の「(2)各プロセスで実施すべき品質管理項目」において「(f)変更プロセス」に規定する「ソフトウェアの変更要否について調査する。」に対するV&Vは行うのかについて、日本電気協会は、次のように説明している[54]。

> *変更プロセスについては，(解説-19) に示すように変更の要否を調査する段階であり，実際の変更内容は設計，製作及び試験におけるそれぞれのプロセスに従うため，V&V としては変更プロセスそのものは対象から外しています。変更の決定を受けて変更内容は設計・製作の図書に反映され，基本的な原子力品質保証活動に基づき，設計チームにて設計検証，妥当性確認が実施されます。さらに変更内容が反映された設計・製作の図書に対して V&V を行います。例えば変更箇所が上位図書の要件から相違がないことの検証等を含めて V&V として確認しています。また，V&V によって変更内容が上位図書の要件に不適切であることが分かった場合などには設計・製作者に対して是正を求めるような活動を実施しています。*

ソフトウェアの変更要否について調査した結果、否としたものについては設計プロセスから外れることになる。調査の判断が間違っていた場合には、変更内容はソフトウェア設計仕様に反映されないが、判断の妥当性はどのように確認するのか、また、その結果に対する V&V は行う必要がないのかなど課題は残る。したがって、「ソフトウェアの変更要否について調査する」に対する V&V を明確にすることを要望する。

「検証」及び「妥当性確認」は各プロセスに応じて実施することが分かるように、各プロセスに応じて実施する旨明確化したこと及び「組織」を「個人又はグループ」に変更したことは妥当と判断する。

① デジタル安全保護系の供給者は、「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]」に従った一般の品質保証活動を実施した上で、デジタル安全保護系のソフトウェアに対し V&V を実施することを明確化したものである。同規程及び指針は「(解説-21) V&V(手順)」において新規追加されたが、「(解説-18) 品質保証活動」においては名称変更及び年版変更に該当する（添付資料－２　引用規格の変更に関する確認結果の「１．デジタル安全保護系規程 2020 における関連規格のデジタル安全保護系規程 2008 からの変更に関する確認結果」参照)。

[54] 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　資料３－２　回答 1. 13)

「(解説-18) 品質保証活動」を引用している「4.19 品質保証」は次のように規定している。

> 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。(解説-18)
> ・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
> (解説-18) 品質保証活動
> ディジタル安全保護系の品質保証活動については，「原子力安全のためのマネジメントシステム規程：JEAC 4111-2013」及び「原子力安全のためのマネジメントシステム規程（JEAC 4111-2013）の適用指針：JEAG 4121-2015[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」を参照する。
> 市販ディジタル計算機，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）

(a) ソフトウェアの品質保証

ソフトウェアの品質保証については、「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。」と規定しているが、日本電気協会の説明によれば、「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」の品質保証について規定しており、それ以外のソフトウェアの品質保証について規定していない。その理由について、日本電気協会は次のように説明している[55]。

> *ソフトウェアに関しては，品質保証活動の中で信頼性を担保しております。ここで，本規定の適用範囲については資料３－２の回答１．３）で記載の通り，核計装や放射線モニタを検出器として取り扱っており，本規程におけるディジタル計算機としての要求適用範囲外としておりますので，核計装や放射線モニタにソフトウェアが適用される場合，そのソフトウェアに関しては JEAC4111/JEAG4121 で規定されている原子力の通常の品質保証活動の中で信頼性を担保することとなります。一方で，資料３－２の回答１．３）で記載した「原子炉停止系及び工学的安全施設作動系の演算・論理回路を実装するソフトウェア」に対しては，原子力の通常の品質保証活動に加えて，本規定で V&V の実施を要求しております。*

保安活動については、「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」第４条第２項において、「原子力事業者等は、保安活動の重要度に応じて、品質マネジメントシステムを確立し、運用しなければならない。」と規定している。このため、保安活動にかかる「4.19 品質保証」は、「原子炉停止系及び工学的

[55] 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　資料３－２　回答 1.3①)

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」かどうかではなく、安全保護装置全体の保安活動の重要度に応じて実施されるべきものである。このため、これらについて「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」に対してのみ対象とするのは妥当ではない。

また、「4.19 品質保証」には、ソフトウェアの健全性を確保する手法として二つの手法が列記されているが、手法を限定する必要はなく、保安活動の重要度に応じて健全性を確保できる手法であればよい。また、「4.17　ソフトウェアの管理外の変更の防止」は、「原子炉停止系及び工学的安全施設作動系の演算・論理回路を実装したアプリケーションのソフトウェア」だけでなくソフトウェアであれば、変更は管理されるべきものである。

したがって、「4.19 品質保証」はデジタル安全保護系を構成する全てのソフトウェアを対象に、保安活動の重要度に応じて実施することとし、「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」とあるのは、「保安活動の重要度に応じ，以下に掲げる事項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」と読み替える。

また、「4.17 ソフトウェアの管理外の変更の防止」の「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。」は、「デジタル安全保護系のデジタル化された演算・論理処理部に装荷するソフトウェア（以下単に「ソフトウェア」という。）は，管理外の変更を防止する設計とすること。」と読み替える。

また、技術基準規則解釈において、デジタル安全保護系規程 2008 の「(解説-12)」は同規格の適用に当たっての条件とされていたことから、、デジタル安全保護系規程 2008 の「(解説-12)」は「4.17 ソフトウェアの管理外の変更に対する防護措置」に加え、ディジタル安全保護系規程 2020 の「(解説-16) ソフトウェアの管理外の変更の防止」は、「4.17 ソフトウェアの管理外の変更の防止」に加える。

なお、規定文中の「ディジタル計算機」については、4.1.1(4)①(a)において、「ディジタル計算機」は「デジタル安全保護系のデジタル化された演算・論理処理部」と読み替えることにしたので、「ディジタル安全保護系に用いられるディジタル計算機」とあるのは、「ディジタル安全保護系に用いられるデジタル化された演算・論理処理部」と読み替える。

(b) 「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]」に関する評価

品質保証活動について、原子力規制委員会は、「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」及び同解釈を制定し、令和 2 年 4 月 1 日から施行している。用語の定義である「3.3 V&V」及び「(解説-18) 品質保証活動」の「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]」は、同規則及び解釈が制定される以前に発行された規格であり、同規則及び解釈の要求事項との関係が明らかでない。したがって、「3.3 V&V」の「「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]」に基づいた品質保証活動」とあるのは、「「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」と読み替える。

また、「4.19 品質保証」にソフトウェアの健全性を確保する手法の一つとして規定する「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」は、「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（「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）」と読み替える。同様に、技術基準規則解釈において、デジタル安全保護系規程 2008 の「（解説-13）」は、同規格の適用に当たっての条件とされていたことから、デジタル安全保護系規程 2020 の「（解説-18） 品質保証活動」は「4.19 品質保証」に加えるが、「ディジタル安全保護系の品質保証活動については，「原子力安全のためのマネジメントシステム規程：JEAC 4111-2013」及び「原子力安全のためのマネジメントシステム規程（JEAC 4111-2013）の適用指針：JEAG 4121-2015[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」を参照する。」は削る。

技術基準規則解釈において、デジタル安全保護系規程 2008 の「（解説-16）」は、同規格の適用に当たっての条件とされていたことから、デジタル安全保護系規程 2008 の「（解説-16）」は「4.18.3 検証及び妥当性確認」に加え、デジタル安全保護系規程 2020 の「（解説-21）V&V（手順）」の「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，ディジタル安全保護系の供給者は，「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]」に従った一般の品質保証活動を実施した上で，ディジタル安全保護系のソフトウェアに対し V&V を実施する。」は「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した上で，デジタル安全保護系のデジタル化された演算・論理処理部に装荷する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を制御するソフトウェアを除いたものに対し V&V を実施する。」と読み替え、読替え後の「（解説-21）V&V（手順）」の内容を「4.19.3 V&V」に加える。

なお、読替前の「（解説-18） 品質保証活動」において、「ディジタル安全保護系の品質保証活動については，「原子力安全のためのマネジメントシステム規程：JEAC 4111-2013」及び「原子力安全のためのマネジメントシステム規程（JEAC 4111-2013）の適用指針：JEAG 4121-2015[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」を参照する」と規定しているが、「4.19 品質保証」には「（略）ソフトウェアの健全性を確保すること」と規定しており、ソフトウェア以外のものに対する品質保証の要求は規定されていない。本文がソフトウェアのみに限定した規定では、それ以外のものについては何も要求されないと誤解される恐れもあることから、本文にソフトウェア以外のものに対する品質保証の要求を明確化することを要望する。

③ 設計プロセス及び製作プロセスにおける V&V は検証、試験プロセスにおける V&V は妥当性確認と、検証と妥当性確認との違いを踏まえて規定を明確化したものであり、妥

当と判断する。

④ 「V&V を実施する個人又はグループ」が中立的立場で V&V を実施できるためには、技術的な独立性と経済面や工程管理面の制約を受けないことが重要であり、変更は妥当と判断する。技術基準規則解釈において、デジタル安全保護系規程 2008 の「(解説-17)」は、同規格の適用に当たっての条件とされていたことから、デジタル安全保護系規程 2008 の「(解説-17)」は「4.18.1 検証及び妥当性確認」に加え、デジタル安全保護系規程 2020 の「(解説-22) V&V (独立性)」は「4.19.3 V&V」に加える。

⑤ デジタル安全保護系規程 2008 等技術評価書の 5.1(1)デジタル安全保護系規程「②検証及び妥当性確認」の適用に当たっての条件は下記としている。

> 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。

これを受けて、技術基準規則解釈 第３５条第４号（２）には、以下のように規定されている。

> （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。

「(解説-23) V&V (文書化)」は上記を反映したものであり、妥当と判断する。

技術基準規則解釈において、デジタル安全保護系規程 2008 の「(解説-18)」は、同規格の適用に当たっての条件とされていたことから、デジタル安全保護系規程 2008 の「(解説-18)」は「4.18.3 検証及び妥当性確認」に加え、デジタル安全保護系規程 2020 の「(解説-23) V&V (文書化)」は「4.19.3 V&V」に加える。

（４） 適用に当たっての条件

①～⑤

読み替える規定	読み替えられる字句	読み替える字句
3.3 V&V	Verification and Validation の略。ディジタル安全保護系のソフトウェアに対して，「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]」に基づいた品質保証活動を前提にして，設計，製作及び試験に携わった者以外の個人又はグループが実施する検証及び妥当性確認。	Verification and Validation の略。デジタル安全保護系のソフトウェアに対して，「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前提にして，設計，製作及び試験に携わった者以外の個人又はグループが実施する検証及び妥当性確認。
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。 （解説-16）ソフトウェアの管理外の変更の防止	デジタル安全保護系のデジタル化された演算・論理処理部に装荷するソフトウェア（以下単に「ソフトウェア」という。）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	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
4.19 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 (解説-18)品質保証活動 ディジタル安全保護系の品質保証活動については，「原子力安全のためのマネジメントシステム規程：JEAC 4111-2013」及び「原子力安全のためのマネジメントシステム規程（JEAC 4111-2013）の適用指針：JEAG 4121-2015[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」を参照する。 市販ディジタル計算機，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	デジタル安全保護系に用いられるデジタル化された演算・論理処理部は，保安活動の重要度に応じ，以下に掲げる事項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（「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） ・V&V 活動 (削る) 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)	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)
4.19.3 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。 (解説-21) 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，ディジタル安全保護系の供給者は，「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]」に従った一般の品質保証活動を実施した上で，ディジタル安全保護系のソフトウェアに対し V&V 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」を参照する。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，参考図３に示す設計，製作，試験及び変更がある。 (解説-22) V&V（独立性） ソフトウェアの設計，製作及び	デ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。 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した上で，デジタル安全保護系のデジタル化された演算・論理処理部に装荷する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を制御するソフトウェアを除いたものに対し V&V 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

	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。 （解説-23）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。	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。

（５） 要望事項

○ 「ソフトウェアの変更要否について調査する」に対する V&V を明確にすることを要望する。

○ 品質保証の要求がソフトウェアのみに限定した規定では、それ以外のものについては何も要求されないと誤解される恐れもあることから、本文にソフトウェア以外のものに対する品質保証の要求を明確化することを要望する。

４．１．１０ ソフトウェアの構成管理

ソフトウェアの構成管理については、「4.19.2 ソフトウェアの構成管理」及び「(解説-20) ソフトウェアの構成管理」に規定している。

（１） 変更の内容（「表 4.1.10-1 ソフトウェアの構成管理に関する規定内容の変更点」参照）

① 構成管理の対象に V&V 手順及び V&V 結果を追加し、ソフトウェア供給者に対する監査又は審査をソフトウェア構成管理のレビュー又は審査に変更した。

② ソフトウェア及び関連文書について、管理対象要素の例に「V&V 手順／V&V 結果」を追加した。

表 4.1.10-1 ソフトウェアの構成管理に関する規定内容の変更点

デジタル安全保護系規程 2020	デジタル安全保護系規程 2008
4.19.2 ソフトウェア構成管理 (略) （解説-20）ソフトウェアの構成管理 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	4.18.2 ソフトウェア構成管理 (略) （解説-15） 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

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。 　具体的には以下に示す。 (1) （略） (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。	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) （略） (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。

（２）　日本電気協会による変更の理由

① 構成管理が確実に実施さていることの確認は、外部のソフトウェア供給者に対してのみ実施すればよいものではなく、ソフトウェア構成管理全般のレビュー又は審査の実施に変更した。

② デジタル安全保護系規程 2008 等技術評価書の 5.1(1)「②検証及び妥当性確認」の適用条件の反映（解説-21 参照）に関連して、構成管理要素として V&V の文書の健全性確認の文書を追加した。

（３）　検討の結果

① 「ソフトウェア供給者に対する監査」を削除したことは、供給者以外にも審査の対象を拡大したものであり、妥当と判断する。

② 管理対象要素の例に「V&V 手順／V&V 結果」を追加したことは、４．１．９項の（３）⑤と同様であり、妥当と判断する。

技術基準規則解釈において、デジタル安全保護系規程 2008 の「(解説-15)」は、同規

格の適用に当たっての条件とされていたことから、デジタル安全保護系規程 2008 の「(解説-15)」は「4.18.2 ソフトウェア構成管理」に加え、デジタル安全保護系規程 2020 の「(解説-20) ソフトウェアの構成管理」は「4.19.2 ソフトウェア構成管理」に加える。

（4） 適用に当たっての条件

①②

読み替える規定	読み替えられる字句	読み替える字句
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。 （解説-20）ソフトウェアの構成管理 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。 (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	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。 (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。	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。

４．１．１１　環境条件の考慮

環境条件の考慮については、「4.9 外的要因」及び「(解説-10) 外的要因（関連規格・指針)」に規定している。

（１）　変更の内容（「表 4.1.11-1　環境条件の考慮に関する規定内容の変更点」参照）

① 外的要因に対する設計の確証規定を追加した。

② 耐サージ性に関する「原子力発電所の耐雷指針：JEAG4608-2007」を削除した。

② 溢水防護上の措置をその他の外的要因に追加し、解説に参照規格として「原子力発電所の内部溢水影響評価ガイド：平成 25 年 6 月 19 日原子力規制委員会決定」を追加した。

④ 耐震性に関する規格を「原子力発電所耐震設計技術指針[重要度分類・許容応力編]：JEAG4601・補-1984」から「原子力発電所耐震設計技術規程：JEAC4601-2015」に変更した。

⑤ 火災防護の規格に「原子力発電所の火災防護規程：JEAC4626-2010」及び審査基準を追加した。

表 4.1.11-1　環境条件の考慮に関する規定内容の変更点

デジタル安全保護系規程 2020	デジタル安全保護系規程 2008
4.9 外的要因 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 4.9.2 耐震性 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を有すること。 4.9.3 その他の外的要因	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。

ディジタル安全保護系は，火災防護上の措置及び溢水防護上の措置を考慮した設計とすること。 4.9.4 設計の確証 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ディジタル安全保護系が機能を維持できることを確証すること。 （解説-10）外的要因（関連規格・指針） 耐震性，火災防護上の措置及び溢水防護上の措置については，以下の規格，指針を参照する。 耐震性：「発電用原子炉施設に関する耐震設計審査指針：平成 18 年 9 月 19 日原子力安全委員会決定」，「原子力発電所耐震設計技術規程：JEAC4601-2015」 火災防護上の措置：「発電用軽水型原子炉施設の火災防護に関する審査指針：昭和 55 年 11 月 6 日原子力安全委員会決定，一部改訂平成 19 年 12 月 27 日原子力安全委員会」，「原子力発電所の火災防護規程：JEAC4626-2010」，「原子力発電所の火災防護指針：JEAG4607-2010」，「実用発電用原子炉及びその附属施設の火災防護に係る審査基準：平成 25 年 6 月 19 日原子力規制委員会決定」 溢水防護上の措置：「原子力発電所の内部溢水影響評価ガイド：平成 25 年 6 月 19 日原子力規制委員会決定」	（解説-8） 耐震性，耐サージ性，火災防護上の措置については，以下の規格，指針を参照する。 耐震性：「発電用原子炉施設に関する耐震設計審査指針：平成 18 年 9 月 19 日原子力安全委員会決定」，「原子力発電所耐震設計技術指針〔重要度分類・許容応力編〕：JEAG4601・補-1984」 耐サージ性：「原子力発電所の耐雷指針：JEAG4608-2007」 火災防護上の措置：「発電用軽水型原子炉施設の火災防護に関する審査指針：昭和 55 年 11 月 6 日原子力安全委員会決定，一部改訂平成 19 年 12 月 27 日原子力安全委員会」，「原子力発電所の火災防護指針：JEAG4607-1999」

（2） 日本電気協会による変更の理由

① デジタル安全保護系規程 2008 等技術評価書の 5.1(1)「③環境条件」の適用に当たっての条件を反映した。

② 耐雷指針については、安全保護系に特化した要求ではないため、削除した。

③ 溢水防護に関する評価ガイドを追加した。

④ 国内規格の最新版に見直した。

⑤ 火災防護の規程を国内規格の最新版に見直し、審査基準を追加した。

（3） 検討の結果

① デジタル安全保護系規程 2008 等技術評価書の 5.1(1)デジタル安全保護系規程「③環境条件」の適用に当たっての条件は下記としている。

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。

これを受けて、技術基準規則解釈 第３５条第４号（３）には、以下のように規定されている。

（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。

「4.9.4 設計の確証」は上記を踏まえ対象範囲を拡大して追加したものである。「4.9.1 及び 4.9.2 で要求された設計」について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規定しており、上記適用に当たっての条件は、デジタル安全保護系規程 2008 の技術評価において、発電用原子力設備に関する技術基準を定める省令の解釈について（平成 17・12・15 原院第 5 号　経済産業省原子力安全・保安院 NISA-322c-05-7、平成 17 年 12 月 16 日）の「ディジタル安全保護系を適用するに当たっての要求事項（別記-7）に規定された次の要件に基づき付されたものである。

４．ディジタル安全保護系は、次の環境条件下においても、その条件を考慮して設計し、機能が実証されていること。
（ａ）想定される温度、湿度、放射線量
（ｂ）想定される電源擾乱、電磁波、アース線等を通じた落雷等の外部からの外乱・ノイズ。

「4.9.4 設計の確証」は上記を反映したものであり、妥当と判断する。

「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は、要求されていない。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」としている[56]。

（解説-11）外的要因（設計の確証）
確証することとは，型式試験，使用実績，解析，又はこれらを組み合わせること等により，それぞれの外的要因に対してディジタル安全保護系が機能を維持できることを確認することをいう。
なお，4.9.3 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、確証の対象外である。

その理由について、日本電気協会は次のように説明している[57]。

「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

[56] 設計の確証を「機能維持」の確証ではなく、「耐力」の確証としている。
[57] 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　資料１－２　回答 1.10）

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。

環境条件や耐震性については、デ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ること、他方、火災防護及び溢水防護については、デ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あることから、これらに対す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としていることは、妥当と判断する。

② 「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」が規定されているが、（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ない。達成すべき水準（具体的な規格基準等）について日本電気協会は次のように説明している[58]。

本規程はディジタル安全保護系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。

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・ノイズへの対策を含む、環境条件に対する達成すべき水準を明確にしなければ、これらを考慮し、対策を取ることができない。デジタル安全保護系規程 2008 では、耐雷指針を引用していたが、改訂により削除されている。「環境条件に対する達成すべき水準」を考慮した設計となっているかを、どのように判断するのかについて、日本電気協会は次のように説明している[59]。

電磁的な外乱・ノイズ等に対して計測制御装置に施す設計上の考慮事項は，フィルタや接地など，原子力発電所の設備に限らず，一般産業の設備と共通的なものです。そのため，ディジタル安全保護系の設計に際しても，設置条件等を踏まえつつ，一般的な規格，基準を適宜活用することで十分に対応できると認識しています。よって本規程においては，これらの外乱・ノイズに対して原子力固有の考慮事項を記載する必要はないと考え，具体的な規格・基準を指定しないこととし，2020 年版では耐雷指針の引用もしておりません。

---

[58] 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　資料３－１　回答 1.9)

[59] 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　資料２－１　回答 1.4)

なお IEEE323 では，耐環境試験の条件を定める際に考慮する「通常時及び異常時の運転条件の一例」として電磁的な影響や電力サージも含まれていますが，同規格では，通常時や事故時の環境が厳しくない設置環境にある設備への耐環境試験を要求していないことから，上記の対応と整合するものと考えております。

日本電気協会は、耐雷指針について「安全保護系に特化した要求ではないため、削除した」としているが、上記②に記載する外乱・ノイズ対策は必要である。また同協会からは改定した「原子力発電所の耐雷指針：JEAG4608-2020」がデジタル安全保護系規程 2020 と同日に発刊されている。さらに、環境条件に対する設計の要件の国際的な動向として、原子力施設の一般的な環境条件については IEC/IEEE 60780-323[60]、電磁両立性については IEC 62003[61]、EPRI TR-102323[62]等の具体的な規格基準類が整備されている例がある。以上のように、環境条件に関する要件としては、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・ノイズへの対策を含む、環境条件に対する達成すべき水準を明確にした上で、その達成すべき水準に対する設計の適切性を確認する必要がある。したがって、「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。」に「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。」を加える。

③④⑤　技術基準規則解釈において、デジタル安全保護系規程 2008 の「(解説-8)」は、同規格の適用に当たっての条件とされている。「(解説-10) 外的要因（関連規格・指針)」には、溢水防護上の措置に参照する関連文書として「原子力発電所の内部溢水影響評価ガイド」が引用されており、同ガイドは原子力規制委員会の審査ガイドである。耐震性については、設置許可基準規則解釈別記２において地震による損傷の防止が規定され、具体的な要求は「耐震設計に係る設工認審査ガイド」に規定されている。変更された「原子力発電所耐震設計技術規程：JEAC 4601-2015」は上記ガイドに記載されておらず、デジタル安全保護系規程 2008 に規定する「原子力発電所耐震設計技術指針[重要度分類・許容応力編]：JEAG 4601・補-1984」が記載されている。また、旧原子力安全委員会決定の「発電用原子炉施設に関する耐震設計審査指針」は上記別記２及び「耐震設計に係る設工認審査ガイド」に引用されていない。火災防護については、「実用発電用原子炉及びその附属施設の火災防護に係る審査基準」が引用されており、「原子力発電所の火災防護規程：JEAC4626-2010」及び「原子力発電所の火災防護指針：JEAG4607-2010」は同審査基準において引用されている。これらの文書を参考とすることに問題はないといえる。技術基準規則解釈において、デジタル安全保護系規程 2008 の「(解説-8)」は、同規格の適用に当たっての条件とされていたが、同解説は参考とする文書に関する解説であることから、デジタル安全保護系規程 2020 の「(解説-10) 外的要因（関連規格・指針)」は技術基準規則解釈に引用しないこととし、デジタル安全保護系規程 2008 の「(解説-8)」も引用しないこととする。

---

[60] IEEE/IEC 60780-323-2016, IEC/IEEE International Standard - Nuclear facilities -- Electrical equipment important to safety -- Qualification

[61] IEC 62003:2020, Nuclear power plants - Instrumentation, control and electrical power systems - Requirements for electromagnetic compatibility testing

[62] TR-102323, Guidelines for Electromagnetic Interference Testing of Power Plant Equipment

（4） 適用に当たっての条件

①なし

②③④⑤

読み替える規定	読み替えられる字句	読み替える字句
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。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
4.9.2 耐震性	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を有すること。	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を有すること。
4.9.3 その他の外的要因	ディジタル安全保護系は，火災防護上の措置及び溢水防護上の措置を考慮した設計とすること。	デジタル安全保護系は，火災防護上の措置及び溢水防護上の措置を考慮した設計とすること。

４．１．１２　健全性を実証できない場合の原理の異なる手段の設置

健全性を実証できない場合の原理の異なる手段の設置については、「5.留意事項」に規定している。

（1） 変更の内容（「表 4.1.12-1　健全性を実証できない場合の原理の異なる手段の設置に関する規定内容の変更点」参照）

① 「ディジタル安全保護系は，「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，共通要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考えられる」との記載を追加し、「ハードウェア設備」を「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」に変更した。

表 4.1.12-1　健全性を実証できない場合の原理の異なる手段の設置に関する規定内容の変更点

デジタル安全保護系規程 2020	デジタル安全保護系規程 2008
5.留意事項 ディジタル安全保護系は，「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，共通要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考えられるが，深層防護の観点から，合理的な範囲で，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	5.留意事項 深層防護の観点から，より一層の信頼性向上を図るため，原子炉設置者が合理的な範囲でハードウェア設備を設けること。

される。	

（2） 日本電気協会による変更の理由

① 本規程の要求事項を満足することで、高品質で信頼度が高く、共通要因故障発生の可能性が十分低くなることを明記した。そのうえで深層防護の観点から追加する設備は、適用技術がハードウェアである必要はなく、ディジタル安全保護系との多様性が確保されていれば良いことを明記した。

（3） 検討の結果

① 「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」とある。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（(解説-24) 参照）があげられるが、その要求が規定されていない。

(解説-24) 動作原理等の異なる追加の設備

ここで示す追加の設備の範囲は「止める（原子炉の緊急停止)」,「冷やす（炉心の冷却)」,「閉じ込める（放射能の外部放出防止)」の必要な機能とする。

本設備は，ハードワイヤード回路の他，ディジタル安全保護系とは異なるディジタル制御装置で構成することも考えられる。

本設備の故障によりディジタル安全保護系の安全機能に影響を与えない限りにおいて，本設備には安全保護系以外の設備も適用可能である。

本設備の具体例として以下がある。

＜ＢＷＲ＞

・手動スクラム操作

中央制御室の手動スクラムスイッチからソフトウェアを介さずに主トリップ継電器回路にハードワイヤード回路で接続する。

・高圧炉心注水系の手動操作

中央制御室の手動スイッチからソフトウェアを介さずにポンプの作動回路にハードワイヤード回路で接続する。

・主蒸気隔離弁及び主要な隔離弁の手動閉止操作

中央制御室の手動スイッチからソフトウェアを介さずに弁の作動回路にハードワイヤード回路で接続する。

・原子炉水位，ドライウェル圧力の監視

現場計器からの信号を，ソフトウェアを介さずに中央制御室にハードワイヤード回路で接続する。

＜ＰＷＲ＞

・手動原子炉トリップ

中央制御室の手動トリップスイッチからソフトウェアを介さずに原子炉トリップ遮断器を開放する不足電圧コイルにハードワイヤード回路で接続する。

・高圧安全注入系の手動操作

中央制御室の手動スイッチからソフトウェアを介さずにポンプの作動回路にハードワイヤード回路で接続する。

・主要な格納容器隔離弁の一括手動閉止操作

中央制御室の手動スイッチからソフトウェアを介さずに弁の作動回路にハードワイヤード回路で接続する。

・蒸気発生器水位，原子炉圧力の監視

現場計器からの信号を，ソフトウェアを介さずに中央制御室にハードワイヤー

ド回路で接続する。

「共通原因故障が発生する可能性は十分低い」とした理由について、日本電気協会は、次のように説明している[63]。

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が，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[64]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。

日本電気協会は、多様性について「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。」としている。一方で、安全保護系内部の多様性については、規格の適用範囲内と思われるにも係わらず、これについて規定していない理由について、日本電気協会

[63] 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 資料１－２ 回答 1.17)
[64] Programmable Digital Device

は、次のように説明している[65]

JEAC4620 は耐震性，耐環境性，ソフトウェアの信頼性等の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。

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，異なる設計のハードウェアを組み合わせてシステムを構築する等，内部の多様性を持たせることで共通要因故障を低減できる可能性があります。一方で，内部で多様性を持たせるということは，その多様な装置間の伝送等，新たな技術を必要とします。全く異なる設計の装置を組み合わせてシステムを構築するには，新たに詳細な設計調整を必要とし，場合によっては，この部分の設計ミスが信頼性低下の要因となる可能性があります。このため，内部の多様性を持たせるには十分な設計検討，場合によっては技術開発が必要となります。

JEAC4620 は海外規格を踏まえつつも，現状の国内のディジタル安全保護系設計を考慮して設定したものです。このため，現在又は近い将来に国内で導入されるディジタル安全保護系の設計を考慮した際に，その採用が技術的に現実的でないものについては記載しておりません（但し，採用を否定するものではありません）。異なる設計のハードウェアを組み合わせてシステムを構築する等，内部の多様性については，前記のような点も踏まえて，その採用がまだ技術的に現実的でないものと考えております。ディジタル安全保護系の設計については，現状の JEAC4620 における要求事項を満足することで十分に高い信頼性を確保できると考えており，内部の多様性については，海外動向，技術動向等を考慮しながら，今後，必要性も含めて検討していく部分と考えております。

なお，ディジタル安全保護系に限定したものではありませんが，安全保護系としては系統の多様性（高圧注水系，低圧注水系等），検出方法の多様性（原子炉水位，格納容器内圧力等）等も考慮されております。

技術基準規則３５条及び解釈では安全保護装置に対して多様性を求めるのは健全性を実証できない場合としている。したがって、デジタル安全保護系規程 2020 において多様性を求める要件としての記載がなく 5. 留意事項としての記載に留めているのは、現行規則へ適合している。

一方、国際的な動向としては、安全保護系について実用的な範囲の多様性を考慮することが求められている（例えば、米国連邦規則における Appendix A to Part 50-General Design Criteria for Nuclear Power Plants, Criterion 22)。ここで多様性は必ずしも追加の設備によるものではなく、安全保護系の内部においても可能な範囲で多様性を有するものとすることを含んでいる。また、多様性にはこうした設備的な多様性以外にも機能的多様性等の多くの属性があり、これらを実用的な範囲で適用することがソフトウエア共通要因故障の発生防止に寄与することが知られている （例えば U.S.NRC

[65] 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　資料２－１　回答 1. 11)

の NUREG/CR-6303[66]、7007[67]ほか)。

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が推奨される」とあり、「推奨される」の意味について日本電気協会は次のように説明している[68]。

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。

日本電気協会からの説明では、「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」はデジタル安全保護系に対する要求ではないため、推奨事項としているとしており、また、ATENA において技術要件書が作成されているため今後の動向を踏まえて必要に応じて検討するとしている。

したがって、本規程の適用にあたり 5. 留意事項は引用しない。一方で、安全保護系に関して考慮することが望ましい多様性について（必ずしも外部に設置する追加設備によらない、内部的な多様性を含む)、国内外の動向を踏まえた適切な記載内容を引き続き検討することを要望する。

（４） 変更点以外の検討

① デジタル安全保護系規程 2020 の巻頭言「「安全保護系へのディジタル計算機の適用に関する規程」について」においては、「IEEE 規格，IEC 規格等の最新の国内外における関連規格（中略）について調査を行い，その結果を踏まえて」改定したとしている。IEEE 規格，IEC 規格から本規程に反映した事項及び反映しなかった部分[69]の内容と理由について説明を求めたところ、日本電気協会は次のように回答している[70]。

---

[66] Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems

[67] Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems

[68] 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　資料１－２　回答 1.16)

[69] 例えば、以下の内容は、規程に反映されていない。
・手動操作回路（4.14 に機能の記載あり）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

[70] 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　資料１－２　回答 1.2)

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。

IEC 規格について調査を行ったとしていることに関し、具体的にどの IEC 規格（規格番号及び Edition 番号）について、どのような調査を行ったのか、日本電気協会は次のように説明している[71]。

JEAC4620 の 2008 年版制定及び 2020 年版改定のそれぞれの検討時において，以下の IEC 規格調査しています。これらは大枠では IEEE 7-4.3.2 に包含されているものと判断いたしました。また，従来より国内の原子力発電所の計装制御に関する規制，規格の多くは米国の規制，規格を参考にしている経緯もあり，最終的には IEEE7-4.3.2 をベースに検討することとしました。そのため以下 IEC 規格についてはそれぞれに記載されている要件については確認しましたが，JEAC4620 との項目対比は実施していません。

IEC 880-1986 Software for computers in the safety systems of nuclear power stations

IEC 60880-2-2000 Software for computers important to safety for nuclear power plants
Part2: Software aspects of defence common cause failures, use of software tools and of pre-developed software

IEC 60880-2006 Nuclear power plants
- Instrumentation and control systems important to safety
- Software aspects for computer-based systems performing category A functions

なお，上記の IEC 60880 等の他に，原子力発電所の重要な計測制御全般に対する規格である IEC 61513，分離指針を示している IEC 60709 等については，ディジタル安全保護系への要件を直接的に記載しているものではないため，参考として調査しています。

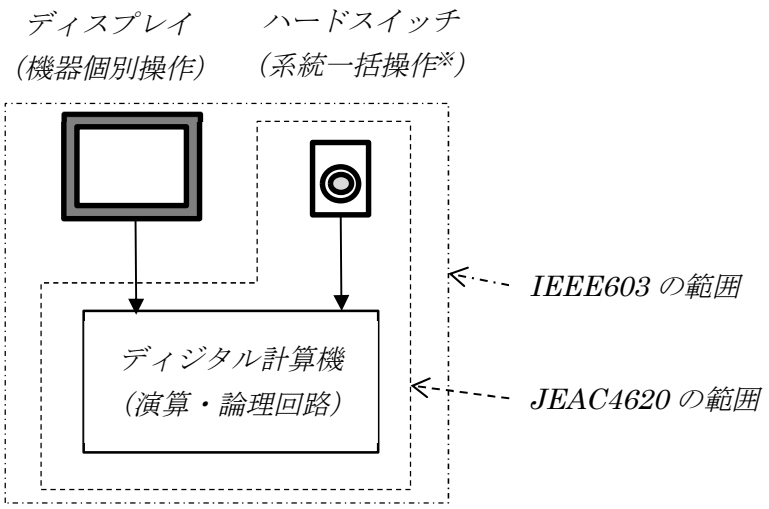
[71] デジタル安全保護系に関する日本電気協会規格の技術評価に関する検討チーム　資料２－１　回答 1.5)

IEEE603[72]等では手動操作系も含め広く安全系のソフトウェアが対象となるが、手動操作回路についてどのように対応したのか、また、規格・ガイドが対象とする設備及び技術の範囲を IEEE の最新版との比較について、日本電気協会は次のように説明している[73]。

国内のディジタル安全保護系に関する手動操作としては，ディスプレイによる機器個別操作（ポンプの起動／停止，弁の開／閉 等）とハードスイッチによる系統一括操作（原子炉停止，ＥＣＣＳ作動 等）に大別されます。原子炉停止系及び工学的安全施設系を作動させる設備として系統一括操作のハードスイッチは安全保護系相当であり，JEAC4620 の対象としています。系統一括操作のハードスイッチの信号はディジタル計算機に入力され，ディジタル計算機内の演算・論理回路を経て弁やポンプなどの起動信号として出力されます。一方，機器の個別操作のためのディスプレイは，ディジタル計算機による工学的安全施設作動系の演算・論理回路に含まれず，JEAC4620 の対象外としています。機器の個別操作のための操作信号や，安全保護系のブロックやリセットの操作信号は安全保護系を直接作動させるための操作信号ではありませんが，ディジタル計算機に入力され，原子炉停止系および工学的安全施設作動系の演算・論理回路において安全保護系が適切に作動できるようロジックが構成されています。なお，IEEE603-2018 は“safety system”を対象としており，機器個別操作も全て含まれていると考えます。

JEAC4620 の「4.14 手動操作」については，2008 年制定当時の安全保護系の規格である JEAG4604-1993 の要件を参照しています。IEEE603 の手動制御の項の中でこれ以外の要件として，操作部の設置場所や操作回数などの最少化などがありますが，これらは制御室の設計や誤操作防止対策などによるものと考え，JEAC4620 に反映しておりません。

[72] IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations
[73] 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　資料３－２　回答 1.2)



※：低圧注水系などを系統単位で起動できる操作

日本電気協会は、海外規格基準との比較について、IEEE7-4.3.2[74]（IEEE603 含む。）との比較を表(2)-1、表(2)-2 に示したとしているが、これらの表は項目単位の対比表であり、その内容の比較としては必ずしも十分ではない。特に、規格基準類の適用範囲について IEEE では操作スイッチ、検出器等を含む広い範囲の安全系設備を対象としているのに対し、デジタル安全保護系規程 2020 の適用範囲はこれに比べて限定的である。

国際標準との比較を実施する際は、項目ごとの整理表に留まらず、適用範囲及び詳細な内容についても整理することを要望する。

（5） 適用に当たっての条件

変更点

① なし

変更点以外

① なし

（6） 要望事項

○安全保護系に関して考慮することが望ましい多様性について（必ずしも外部に設置する追加設備によらない、内部的な多様性を含む)、国内外の動向を踏まえた適切な記載内容を引き続き検討することを要望する。

○国際標準との比較を実施する際は、項目ごとの整理表に留まらず、適用範囲及び詳細な内容についても整理することを要望する。

[74] IEEE Standard Criteria for Programmable Digital Devices in Safety Systems of Nuclear Power Generating Stations

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

４．２　デジタル安全保護系 V&V 指針 2020

４．２．１　検証及び妥当性確認（V&V）

検証及び妥当性確認（V&V）については、「4. V&V」に規定している。

（１）　変更の内容(「表 4.2.1-1　検証及び妥当性確認(V&V)に関する規定内容の変更点」参照)

① V&V の対象規格を JEAC4620 から JEAC4620 等に変更し、V&V 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ことを追加した。(4. 1 V&V の目的と概要)

② V&V を実施する個人又はグループの力量及び経済面、工程管理に関する制約を受けないことを追加した。(4. 2 V&V の実施(2)体制)

③ なお書きで規定していた設計・製作者の各作業項目及び検証者の各作業項目を削除した。(4. 2 V&V の実施(2)体制)

④ 図１の設計・製作作業の範囲を示す一点鎖線の範囲の各ステップに設計検証を追加した。(4. 2 V&V の実施)

⑤ ソフトウェアの品質確保に適用する品質保証仕様書の項番号を「7.6 監視機器及び測定機器の管理」から「7.1.5 監視及び測定のための資源」に変更した。((解説-10) ソフトウェアツール)

表 4.2.1-1　検証及び妥当性確認（V&V）に関する規定内容の変更点

デジタル安全保護系 V&V 指針 2020	デジタル安全保護系 V&V 指針 2008
4. V&V 4. 1 V&V の目的と概要 (1)V&V は，JEAC4620 等のディジタル安全保護系に対する要求事項が設計，製作，試験及び変更の各プロセスにおいて正しく実現されていることを保証するための活動である。V&V 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。 (2)設計・製作作業のステップごとに上位仕様と下位仕様の整合性チェックを主体として，以下の観点から検証作業を行う。 (a)ディジタル安全保護系に対する要求事項がハードウェア・ソフトウェアの設計要求仕様（ハードウェア・ソフトウェア統合要求仕様，ハードウェア設計要求仕様及びソフトウェア設計要求仕様からなる。）に正しく反映されていること。 (b)、(c)（略） (3)（略） 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。	4. 検証及び妥当性確認 4. 1 検証及び妥当性確認の目的 (1)検証及び妥当性確認は，JEAC4620-2008（以下「JEAC4620」という）のディジタル安全保護系システム要求事項が設計・製作・試験・変更の各プロセスにおいて正しく実現されていることを保証するための活動である。 (2)設計・製作プロセスの各ステップごとに上位仕様と下位仕様の整合性チェックを主体として，下記の観点から検証作業を行う。 (a)ディジタル安全保護系システム要求事項がハードウェア・ソフトウェアの設計要求仕様に正しく反映されていること。 (b)、(c)（略） (3)（略） 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。

（略） （図１の変更点は添付新旧対照表を参照） (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 （略） (4)ソフトウェアツールの管理 （略） （解説-10）ソフトウェアツール ソフトウェアツールの品質の確保とは，「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]」の附属書－１「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」の「7.1.5 監視及び測定のための資源」に基づいた品質保証活動の結果として確保することである。	（略） （図１の変更点は添付新旧対照表を参照） (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。 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 （略） (4)ソフトウェアツールの管理 （略） （解説-9）ソフトウェアツール ソフトウェアツールの品質の確保とは，「原子力発電所における安全のための品質保証規程（JEAC4111-2003）の適用指針－原子力発電所の運転段階－：JEAG4121-2005[2007 年追補版]」の附属書「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」の「7.6 監視機器及び測定機器の管理」に基づいた品質保証活動の結果として確保することである。

（２）　日本電気協会による変更の理由

①　ディジタル安全保護系に対する要求事項は JEAC4620 に限定したものではないため、「等」を追記した。検証及び妥当性確認を行うものは技術的な専門家の集団であることから、「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]」に合わせて「個人又はグループ」とした。

② (a)の V&V を実施する組織と(b)の V&V の実施を管理する組織とが別でなければならないようにも読めるため、「V&V を実施する個人又はグループ」に表現を統一した。技術面の独立性については、必要な力量を持つこととし、経済面、工程管理の独立性については、それぞれの制約を受けないものとするよう記載を見直した。

③ 設計・製作作業内容は「図１ V&V 概要」及び「(解説―6) 設計・製作作業内容」 に、V&V 実施内容は「4.2 V&V の実施」の「(1) V&V の手順及び内容」にそれぞれ記載しているため削除した。

④ 「(解説-1) 品質保証活動の概要」における「参考図-1 ディジタル安全保護系の品質保証活動の概要」に示す「設計チームによる品質保証活動」の記載に合わせた。

⑤ JEAG4121 改定に伴い参照項を変更した。

（３） 検討の結果

① デジタル安全保護系規程 2020 は「1.目的」において、「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と，そのソフトウェアに対する品質上の要求事項を規定するもの」としている。デジタル安全保護系 V&V 指針 2020 の「4. 1 V&V の目的と概要」(1)に規定する「JEAC4620 等のディジタル安全保護系に対する要求事項」は、デジタル安全保護系に対する要求事項がデジタル安全保護系規程 2020 の要求事項以外にも存在し、それを含めた要求事項について V&V を行うとしている。

「V&V は，JEAC4620 等のデジタル安全保護系に対する要求事項が設計，製作，試験及び変更の各プロセスにおいて正しく実現されていることを保証するための活動である。」と規定しているうちの「JEAC4620 等」の「等」について、想定している規格について、日本電気協会は、次のように説明している[75]。

> *ディジタル安全保護系は，原子炉施設の異常状態を検知し必要な場合に各信号回路を直接動作させる設備であり，その要求事項は「発電用軽水型原子炉施設に関する安全設計指針」及び「実用発電用原子炉及びその付属施設の技術基準に関する規則」を代表とするプラント安全設計に必要な事項並びに各プラント固有の設計要求である設置許可申請書を想定していることから、「JEAC4620 等」の記載としています。*

技術基準規則等の規制要求が「JEAC4620 等」として「等」に含まれていることを規格から読み取ることは困難である。「JEAC4620 等」は無くても意味は通じるので、記載の適正化を要望する。「JEAC4620 等のディジタル安全保護系に対する要求事項」は、これ以外に「4.1 V&V の目的と概要」(3)、「4.2 V&V の実施」(1)(b)及び(g)にも記載されていることから、同様に記載の適正化を要望する。

また、V&V 作業は「設計・製作作業と別の人間が行う」としていたものを「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」に変更した件は、第 3 者が実施する

[75] 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 資料２－１ 回答 2.1)

ことを明確にしたものであり、妥当と判断する。

② V&V を実施する組織と V&V の実施を管理する組織とが別である必要はなく、V&V を実施する個人又はグループの力量を有することを組織が認めた者及び経済面、工程管理に関する制約を受けないことを明確にしたものであり、妥当と判断する。

設計・製作作業の内容は「図１ V&V 概要」及び「(解説―6) 設計・製作作業内容」に、V&V 実施内容は「4.2 V&V の実施」の「(1) V&V の手順及び内容」に記載されている。「図１V&V 概要」には、検証（検証１～５）として各設計段階の文書を直接的なインプットとしてその間の整合を確認するように矢印が記載されているが、妥当性確認については「試験」から直接矢印が１本だけ引かれており、妥当性確認の対象（例えば試験要領書/成績書等の文書か、試験行為自体か）が具体的に記載されていない。 妥当性確認の対象と実施内容について、日本電気協会は、次のように説明している[76]。

妥当性確認の対象は，試験要領書/成績書などの文書であり，試験行為自体は V&V の対象とは考えておりません。妥当性確認では，最終製品が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，実施する試験内容・判断基準、及び、実施された試験結果を確認することで確認します。

また、妥当性確認に関連して、「試験」が V&V の範囲を示す(注２)の破線内に記載されており、試験は、妥当性確認を実施する独立した体制で実施すると理解してよいかについて、日本電気協会は、次のように説明している[77]。

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体制で行うこととしております。試験を実施する行為自体は、V&V 作業ではありませんので「独立した体制」では実施しません。

V&V 作業を含む品質保証活動の全体概要については，(解説-1) の参考図 1 で示しております。ここで，基本的な原子力品質保証活動の中での妥当性確認は，JEAC4111/JEAG4121 で記載されている通り“試験”自体を指しており，設計チームが最終的な製品に対して要求事項を満たしていることを確認しております。一方で，V&V 作業では，設計，製作及び試験に携わった組織から独立した体制が，実施する試験内容・判断基準，及び，実施された試験結果を設計チームのそれとは別に妥当性確認を行うことで，独立性を確保しております。

また一方で，図 1 は V&V 作業の概要を説明するための図であり，(注 1) の一点鎖線で (解説-6) で説明している設計・製作作業の範囲を，(注 2) の破線で V&V の範囲を示しております。いずれも現状の記載に誤りはございませんが，試験行為も含めた形で V&V 作業と見えてしまう点など，本文の記載表現に関しては今回ご質問頂いた内容を踏まえ次回改定時に見直しを検討したいと考えます。

「図 1 V&V 概要」において、「試験」についての設計チームの妥当性確認はなく、V&V チームが妥当性確認を行うことになっている。注２の範囲について見直すことを要望する。なお、「図 1 V&V 概要」は概要を示すものであり、規定本文を優先する考えから

[76] 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 資料２－１ 回答 2. 2) ①

[77] 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 資料３－２ 回答 2. 2) ②

適用除外とする。これに伴い、「4. 2 V&V の実施」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」とあるのは、「各ステップにおいて，V&V 作業を実施する」と読み替え、同「(1)V&V の手順及び内容」の「図１に示された，設計・製作作業」は「設計・製作作業」と、同「(3)文書管理」の「(a)設計，製作作業の文書化」における「図１に示されるステップごとに必要な設計，製作」は「ステップごとに必要な設計，製作」と読み替える。

③　V&V の実施内容は設計・製作作業と対応させる必要があり、設計・製作作業の内容を本文から除外するのは適切でない。したがって、「(解説―6) 設計・製作作業内容」は「4. V&V」に加え、規定の「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。」及び同解説の「図１に示す設計・製作作業の各ステップの内容を以下に示す。」とあるのは、併せて「ソフトウェアに関する V&V の設計・製作作業の各ステップの内容は，以下の(1)～(6)に示す手法によるものとする。」と読み替える。

④　図１の設計・製作作業の範囲を示す一点鎖線の範囲の各ステップに設計検証を追加したことは、「(解説-1) 品質保証活動の概要」における「参考図-1 ディジタル安全保護系の品質保証活動の概要」に示す「設計チームによる品質保証活動」の記載に合わせたものであり、妥当と判断するが③の検討価結果から適用除外が優先される。

⑤　技術基準規則解釈において、デジタル安全保護系 V&V 指針 2008 の「(解説-9) ソフトウェアツール」は、同規格の適用に当たっての条件とされていたことから、デジタル安全保護系 V&V 指針 2020 の「(解説-10) ソフトウェアツール」は、「4. 2 V&V の実施」の「(4)ソフトウェアツールの管理」を適用するに当たっての条件となるが、「４．１．９　検証及び妥当性確認（V&V)」（３）②で述べたとおり、JEAG4121-2015[2018 年追補版］は適用除外としている。したがって、デジタル安全保護系 V&V 指針 2008 の「(解説-9) ソフトウェアツール」は「4.2 検証及び妥当性確認の実施」の「(4)ソフトウェアツールの管理」に加える。また、デジタル安全保護系 V&V 指針 2020「(解説-10) ソフトウェアツール」の「ソフトウェアツールの品質の確保とは，「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]」の附属書－１「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」の「7.1.5 監視及び測定のための資源」に基づいた品質保証活動の結果として確保することである。」は適用除外とする。

（４）　変更点以外の評価

①　４．１．１（４）で述べたたように、デジタル安全保護系規程 2020 における「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）に対する要求事項を「デジタル安全保護系のデジタル化された演算・論理処理部」（核計装・放射線計装も含む安全保護系全体）に適用することとし、同規程の「４．ディジタル安全保護系に対する要求事項」及び解説において、内容に安全保護系の機能が規定されている場合の「ディジタル計算機」は、「(デジタル安全保護系の) デジタル化された演算・論理処理部」と読み替え、個々に明示することとしている。「(解説-3) 機能を実現するソフトウェア」の「安全保護系としての機能を実現するソフトウェア」に限定する記載を適用除外とすることでソフトウェアの範囲を広く捉えることにしている。また、４．

１．９（３）②においては品質保証に係る読替が記載されている。

これらの読替の趣旨に沿ってデジタル安全保護系 V&V 指針 2020 の規定を確認した結果、以下に示す読替を行う。

「1. 目的」において、「安全保護系にディジタル計算機を適用するに当たっては，ソフトウェアの品質を確保することが重要」とあるのは、「安全保護系にデジタル化された演算・論理処理部を適用するに当たっては，保安活動の重要度に応じ，当該処理部に装荷するソフトウェア（以下単に「ソフトウェア」という。）の品質を確保することが重要」と読み替え、「ディジタル安全保護系のソフトウェア」とあるのは、「デジタル化された演算・論理処理部を適用した安全保護系（以下「デジタル安全保護系」という。）のソフトウェア」と読み替える。

「(解説-3) 適用範囲（概念図)」は適用除外とする。

「3. 3 V&V」の「「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]」に基づいた品質保証活動」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」と読み替える。

「3. 4 検証」の「ディジタル計算機」は「デジタル化された演算・論理処理部」と読み替える。

「4.V&V」の「ディジタル安全保護系に装荷するソフトウェア」は、「デジタル安全保護系のデジタル化された演算・論理処理部に装荷するソフトウェア」と読み替え、「(解説-6) 設計・製作作業内容」の「(4)ソフトウェア製作」における「ディジタル計算機」は、「デジタル化された演算・論理処理部」と読み替える。

（５）　適用に当たっての条件

①②④　なし

③⑤及び変更点以外①

読み替える規定	読み替えられる字句	読み替える字句
1. 目的	原子力発電所の安全保護系にディジタル計算機を適用するに当たっては，ソフトウェアの品質を確保することが重要である。このため本指針は，ディジタル安全保護系のソフトウェアの設計，製作，試験及び変更の各プロセスにおいて，安全保護上要求される機能が正しく確実に実現されていることを保証する活動である V&V に対する基本的事項を示すものである。	原子力発電所の安全保護系にデジタル化された演算・論理処理部を適用するに当たっては，保安活動の重要度に応じ，当該処理部に装荷するソフトウェア（以下単に「ソフトウェア」という。）の品質を確保することが重要である。このため本指針は，デジタル化された演算・論理処理部を適用した安全保護系（以下「デジタル安全保護系」という。）のソフトウェアの設計，製作，試験及び変更の各プロセスにおいて，安全保護上

		要求される機能が正しく確実に実現されていることを保証する活動であるV&V に対する基本的事項を示すものである。
3. 3 V&V	Verification and Validation の略。 ディジタル安全保護系のソフトウェアに対して,「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]」に基づいた品質保証活動を前提にして,設計,製作及び試験に携わった者以外の個人又はグループが実施する検証及び妥当性確認。	Verification and Validation の略。 デジタル安全保護系のソフトウェアに対して,「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前提にして,設計,製作及び試験に携わった者以外の個人又はグループが実施する検証及び妥当性確認。
3. 4 検証	ディジタル計算機を適用した対象システムのソフトウェアの設計,製作の各プロセスにおける各ステップの製品が,直前のステップから課せられた要求を満たしているか否かの確認作業。 本用語は,一般的な品質保証の用語(JIS Q 9000-2015 を参照)でもあるが,本指針内に限り上記の定義に従うものとする。	デジタル化された演算・論理処理部を適用した対象システムのソフトウェアの設計,製作の各プロセスにおける各ステップの製品が,直前のステップから課せられた要求を満たしているか否かの確認作業。 本用語は,一般的な品質保証の用語(JIS Q 9000-2015 を参照)でもあるが,本指針内に限り上記の定義に従うものとする。
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。 (解説-6) 設計・製作作業内容 図1に示す設計・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	デジタル安全保護系のデジタル化された演算・論理処理部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(1)～(6)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等のディ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，ディ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。	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,デジタル化された演算・論理処理部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	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。

	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 4）	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。	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。 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	(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。 (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

○「(解説-3) 適用範囲（概念図)」は適用除外とする。

○「(解説-10) ソフトウェアツール」は適用除外とする。

（６） 要望事項

○「JEAC4620 等」は無くても意味は通じるので、記載の適正化を要望する。「JEAC4620 等のディジタル安全保護系に対する要求事項」は、これ以外に「4.1 V&V の目的と概要」(3)、「4.2 V&V の実施」(1)(b)及び(g)にも記載されていることから、同様に記載の適正化を要望する。

○「図 1 V&V 概要」において、「試験」についての設計チームの妥当性確認はなく、V&V チームが妥当性確認を行うことになっている。注２の範囲について見直すことを要望する。

４．３ 以前の技術評価についての反映状況

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についての確認結果を表 4.3-1 に示す。デジタル安全保護系規程 2020 に反映しなかった内容について、日本電気協会はその理由を次のように説明している[78]。

表 4.3-1 デジタル安全保護系規程 2008 等技術評価書の記載内容と確認結果

No	デジタル安全保護系規程 2008 等技術評価書の適用にあたって	日本電気協会の回答内容	確認結果

[78] 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 資料１－２ 回答 1.1)

	の条件		
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。	【反映済】 本技術評価書 4.1.1 項にて技術評価
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。	【反映済】 本技術評価書 4.1.9 項にて技術評価
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。	【反映済】 本技術評価書 4.1.11 項にて技術評価
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。	【前段は反映済、後段は未反映】 本技術評価書 4.1.6 項にて技術評価
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。	【反映済】 本技術評価書 4.1.5 項にて技術評価

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。	【未反映】 本技術評価書 4.1.1 項にて技術評価
7	なお、別記-7No.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。	【未反映】 本技術評価書 4.1.12 項にて技術評価 なお、デジタル安全保護系への要求事項ではないことから，デジタル安全保護系規程 2020 に対する要求からは削除する。

４．４　技術基準規則解釈に引用する解説の本文規程への取り込み

技術基準規則解釈第３５条第４号においては、「表 2.3-1　技術基準規則及び解釈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」に示すように、デジタル安全保護系の適用に当たって、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 の解説番号を引用している。

（１）　検討の結果

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 の解説については、4.1 項及び 4.2 項において技術評価対象から外れたものも存在することから、すべての解説について技術基準規則解釈への反映要否について確認した。その結果を「表 4.4-1　「安全保護系へのディジタル計算機の適用に関する規程（JEAC4620)」解説の技術基準規則解釈反映要否」及び「表 4.4-2　「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（JEAG4609)」解説の技術基準規則解釈反映要否」に示す。

デジタル安全保護系規程 2020 については、技術評価を行ったものに加え、以下に示すものを本文とする読替を行う。

・(解説-6) リアルタイム性能

デジタル安全保護系 V&V 指針 2020 については、該当なしである。

表 4.4-1　デジタル安全保護系規程 2020 解説の技術基準規則解釈反映要否

JEAC4620-2020　解説	技術評価の項番号	技術基準規則解釈反映要否	JEAC4620-2008 解説
(解説-1) 目的	4.1.1(4)①(c)	否（一部本文移行を要望)	(解説-1)
(解説-2) 適用範囲（概念図)	4.1.1(4)①(a)	否（見直しを要望)	(解説-2)
(解説-3) 機能を実現するソフトウェア	4.1.1(4)①(b)	否	(解説-3)
(解説-4) アンアベイラビリティ及び誤動作率の評価	4.1.1(4)②	否（見直しを要望)、現行第３５条第４号（６）採用	－
(解説-5) 過渡時及び地震時の機能	4.1.1(3)①	要(一部)	－
(解説-6) リアルタイム性能	－	要	★(解説-4)
(解説-7) 多重化されたチャンネル間の通信	4.1.2(3)②③	要	★(解説-5)
(解説-8) 計測制御系との分離	4.1.6(3) ②③	要	★(解説-6)
(解説-9) ソフトウェアの試験	－	否	(解説-7)
(解説-10) 外的要因（関連規格・指針)	4.1.11(3)①③④⑤	要	★(解説-8)
(解説-11) 外的要因（設計の確証)	4.1.11(3)②	否	－
(解説-12) 適切な設定変更	－	否	－
(解説-13) 直接検出できない変数の例	－	否	(解説-9)
(解説-14) 手動操作の機能	－	否	(解説-10)
(解説-15) 自己診断機能	4.1.1(4)①(a)	要	★(解説-11)
(解説-16) ソフトウェアの管理外の変更の防止	4.1.1(4)①(b)	要	★(解説-12)
(解説-17) 不正アクセス行為等の被害の防止	4.1.5(3)①	要（要望事項あり）	－
(解説-18) 品質保証活動	4.1.9(3)②	要（適用除外あり）	★(解説-13)
(解説-19) ソフトウェアライフサイクル	4.1.8(3)①② 4.1.9(3)①	要	★(解説-14)
(解説-20) ソフトウェアの構成管理	4.1.10(3)②	要	★(解説-15)
(解説-21) V&V（手順)	4.1.9(3)①②	要	★(解説-16)
(解説-22) V&V（独立性)	4.1.9(3)④	要	★(解説-17)
(解説-23) V&V（文書化)	4.1.9(3)⑤	要	★(解説-18)
(解説-24) 動作原理等の異なる追加の設備	4.1.12(3)①	否	(解説-19)
－			(解説-20)

★:技術基準規則解釈に記載のもの

表 4.4-2　デジタル安全保護系 V&V 指針 2020 解説の技術基準規則解釈反映要否

JEAG4609-2020　解説	技術評価の項番号	技術基準規則解釈反映要否	JEAG4609-2008 解説
(解説-1) 品質保証活動の概要	4.2.1(3)③	否（要望事項あり）	(解説-6) 品質保証活動の概要
(解説-2) 目的	－	否	(解説-1) 目的
(解説-3) 適用範囲（概念図）	－	否（見直しを要望）	(解説-2) 適用範囲（概念図）
(解説-4) ハードウェア・ソフトウェアの設計要求仕様	－	否	(解説-5) (2)①②③から移行
(解説-5) V&V が可能なソフトウェア設計	－	否	(解説-3) 検証及び妥当性確認が可能なソフトウェア設計
(解説-6) 設計・製作作業内容	4.2.1(3)③	要	(解説-5) 設計・製作作業内容 (2)①②③の内容は 2020 年版の(解説-4)へ移行
(解説-7) 変更作業	－	否	(解説-4) 変更作業
(解説-8) V&V で行う上で着目すべき観点		否	(解説-7) 検証及び妥当性確認
(解説-9) 管理面の独立	－	否	(解説-8) 管理面の独立
(解説-10) ソフトウェアツール	4.2.1(3)⑤	否	★(解説-9) ソフトウェアツール
(解説-11) ソフトウェアの再利用	－	否	(解説-10) ソフトウェアの再利用
(解説-12) 変更管理	－	否	(解説-11) 変更管理

★:技術基準規則解釈に記載のもの

（2）　適用に当たっての条件

読み替える規定	読み替えられる字句	読み替える字句
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。 （解説-6）リアルタイム性能 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，	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。	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。

５．デジタル安全保護系規程及びデジタル安全保護系 V&V 指針の適用に当たっての条件

デジタル安全保護系規程 2020 及びデジタル安全保護系規程 2008 並びにデジタル安全保護系 V&V 指針 2020 及びデジタル安全保護系 V&V 指針 2008 の適用に当たっての条件を以下に示す。なお、技術評価の対象外としたものは記載していない。

５．１　デジタル安全保護系規程 2020

読み替える規定	読み替えられる字句	読み替える字句
1.目的	本規程は，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（以下，ディジタル安全保護系という。）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するものである。	本規程は，原子力発電所の安全保護系においてデジタル化された演算・論理処理部を有するもの（以下，デジタル安全保護系という。）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するものである。
（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）
3.3 V&V	Verification and Validation の略。ディジタル安全保護系のソフトウェアに対して，「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]」に基づいた品質保証活動を前提にして，設計，製作及び試験に携わった者以外の個人又はグループが実施する検証及び妥当性確認。	Verification and Validation の略。デジタル安全保護系のソフトウェアに対して，「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前提にして，設計，製作及び試験に携わった者以外の個人又はグループが実施する検証及び妥当性確認。
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	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

	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。	に相応した高い信頼性を有すること。 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。 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。
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。 （解説-6）リアルタイム性能 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。	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。 （解説-7）多重化されたチャンネル間の通信 多重化されたチャンネル間の通信の機能的分離の措置の例としては以下がある。 (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) ディ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。	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を含む複数の手段の適切な組合せを考慮する。 (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。 （解説-8）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，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	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，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。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。 ・ディ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。 また，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は以下がある。 (1)試験時又は保守時を除き，計測制御系からの情報を受けない設計とする。 (2)試験時又は保守時に計測制御系からの情報を受ける場合には，当該チャンネルをバイパス又はトリップとする。 (3)ディジタル安全保護系から計測制御系への通信は，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。 (4)ディ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。	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。 (削る)
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
4.9.2 耐震性	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を有するこ	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を有するこ

	と。	と。
4.9.3 その他の外的要因	ディジタル安全保護系は，火災防護上の措置及び溢水防護上の措置を考慮した設計とすること。	デジタル安全保護系は，火災防護上の措置及び溢水防護上の措置を考慮した設計とすること。
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。 （解説-15）自己診断機能 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ィ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。	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安全保護系のデジタル化された演算・論理処理部の異常を検知した場合には，当該処理部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安全保護系のデジタル化された演算・論理処理部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。 （解説-16）ソフトウェアの	デジタル安全保護系のデジタル化された演算・論理処理部に装荷するソフトウェア（以下単に「ソフトウェア」という。）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

	管理外の変更の防止 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	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 （解説-17）不正アクセス行為等の被害の防止 不正アクセス行為等の被害の防止に必要な措置の例としては，以下がある。 (1) 外部ネットワーク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。 (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。	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。 ・デジタル化された演算・論理処理部に使用目的に沿うべき動作をさせない行為 ・デジタル化された演算・論理処理部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) 解説-16の(2)鍵付きスイッチの設置及び(3)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。	(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 （解説-18）品質保証活動 ディジタル安全保護系の品質保証活動については，「原子力安全のためのマネジメントシステム規程：JEAC 4111-2013」及び「原子力安全のためのマネジメントシステム規程（JEAC 4111-2013）の適用指針：JEAG 4121-2015[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」を参照する。 市販ディジタル計算機，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）	デジタル安全保護系に用いられるデジタル化された演算・論理処理部は，保安活動の重要度に応じ，以下に掲げる事項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 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）

4.19.1 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。 （解説-19）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 ディ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	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。 (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 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。 (h)開発プロセス:製品を製作する前の研究，試作等であり，製品設計とは直結しないプロセスである。 (i)保守プロセス:ソフトウェアの保守としては実施する内容がない。なお，システムの保守としては定期検査時の試験がある。 (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	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。 (h)開発プロセス:製品を製作する前の研究，試作等であり，製品設計とは直結しないプロセスである。 (i)保守プロセス:ソフトウェアの保守としては実施する内容がない。なお，システムの保守としては定期検査時の試験がある。 (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。 以上のプロセスの状態を参考図３に示す。	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。 (削る)
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。 (解説-20) ソフトウェアの構成管理 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	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。 (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。	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	デ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。 （解説-21） 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，ディジタル安全保護系の供給者は，「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]」に従った一般の品質保証活動を実施した上で，ディジタル安全保護系のソフトウェアに対し V&V 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」を参照する。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，参考図３に示す設計，製作，試験及び変更がある。 （解説-22） 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	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した上で，デジタル安全保護系のデジタル化された演算・論理処理部に装荷する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を制御するソフトウェアを除いたものに対し V&V 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

	管理に関する制約を受けない。 （解説-23）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。	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。

○「(解説-4) アンアベイラビリティ及び誤動作率の評価」は適用除外とする。

○「(解説-10) 外的要因（関連規格・指針)」は適用除外とする。

５．２　デジタル安全保護系規程 2008

読み替える規定	読み替えられる字句	読み替える字句
1.目的	本規程は，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（以下，ディジタル安全保護系と呼ぶ）に対し，その性能及び信頼度の面から必要とされる事項を規定するものである。	本規程は，原子力発電所の安全保護系においてデジタル化された演算・論理処理部を有するもの（以下，デジタル安全保護系という。）に対し，その性能及び信頼度の面から必要とされる事項を規定するものである。
（解説-3）	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，安全保護系設備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。
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。 (追加)	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。 （解説-4） 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。	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。 （解説-5） 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	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。	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。 （解説-6） 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，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。 また，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は具体的には（解説-5）の事項を考慮する。	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。 （削る）
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	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

	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。	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。 （解説-11） 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や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ィ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，ウォッチドックタイマ，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。	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安全保護系のデジタル化された演算・論理処理部の異常を検知した場合には，当該処理部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安全保護系のデジタル化された演算・論理回路機器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	ディジタル安全保護系に装荷するソフトウェアは，管	デジタル安全保護系のデジタル化された演算・論理処

防護措置	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。 （解説-12） 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	理部に装荷するソフトウェア（以下単に「ソフトウェア」という。）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 （解説-13） ディジタル安全保護系の品質保証活動については，「原子力発電所における安全のための品質保証規程：JEAC 4111-2003」並びに「原子力発電所における安全のための品質保証規程（JEAC 4111-2003）の適用指針 －原子力発電所の運転段階－:JEAG 4121-2005[2007年追補版]」の附属書「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」を参照する。 市販ディジタル計算機，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	安全保護系に用いられるデジタル化された演算・論理処理部は，保安活動の重要度に応じ，以下に掲げる事項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（「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） ・検証及び妥当性確認活動 デジタル安全保護系の品質保証活動については，「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」の施行日より前に出された工事計画は，「原子力発電所における安全のための品質保証規程：JEAC 4111-2003」並びに「原子力発電所における安全のための品質保証規程（JEAC 4111-2003）の適用指針 －原子力発電所の運転段階－：JEAG 4121-2005[2007年追補版]」の附属書「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」によること

	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）	ができる。 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。 （解説-14） ディ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毎の管理を実施する。 (1) ライフサイクルプロセス ディ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，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	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毎の管理を実施する。 (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，下記の理由により，開発，保守プロセスを定義していない。 開発プロセス：製品を製作する前の研究，試作等であり，製品設計とは直結しないプロセスである。 保守プロセス：ソフトウェアの保守としては実施する内容がない。なお，システムの保守としては定期検査時の試験がある。 (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	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。 開発プロセス：製品を製作する前の研究，試作等であり，製品設計とは直結しないプロセスである。 保守プロセス：ソフトウェアの保守としては実施する内容がない。なお，システムの保守としては定期検査時の試験がある。 (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・試験のプロセスに従う。 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。 以上のプロセスの状態を参考図３に示す。	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。 （削る）
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	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

	ること。 （解説-15） 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。	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	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。 (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れ，再利用の妥当性を示す根拠が文書化されていること。 （解説-16） 検証及び妥当性確認については，「ディジタル安全保護系の検証及び妥当性確認に関する指針：JEAG 4609-2008」を参照する。新規設計や変更により検証及び妥当性確認が必要なプロセスとして，設計，製作，試験，変更を対象とする。 なお，ソフトウェアライフサイクルプロセスにおける検証及び妥当性確認の対象を参考図３に示す。 （解説-17） 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。 (1)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。 (2)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。 （解説-18） 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。	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。

○（解説-2）は適用除外とする。

○（解説-8）は適用除外とする。

５．３　デジタル安全保護系 V&V 指針 2020

読み替える規定	読み替えられる字句	読み替える字句
1. 目的	原子力発電所の安全保護系にディジタル計算機を適用するに当たっては，ソフトウェアの品質を確保することが重要である。このため本指針は，ディジタル安全保護系のソフトウェアの設計，製作，試験及び変更の各プロセスにおいて，安全保護上要求される機能が正しく確実に実現されていることを保証する活動である V&V に対する基本的事項を示すものである。	原子力発電所の安全保護系にデジタル化された演算・論理処理部を適用するに当たっては，保安活動の重要度に応じ，当該処理部に装荷するソフトウェア（以下単に「ソフトウェア」という。）の品質を確保することが重要である。このため本指針は，デジタル化された演算・論理処理部を適用した安全保護系（以下「デジタル安全保護系」という。）のソフトウェアの設計，製作，試験及び変更の各プロセスにおいて，安全保護上要求される機能が正しく確実に実現されていることを保証する活動である V&V に対する基本的事項を示すものである。
3. 3 V&V	Verification and Validation の略。 ディジタル安全保護系のソフトウェアに対して，「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]」に基づいた品質保証活動を前提にして，設計，製作及び試験に携わった者以外の個人又はグループが実施する検証及び妥当性確認。	Verification and Validation の略。 デジタル安全保護系のソフトウェアに対して，「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前提にして，設計，製作及び試験に携わった者以外の個人又はグループが実施する検証及び妥当性確認。
3. 4 検証	ディジタル計算機を適用した対象システムのソフトウェアの設計，製作の各プロセスにおける各ステップの製品が，直前のステップから課せられた要求を満たし	デジタル化された演算・論理処理部を適用した対象システムのソフトウェアの設計，製作の各プロセスにおける各ステップの製品が，直前のステップから課せら

	ているか否かの確認作業。 本用語は，一般的な品質保証の用語（JIS Q 9000-2015を参照）でもあるが，本指針内に限り上記の定義に従うものとする。	れた要求を満たしているか否かの確認作業。 本用語は，一般的な品質保証の用語（JIS Q 9000-2015を参照）でもあるが，本指針内に限り上記の定義に従うものとする。
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。 （解説-6）設計・製作作業内容 図１に示す設計・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等のディ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)	デジタル安全保護系のデジタル化された演算・論理処理部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 の設計・製作作業の各ステップの内容は，以下の(1)～(6)に示す手法によるものとする。 (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，ディ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)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，デジタル化された演算・論理処理部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。(図１は略) 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	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	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 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。 (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	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 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。 (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

○「(解説-3) 適用範囲（概念図)」は適用除外とする。

○「(解説-10) ソフトウェアツール」は適用除外とする。

５．４　デジタル安全保護系 V&V 指針 2008

読み替える規定	読み替えられる字句	読み替える字句
1. 目的	原子力発電所の安全保護系にディジタル計算機を適用するに当たっては，ソフトウェアの品質を確保することが重要である。このため本指針は，ディジタル計算機を適用した安全保護系（以下これを「ディジタル安全保護系」という）のソフトウェアの設計，製作，試験・変更の各プロセスにおいて，安全保護上要求される機能が正しく確実に実現されていることを保証する活動に関して，検証と妥当性確認に対する基本的事項を示したものである。	原子力発電所の安全保護系にデジタル化された演算・論理処理部を適用するに当たっては，保安活動の重要度に応じ，当該処理部に装荷するソフトウェア（以下単に「ソフトウェア」という。）の品質を確保することが重要である。このため本指針は，デジタル化された演算・論理処理部を適用した安全保護系（以下「デジタル安全保護系」という。）のソフトウェアの設計，製作，試験・変更の各プロセスにおいて，安全保護上要求される機能が正しく確実に実現されていることを保証する活動に関して，検証と妥当性確認に対する基本的事項を示したものである。
3. 2 検証	ディジタル計算機を適用した対象システムのソフトウェアの設計・製作の各プロセスにおける各ステップの製品が，直前のステップから課せられた要求を満たしているか否かのチェック作業。	デジタル化された演算・論理処理部を適用した対象システムのソフトウェアの設計・製作の各プロセスにおける各ステップの製品が，直前のステップから課せられた要求を満たしているか否かのチェック作業。
4. 検証及び妥当性確認	ディジタル安全保護系に装荷するソフトウェアは，検証及び妥当性確認を実施して，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が確認されるべきである。 ソフトウェアに関する検証及び妥当性確認は，以下の手法によるものとする。 （解説-5）設計・製作作業内容 図１に示す設計・製作作業の各ステップの内容を以下に示す。	デジタル安全保護系のデジタル化された演算・論理処理部に装荷するソフトウェアは，検証及び妥当性確認を実施して，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が確認されるべきである。 ソフトウェアに関する検証及び妥当性確認の設計・製作作業の各ステップの内容は，以下の(1)～(6)に示す手法によるものとする。

	(1)システム設計要求仕様作成 JEAC 4620 のディジタル安全保護系システム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 ハードウェアとソフトウェアで実現する機能範囲及びそのインターフェイスを図，表などを用いて規定する。（例；機能ブロック図，入出力点一覧表等） ②ハードウェア設計要求仕様 全体ハードウェア及び構成されるハードウェア要素（マイクロプロセッサ，電源等）それぞれについての機能・性能を規定する。 （例；ハードウェアシステム構成図，ハードウェア機器仕様書等） ③ソフトウェア設計要求仕様 入力処理，演算処理，出力処理等のソフトウェア及びこれらを組合せて実現する全体ソフトウェア構成について機能・性能を規定する。 （例；ソフトウェア構成図，ソフトウェア機能仕様書等） (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。この時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	(1)システム設計要求仕様作成 JEAC 4620 のデジタル安全保護系システム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 ハードウェアとソフトウェアで実現する機能範囲及びそのインターフェイスを図，表などを用いて規定する。（例；機能ブロック図，入出力点一覧表等） ②ハードウェア設計要求仕様 全体ハードウェア及び構成されるハードウェア要素（マイクロプロセッサ，電源等）それぞれについての機能・性能を規定する。 （例；ハードウェアシステム構成図，ハードウェア機器仕様書等） ③ソフトウェア設計要求仕様 入力処理，演算処理，出力処理等のソフトウェア及びこれらを組合せて実現する全体ソフトウェア構成について機能・性能を規定する。 （例；ソフトウェア構成図，ソフトウェア機能仕様書等） (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。この時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，ディ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 ハードウェア機能・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。	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,デジタル化された演算・論理処理部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 ハードウェア機能・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 検証及び妥当性確認の実施	(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 （解説-9）ソフトウェアツール ソフトウェアツールの品質の確保とは，「原子力発電所における安全のための品質保証規程（JEAC4111-2003）の適用指針－原子力発電所の運転段階－：JEAG4121-2005[2007年追補版]」の附属書「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」の「7.6 監視機器及び測定機器の管理」に基づいた品質保証活動の結果として確保することである。	(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。ただし，上記規則の施行日より前に出された工事計画については、「原子力発電所における安全のための品質保証規程（JEAC4111 -2003）の適用指針－原子力発電所の運転段階－：JEAG4121-2005[2007年追補版]」の附属書「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」の「7.6 監視機器及び測定機器の管理」に基づいた品質保証活動の結果として確保する。 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

○「(解説-2) 適用範囲（概念図)」は適用除外とする。

６． 過去の技術評価における要望事項

過去の技術評価において要望事項となっていたものについて、未反映であるものを下表に示す。これらについては、今後規格に反映することを要望する。

表 6-1 デジタル安全保護系規程 2008 等技術評価書における「**デジタル安全保護系規程 2008 に関する要望事項と反映状況**

要望事項	反映状況
①「4.8 環境条件」に、耐震性、耐サージ性、火災防護上の措置として使用する規格、指針が記載されているが、具体的な仕様が明確になっていないため、デジタル安全保護系に適用する際の規格、指針の該当箇所を明示することが望まれる。なお、「原子力発電所耐震設計技術指針[重要度分類・許容応力編]：JEAG4601・補-1984」は「発電用原子炉施設に関する耐震設計審査指針：平成 18 年 9 月 19 日原子力安全委員会決定」とクラス分類の名称が異なるため、読み替えて使用すること。	未反映
②「4.2 精度と応答時間」で、プロセス信号のサンプリング周期、処理速度に対する具体的な仕様が記載されていないため、サンプリング周期、処理速度の選定方法の考え方を記載することが望まれる。	未反映
③「4.18.1 ソフトウェアライフサイクル」でソフトウェアのライフサイクルに関し、廃止プロセスを分かりやすく定義することが望まれる。	反映済み（4.1.8 項にて技術評価）
④「4.18.2 ソフトウェア構成管理」で具体的な管理手法の活動項目を明確にすることが望まれる。	未反映

表 6-2 デジタル安全保護系規程 2008 等技術評価書における**デジタル安全保護系 V&V 指針 2008 に関する要望事項と反映状況**

要望事項	反映状況
①「図１　検証・妥当性確認概要」で、「作業段階のつながり」を示した矢印と「情報の流れ」を示した矢印が同じ記号で記載されているため、これを区別して表記することが望まれる。	反映済み
②今回「デジタル安全保護系 V&V 指針」を技術評価したことから、「デジタル安全保護系 V&V 指針」を規程化することが望まれる。	未反映

７． 日本電気協会規格の策定に関する要望事項

（１） 日本電気協会の説明では、デジタル安全保護系規程 2020 は性能規定を示したとあるが、技術評価は「性能規定化された規制要求に対する容認可能な実施方法」について

行うものであることから、仕様規定化することを要望する。

（２）　当庁からの質問に対する日本電気協会の回答においては、「デジタル計算機とは、原子炉停止系及び工学的安全施設作動系の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設備をいう。」等の明確に規定されていない解釈に基づく回答があった。規格策定時に前提としたとのことであるが、そのように読むことは困難であることから、日本電気協会には、審議レベル間で規程の対象範囲・前提条件について認識の差異が生じないよう工夫することを要望する。

（３）　（追而）

添付資料－１　変更点一覧

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 4620-2020 における同 JEAC 4620-2008 からの変更点一覧

変更点の分類：

①　記載の適正化のための変更（用語の統一、表現の明確化、題目の修正、条項番号の変更、単位換算の見直し、記号の変更）

②　引用されている法令、規格の引用年版等の変更（年版改正の反映、新たな規格の反映）

③　国内外の知見の反映等（国内外における試験研究成果の反映等）

④　技術評価対象外

No.	頁	規定番号	変更内容	分類
1	1	1. 目的	・記載の適正化 ・規定の範囲を「性能及び信頼度の面から必要とされる事項」から「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」に変更し明確化 「本規程は，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（以下，ディジタル安全保護系と呼ぶ）に対し，その性能及び信頼度の面から必要とされる事項を規定するものである。」 →「本規程は，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（以下，ディジタル安全保護系という。）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するものである。」	① ①
2	1	3. 用語の定義	・記載の適正化 ・「3.2 検証」、「3.3 妥当性確認」及び「3.4 文書」を削除、「3.2 安全保護系」及び「3.3 V&V」を追加し以降の項番号繰上げ ・表現の明確化 「3.1 ディジタル計算機 内蔵されたプログラムによって制御され，人手の介入なしにディジタルデータの算術演算や論理演算などの計算を行う装置。 3.2 検証 ディジタル計算機を適用した対象システムのソフトウェアの設計・製作の各プロセスにおける各ステップの製品が，直前のステップから課せられた要求を満たしているか否かのチェック作業。 3.3 妥当性確認	① ④ ①

No.	頁	規定番号	変更内容	分類
			ソフトウェアとハードウェアを統合して製作された最終製品としての計算機システムが，機能要求，性能要求，インターフェイス要求を満たしていることの，試験プロセスにおける確認作業。 3.4 文書 品質保証に対する活動，要求事項，要領若しくは結果を明確にし，規定し，報告し又は証明するための記述されたあるいは図示された情報。 3.5 応答時間 検出器の出力信号から原子炉停止系あるいは工学的安全施設の作動信号を発信するまでの時間。 3.6 外部ネットワーク インターネット等のプラント外部のネットワーク。」 →「3.1 ディジタル計算機 内蔵されたプログラムによって制御され，人手の介入なしにディジタルデータの算術演算，論理演算等の計算を行う装置。 3.2 安全保護系 原子炉施設の異常状態を検知し，必要な場合，原子炉停止系（原子炉の緊急停止機能），工学的安全施設の作動を直接開始させるよう設計された設備であり，検出器から動作装置入力端子までをいう。 3.3 V&V Verification and Validation の略。ディジタル安全保護系のソフトウェアに対して，「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]」に基づいた品質保証活動を前提にして，設計，製作及び試験に携わったもの以外の個人又はグループが実施する検証及び妥当性確認。 3.4 応答時間 検出器の出力信号から原子炉停止系（原子炉の緊急停止機能）又は工学的安全施設の作動信号を発信するまでの時間。 3.5 外部ネットワーク 原子力施設で管理していない情報システム。インターネット，事業者の社内業務用ネットワーク，国の原子力防災用ネットワーク等が該当する。」	
3	2	4.1 過渡時及び地震時の機能 4.2 事故時の機	・過渡時及び地震時の機能と事故時の機能に分割し、前者は「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」、後者は「異常な状態を検知し，原子炉停止系（原子炉の緊急停止機能）及び必要な工学的安全施設を自動的に作	③

No.	頁	規定番号	変更内容	分類
		能	動させる設計」に明確化、以降の項番号繰下げ 「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。」 →「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。 4.2 事故時の機能 ディジタル安全保護系は，設計基準事故が発生する場合において，その異常な状態を検知し，原子炉停止系（原子炉の緊急停止機能）及び必要な工学的安全施設を自動的に作動させる設計とすること。」	
4	2	4.3 精度及び応答時間	・項番号の繰下げ、記載の適正化 「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。」 →「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。」	①
		（解説-6）リアルタイム性能	・題目を記載、表現の明確化 「(解説-4) 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。」 →「(解説-6) リアルタイム性能 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。」	①
5	2	4.4 多重性	・項番号の繰下げ、表現の明確化 「4.3 多重性 ディジタル安全保護系は，システム構成機器又はチャンネルの単一故障あるいは単一取り外し，バイパス	①

No.	頁	規定番号	変更内容	分類
			に対して機能を喪失することがないように，多重性を有する設計とすること。」 →「4.4 多重性 ディジタル安全保護系は，システム構成機器又はチャンネルの，単一故障，単一の取り外し又はバイパスに対して機能を喪失することがないように，多重性を有する設計とすること。」	
6	2	4.5 独立性	・項番号の繰下げ ・チャンネル間に通信を用いる場合の機能的分離を追加 「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。」 →「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。」	④ ③
		（解説-7）多重化されたチャンネル間の通信	・題目を記載 ・多重化されたチャンネル間の通信の機能的分離の措置を考慮事項から例示事項に変更 ・多重化されたチャンネル間の通信例を「通信接続の制御を受信側の異常が発信側に影響しない設計」から「ディ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」に変更 「(解説-5) 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。」 →「(解説-7) 多重化されたチャンネル間の通信 多重化されたチャンネル間の通信の機能的分離の措置の例としては以下がある。 (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)ディ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。」	① ③ ③

No.	頁	規定番号	変更内容	分類
7	2	4.6 計測制御系との分離	・項番号の繰下げ、表現の明確化 「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。」 →「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。」	①
		（解説-8）計測制御系との分離	・題目を記載 ・アイソレーションデバイスは安全保護系に属する旨を追記 ・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の措置を考慮事項から例示に変更し、計測制御系からの情報受け制限と試験時及び保守時の例外扱いを追加 ・ディ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例示を追加 「(解説-6) 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，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。また，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は具体的には（解説-5）の事項を考慮する。」 →「(解説-8) 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，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。 ・ディ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。 また，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は以下がある。 (1)試験時又は保守時を除き，計測制御系からの情報を受けない設計とする。 (2)試験時又は保守時に計測制御系からの情報を受ける場合には，当該チャンネルをバイパス又はトリップとする。	① ③ ③ ③

No.	頁	規定番号	変更内容	分類
			(3)ディジタル安全保護系から計測制御系への通信は，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。 (4)ディ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。」	
8	2	4.7 故障時の機能	・項番号の繰下げ ・駆動源の喪失を安全保護系の駆動源喪失と明確化し、フェイルセーフの記載のほかにフェイルアズイズを追加 「4.6 故障時の機能 ディジタル安全保護系は，駆動源の喪失，系の遮断及びその他の不利な状況になっても最終的に原子炉施設が安全な状態に落ち着く設計とすること。」 →「4.7 故障時の機能 ディジタル安全保護系は，その駆動源の喪失，系の遮断及びその他の不利な状況になっても，最終的に原子炉施設を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，原子炉施設の安全上支障がない状態を維持できる設計とすること。」	④ ③
9	2	4.8 試験可能性	・項番号の繰下げ、表現の明確化 「4.7 試験可能性 ディジタル安全保護系は，安全保護機能の健全性及び多重性の維持が確認できるように原子炉運転中でも試験ができる機能を有する設計とすること。」 →「4.8 試験可能性 ディジタル安全保護系は，安全保護機能の健全性及び多重性の維持が確認できるように，原子炉運転中でも各チャンネルが独立に試験ができる設計とすること。」	①
10	3	4.9 外的要因	・項番号の繰下げ ・題目を外的要因に変更し、環境条件、耐震性、その他の外的要因に分けて記載し、溢水防護上の措置をその他の外的要因に追加 ・外的要因に対する設計の確証規定を追加 「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。」	④ ③ ③

No.	頁	規定番号	変更内容	分類
			→「4.9 外的要因 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 4.9.2 耐震性 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を有すること。 4.9.3 その他の外的要因 ディジタル安全保護系は，火災防護上の措置及び溢水防護上の措置を考慮した設計とすること。 4.9.4 設計の確証 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ディジタル安全保護系が機能を維持できることを確証すること。」	
		（解説-10）外的要因（関連規格・指針）	・題目を記載 ・耐サージ性に関する「原子力発電所の耐雷指針：JEAG4608-2007」を削除 ・耐震性に関する規格を「原子力発電所耐震設計技術指針[重要度分類・許容応力編]：JEAG4601・補-1984」から「原子力発電所耐震設計技術規程：JEAC4601-2015」に変更 ・火災防護の規格に「原子力発電所の火災防護規程：JEAC4626-2010」を追加し、原子力発電所の火災防護指針：JEAG4607-1999」を「原子力発電所の火災防護指針：JEAG4607-2010」に変更 ・溢水防護上の措置の規格として「原子力発電所の内部溢水影響評価ガイド：平成 25 年 6 月 19 日原子力規制委員会決定」を追加 「(解説-8) 耐震性，耐サージ性，火災防護上の措置については，以下の規格，指針を参照する。 耐震性：「発電用原子炉施設に関する耐震設計審査指針：平成 18 年 9 月 19 日原子力安全委員会決定」，「原子力発電所耐震設計技術指針[重要度分類・許容応力編]：JEAG4601・補-1984」 耐サージ性：「原子力発電所の耐雷指針：JEAG4608-2007」 火災防護上の措置：「発電用軽水型原子炉施設の火災防護に関する審査指針：昭和 55 年 11 月 6 日原子力安全委員会決定，一部改訂平成 19 年 12 月 27 日原子力安全委員会」，「原子力発電所の火災防護指針：JEAG4607-1999」」 →「(解説-10) 外的要因（関連規格・指針）	④ ③ ② ③ ② ③

No.	頁	規定番号	変更内容	分類
			耐震性，火災防護上の措置及び溢水防護上の措置については，以下の規格，指針を参照する。 耐震性：「発電用原子炉施設に関する耐震設計審査指針：平成 18 年 9 月 19 日原子力安全委員会決定」，「原子力発電所耐震設計技術規程：JEAC4601-2015」 火災防護上の措置：「発電用軽水型原子炉施設の火災防護に関する審査指針：昭和 55 年 11 月 6 日原子力安全委員会決定，一部改訂平成 19 年 12 月 27 日原子力安全委員会」，「原子力発電所の火災防護規程：JEAC4626-2010」，「原子力発電所の火災防護指針：JEAG4607-2010」，「実用発電用原子炉及びその附属施設の火災防護に係る審査基準：平成 25 年 6 月 19 日原子力規制委員会決定」 溢水防護上の措置：「原子力発電所の内部溢水影響評価ガイド：平成 25 年 6 月 19 日原子力規制委員会決定」」	
11	3	4.10 非常用電源の使用	・項番号の繰下げ ・外部電源系が喪失した場合あるいは短時間の全交流動力電源喪失の場合でも安全保護機能を果たすことが可能なようにする規定を削除し、非常用所内電源系からの給電を明確化 「4.9 非常用電源の使用 ディジタル安全保護系は，外部電源系が喪失した場合あるいは短時間の全交流動力電源喪失の場合でも安全保護機能を果たすことが可能なように，非常用所内電源系より給電される設計とすること。」 →「4.10 非常用電源の使用 ディジタル安全保護系は，非常用所内電源系より給電される設計とすること。」	④ ③
12	3	4.11 設定値の変更	・項番号の繰下げ ・作動設定値を変更する必要がある場合に、手動による変更ができる設計から適切な変更が可能な設計に修正 「4.10 設定値の変更 ディジタル安全保護系は，運転条件に応じた適切な保護を行うために設定値を変更する必要がある場合には，手動にて作動設定値を変更できる設計とすること。」 →「4.11 設定値の変更 ディジタル安全保護系は，運転条件に応じた適切な保護を行うために設定値を変更する必要がある場合には，適切な設定変更が可能な設計とすること。」	④ ③
13	3	4.12 入力変数の選定	・項番号の繰下げ ・規定の主語を「ディジタル安全保護系の入力」から「ディジタル安全保護系」に変更 「4.11 入力変数の選定	④ ①

No.	頁	規定番号	変更内容	分類
			ディジタル安全保護系の入力は，実用上可能な限り，その把握すべき変数の直接検出によって得られる信号である設計とすること。」 →「4.12 入力変数の選定 ディジタル安全保護系は，実用上可能な限り，その把握すべき変数の直接検出によって得られる信号を用いた設計とすること。」	
14	3	4.13 保護動作の完全性	・項番号の繰下げ ・保護動作が完全に終了するまで作動信号を継続する設計とすることを明確化 「4.12 保護動作の完全性 ディジタル安全保護系は，その保護動作が一度開始されたならばそれが完全に終了する設計であること。なお，通常運転状態への復帰は，運転員の操作によって行う設計とすること。」 →「4.13 保護動作の完全性 ディジタル安全保護系は，その保護動作が一度開始されたならばその動作が完全に終了するまで作動信号を継続する設計とすること。なお，通常運転状態への復帰は，運転員の操作によって行う設計とすること。」	④ ①
15	3	4.14 手動操作	・項番号の繰下げ、表現の明確化 「4.13 手動操作 ディジタル安全保護系は，必要な場合に手動でも原子炉停止系又は工学的安全施設の作動を行うことができる設計であること。この場合，実用上可能な限り自動保護回路の故障によって手動操作の機能が損なわれない設計とすること。」 →「4.14 手動操作 ディジタル安全保護系は，必要な場合に手動でも原子炉停止系（原子炉の緊急停止機能）及び工学的安全施設の作動を行うことができる設計とすること。この場合，実用上可能な限り自動保護回路の故障によって手動操作の機能が損なわれない設計とすること。」	①
16	3	4.15 動作及びバイパスの表示	・項番号の繰下げ、表現の明確化 「4.14 動作及びバイパスの表示 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であること。システム構成機器又はチャンネルがバイパス又は使用状態から取外しされているときは，それが連続的に中央制御室に表示される設計とすること。」 →「4.15 動作及びバイパスの表示	①

No.	頁	規定番号	変更内容	分類
			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。システム構成機器又はチャンネルが，バイパス又は使用状態から取り外しされている場合は，それが連続的に中央制御室に表示される設計とすること。」	
17	4	4.16 自己診断機能	・項番号の繰下げ 「4.15 自己診断機能 （略）」 →「4.16 自己診断機能 （略）」	④
		（解説-15）自己診断機能	・題目を記載、表現の明確化 「（解説-11） 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や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。 （略） 自己診断の例として，ウォッチドックタイマ，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。」 →「（解説-15）自己診断機能 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。 （略） 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。」	①
18	4	4.17 ソフトウェアの管理外の変更の防止	・題目及び規定の防護措置を防止に変更 「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。」 →「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。」	①

No.	頁	規定番号	変更内容	分類
		（解説-16）ソフトウェアの管理外の変更の防止	・題目を記載、防護措置を防止に変更 「(解説-12) 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 →「(解説-16) ソフトウェアの管理外の変更の防止 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」	①
19	4	4.18 不正アクセス行為等の被害の防止	・外部ネットワークとの遮断規定を削除し、不正アクセス行為等による被害を防止するために必要な措置を講じる設計とする規定を追加 「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。」 →「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 （解説-17）不正アクセス行為等の被害の防止 不正アクセス行為等の被害の防止に必要な措置の例としては，以下がある。 (1) 外部ネットワーク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。 (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

No.	頁	規定番号	変更内容	分類
			(3) 解説-16 の(2)鍵付きスイッチの設置及び(3)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。」	
20	4	4.19 品質保証	・項番号の繰下げ、題目を品質管理から品質保証に変更 ・「検証及び妥当性確認活動」を「V&V 活動」に変更 「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」 →「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」	① ①
		（解説-18）品質保証活動	・題目を記載 ・「原子力発電所における安全のための品質保証規程：JEAC 4111-2003」並びに「原子力発電所における安全のための品質保証規程（JEAC 4111-2003）の適用指針 －原子力発電所の運転段階－：JEAG 4121-2005[2007 年追補版]」から「原子力安全のためのマネジメントシステム規程：JEAC 4111-2013」及び「原子力安全のためのマネジメントシステム規程（JEAC 4111-2013）の適用指針：JEAG 4121-2015[2018 年追補版]」に変更 「(解説-13) ディジタル安全保護系の品質保証活動については，「原子力発電所における安全のための品質保証規程：JEAC 4111-2003」並びに「原子力発電所における安全のための品質保証規程（JEAC 4111-2003）の適用指針 －原子力発電所の運転段階－：JEAG 4121-2005[2007 年追補版]」の附属書「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」を参照する。 市販ディジタル計算機，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。(略)」 →「(解説-18) 品質保証活動 ディジタル安全保護系の品質保証活動については，「原子力安全のためのマネジメントシステム規程：	① ②

No.	頁	規定番号	変更内容	分類
			JEAC 4111-2013」及び「原子力安全のためのマネジメントシステム規程（JEAC 4111-2013）の適用指針：JEAG 4121-2015[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」を参照する。 市販ディジタル計算機，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。 (略)」	
		4.19.1 ソフトウェアライフサイクル （解説-19）ソフトウェアライフサイクル	・項番号の繰下げ 「4.18.1 ソフトウェアライフサイクル（略)」 →「4.19.1 ソフトウェアライフサイクル（略)」	①
			・題目を記載、表現の明確化 ・ソフトウェア単体では確認できない内容をシステムとして確認する範囲については、事前に計画することを規定 ・廃止されたソフトウェアの誤使用防止措置を講じる規定を追加 「(解説-14) ディ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 ディ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，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：(略) 製作プロセス：(略) 試験プロセス：(略) 装荷プロセス：(略) 運転プロセス：(略) 変更プロセス：(略) 廃止プロセス：(略) ソフトウェアライフサイクルプロセスには，下記の理由により，開発，保守プロセスを定義していない。 開発プロセス：(略)	① ③ ③

No.	頁	規定番号	変更内容	分類
			保守プロセス：(略) (2) 各プロセスで実施すべき品質管理項目 （略） 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 （略） 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 （略） 5）運転プロセス （略） 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・試験のプロセスに従う。 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。 （略）」 →「(解説-19) 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 ディ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。	

No.	頁	規定番号	変更内容	分類
			(a)設計プロセス：(略) (b)製作プロセス：(略) (c)試験プロセス：(略) (d)装荷プロセス：(略) (e)運転プロセス：(略) (f)変更プロセス：(略) (g)廃止プロセス：(略) 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。 (h)開発プロセス：(略) (i)保守プロセス：(略) (2) 各プロセスで実施すべき品質管理項目 （略） (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 （略） (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 （略） (e) 運転プロセス （略） (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。	

No.	頁	規定番号	変更内容	分類
			(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。 （略）」	
		4.19.2 ソフトウェア構成管理	・項番号の繰下げ、記載の明確化 「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。」 →「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。」	①
		（解説-20）ソフトウェアの構成管理	・題目を記載 ・構成管理の対象に V&V 手順及び V&V 結果を追加し、ソフトウェア供給者に対する監査又は審査をソフトウェア構成管理のレビュー又は審査に変更 ・ソフトウェア及び関連文書について，管理対象要素の例に「V&V 手順／V&V 結果」を追加 「(解説-15) 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) （略） (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	① ③ ③

No.	頁	規定番号	変更内容	分類
			・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。」 →「(解説-20) ソフトウェアの構成管理 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。 具体的には以下に示す。 (1) (略) (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	

No.	頁	規定番号	変更内容	分類
			・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	・項番号の繰下げ、題目を記載、表現の明確化 ・V&V を行う体制を「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」から「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」に変更 「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れ，再利用の妥当性を示す根拠が文書化されていること。」 →「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。」	① ③
		（解説-21） V&V (手順)	・題目を記載 ・ディジタル安全保護系の供給者に対する品質保証活動を要求 ・V&V としての検証は設計プロセス及び製作プロセス、V&V としての妥当性確認は試験プロセスと明確化 「(解説-16) 検証及び妥当性確認については，「ディジタル安全保護系の検証及び妥当性確認に関する指針：JEAG 4609-2008」を参照する。新規設計や変更により検証及び妥当性確認が必要なプロセスとして，設計，製作，試験，変更を対象とする。	① ③ ③

No.	頁	規定番号	変更内容	分類
			なお，ソフトウェアライフサイクルプロセスにおける検証及び妥当性確認の対象を参考図３に示す。」 →「(解説-21) 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，ディジタル安全保護系の供給者は，「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]」に従った一般の品質保証活動を実施した上で，ディジタル安全保護系のソフトウェアに対し V&V 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」を参照する。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，参考図３に示す設計，製作，試験及び変更がある。」	
		（解説-22） V&V（独立性）	・題目を記載 ・V&V を実施する個人又はグループの力量及び経済面，工程管理に関する制約を受けないことを追加 「(解説-17) 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。 (1)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。 (2)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。」 →「(解説-22) 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。」	① ③
		（解説-23） V&V	・題目を記載、表現の明確化 ・V&V に係る文書は構成管理計画の中で保存及び管理を追加 「(解説-18) 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。」	① ③

No.	頁	規定番号	変更内容	分類
		（文書化）	→「(解説-23) 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。」	
21	5	5.留意事項	・「ディジタル安全保護系は，「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，共通要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考えられる」との記載を追加し、「ハードウェア設備」を「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」に変更 「深層防護の観点から，より一層の信頼性向上を図るため,原子炉設置者が合理的な範囲でハードウェア設備を設けること。」 →「ディジタル安全保護系は，「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，共通要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考えられるが，深層防護の観点から，合理的な範囲で，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。」	③

２．日本電気協会　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 における同 JEAG 4609-2008 からの変更点一覧

変更点の分類：

① 記載の適正化のための変更（用語の統一、表現の明確化、題目の修正、条項番号の変更、単位換算の見直し、記号の変更）

② 引用されている法令、規格の引用年版等の変更（年版改正の反映、新たな規格の反映）

③ 国内外の知見の反映等（国内外における試験研究成果の反映等）

④ 技術評価対象外

No.	頁	規定番号	変更内容	分類
1	2	1. 目的	・表現の明確化 「1. 目的 原子力発電所の安全保護系にディジタル計算機を適用するに当たっては，ソフトウェアの品質を確保することが重要である。このため本指針では，ディジタル計算機を適用した安全保護系（以下これを「ディジタル安全保護系」という）のソフトウェアの設計・製作・試験・変更の各プロセスにおいて，安全保護上要求される機能が正しく確実に実現されていることを保証する活動に関して，検証と妥当性確認に対する基本的事項を示したものである。」 →「1. 目的 原子力発電所の安全保護系にディジタル計算機を適用するに当たっては，ソフトウェアの品質を確保することが重要である。このため本指針は，ディジタル安全保護系のソフトウェアの設計，製作，試験及び変更の各プロセスにおいて，安全保護上要求される機能が正しく確実に実現されていることを保証する活動である V&V に対する基本的事項を示すものである。」	①
2	2	2. 適用範囲	・表現の明確化 ・品質保証活動の指針 JEAG4121 を削除（3.3 V&V に移行） 「2. 適用範囲 本指針は，原子力発電所の計測制御装置のうち，安全保護系に適用するディジタル計算機を対象とする。 更に，ディジタル計算機は，ハードウェアと，このハードウェア上で動作するソフトウェアによって構成され，ソフトウェアは，安全保護系設備としての機能を実現するソフトウェアとそれ以外に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によって構成される。 このうち安全保護系設備としての機能を実現するソフトウェアは，設備ごと・プラントごとに異なったものとなる可能性があり，特にきめの細かい管理を行い，その品質について第三者への立証性を確保する	① ①

No.	頁	規定番号	変更内容	分類
			ことが必要と考えられる。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を適用範囲とする。 なお，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は，ハードウェアとともに，「原子力発電所における安全のための品質保証規程（JEAC4111-2003）の適用指針－原子力発電所の運転段階－：JEAG4121-2005[2007 年追補版]」の附属書「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を実施する。」 →「2. 適用範囲 本指針は，原子力発電所の計測制御装置のうち，ディジタル安全保護系を対象とする。 さらに，ディジタル計算機は，ハードウェアと，このハードウェア上で動作するソフトウェアによって構成され，ソフトウェアは，安全保護系設備としての機能を実現するソフトウェアとそれ以外に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によって構成される。 このうち安全保護系設備としての機能を実現するソフトウェアは，設備ごと，プラントごとに異なったものとなる可能性があり，特にきめの細かい管理を行い，その品質について第三者への立証性を確保することが必要と考えられる。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。 なお，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は，ハードウェアとともに，基本的な原子力品質保証活動を実施する。」	
3	2	3. 用語の定義 3. 1 ディジタル計算機	・表現の明確化 「3. 1 ディジタル計算機 内蔵されたプログラムによって制御され，人手の介入なしにディジタルデータの算術演算や論理演算などの計算を行う装置。」 →「3. 1 ディジタル計算機 内蔵されたプログラムによって制御され，人手の介入なしにディジタルデータの算術演算，論理演算等の計算を行う装置。」	①
4	2	3. 2 安全保護系	・安全保護系の定義を追加 「(なし)」 →「3. 2 安全保護系 原子炉施設の異常状態を検知し，必要な場合，原子炉停止系（原子炉の緊急停止機能），工学的安全施設の作動を直接開始させるよう設計された設備であり，検出器から動作装置入力端子までをいう。」	④

No.	頁	規定番号	変更内容	分類
5	2	3. 3 V&V	・V&V の定義を追加 「(なし)」 →「3. 3 V&V Verification and Validation の略。 ディジタル安全保護系のソフトウェアに対して，「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]」に基づいた品質保証活動を前提にして，設計，製作及び試験に携わった者以外の個人又はグループが実施する検証及び妥当性確認。」	④
6	3	3. 4 検証	・表現の明確化 ・用語「検証」の定義を指針内限定とし、一般的な品質保証の用語と区別 「3. 2 検証 ディジタル計算機を適用した対象システムのソフトウェアの設計・製作の各プロセスにおける各ステップの製品が，直前のステップから課せられた要求を満たしているか否かのチェック作業。」 →「3. 4 検証 ディジタル計算機を適用した対象システムのソフトウェアの設計，製作の各プロセスにおける各ステップの製品が，直前のステップから課せられた要求を満たしているか否かの確認作業。 本用語は，一般的な品質保証の用語（JIS Q 9000-2015 を参照）でもあるが，本指針内に限り上記の定義に従うものとする。」	① ②
7	3	3. 5 妥当性確認	・表現の明確化 ・用語「妥当性確認」の定義を指針内限定とし、一般的な品質保証の用語と区別 「3. 3 妥当性確認 ソフトウェアとハードウェアを統合して製作された最終製品としての計算機システムが，機能要求，性能要求，インターフェイス要求を満たしていることの，試験プロセスにおける確認作業。」 →「3. 5 妥当性確認 ソフトウェアとハードウェアを統合して製作された最終製品としての計算機システムが，機能要求，性能要求及びインタフェース要求を満たしていることの，試験プロセスにおける確認作業。 本用語は，一般的な品質保証の用語でもあるが，本指針内に限り上記の定義に従うものとする。」	① ①
8	－	－	・文書の定義を削除 「3. 4 文書	④

No.	頁	規定番号	変更内容	分類
			品質保証に対する活動，要求事項，要領若しくは結果を明確にし，規定し，報告し又は証明するための記述されたあるいは図示された情報。」 →「(なし)」	
9	3	4. V&V	・表現の明確化 「4. 検証及び妥当性確認 ディジタル安全保護系に装荷するソフトウェアは，検証及び妥当性確認を実施して，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が確認されるべきである。 ソフトウェアに関する検証及び妥当性確認は，以下の手法によるものとする。」 →「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。」	①
10	3	4. 1 V&V の目的と概要	・表現の明確化 ・V&V の対象規格を JEAC4620 から JEAC4620 等に変更し、V&V 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ことを追加 ・ハードウェア・ソフトウェアの設計要求仕様にハードウェア・ソフトウェア統合要求仕様が含まれることを解説から移行 「4. 1 検証及び妥当性確認の目的 (1)検証及び妥当性確認は，JEAC4620-2008（以下「JEAC4620」という）のディジタル安全保護系システム要求事項が設計・製作・試験・変更の各プロセスにおいて正しく実現されていることを保証するための活動である。 (2)設計・製作プロセスの各ステップごとに上位仕様と下位仕様の整合性チェックを主体として，下記の観点から検証作業を行う。 (a)ディジタル安全保護系システム要求事項がハードウェア・ソフトウェアの設計要求仕様に正しく反映されていること。 (b)上記設計要求仕様に基づいてソフトウェアが設計製作されていること。 (c)検証及び妥当性確認が可能なソフトウェア設計となっていること。 (3)必要な検証を経て製作されたソフトウェアをハードウェアと統合した後の全体システムについて，最終的に JEAC4620 のディジタル安全保護系システム要求事項が正しく実現されていることの確認をする	① ③ ① ①

No.	頁	規定番号	変更内容	分類
			ために，試験プロセスにおいて，妥当性確認作業を行う。」 →「4．1 V&V の目的と概要 (1)V&V は，JEAC4620 等のディジタル安全保護系に対する要求事項が設計，製作，試験及び変更の各プロセスにおいて正しく実現されていることを保証するための活動である。V&V 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。 (2)設計・製作作業のステップごとに上位仕様と下位仕様の整合性チェックを主体として，以下の観点から検証作業を行う。 (a)ディジタル安全保護系に対する要求事項がハードウェア・ソフトウェアの設計要求仕様（ハードウェア・ソフトウェア統合要求仕様，ハードウェア設計要求仕様及びソフトウェア設計要求仕様からなる。）に正しく反映されていること。 (b)上記設計要求仕様に基づいてソフトウェアが設計，製作されていること。 (c)V&V が可能なソフトウェア設計となっていること。 (3)必要な検証を経て製作されたソフトウェアをハードウェアと統合した後の全体システムについて，最終的に 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実現されていることの確認をするために，試験プロセスにおいて，妥当性確認作業を行う。」	
11	3	4．2 V&V の実施	・題目の変更、表現の明確化 ・V&V を実施する個人又はグループの力量及び経済面，工程管理に関する制約を受けないことを追加 ・なお書きで規定していた設計・製作者の各作業項目及び検証者の各作業項目を削除 ・図１の設計・製作作業の範囲を示す一点鎖線の範囲の各ステップに設計検証を追加 「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の変更点は添付新旧対照表を参照) 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	① ③ ③ ③

No.	頁	規定番号	変更内容	分類
			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 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） （略） (d)ソフトウェア設計検証（検証 3） （略） (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，JEAC4620 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	

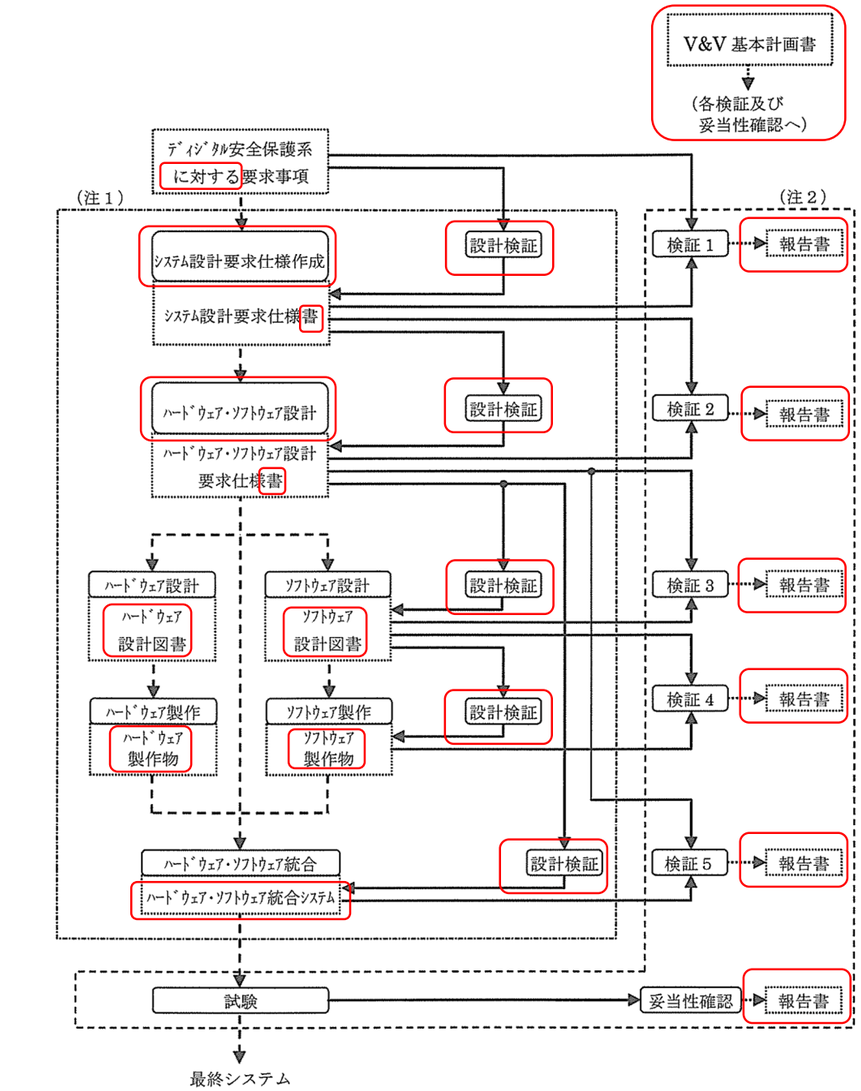
No.	頁	規定番号	変更内容	分類
			成，ソフトウェア設計，ソフトウェア製作，ハードウェア・ソフトウェア統合の各作業を行い，検証者は検証・妥当性確認基本計画立案，システム設計要求仕様検証，ハードウェア・ソフトウェア設計要求検証，ソフトウェア設計検証，ソフトウェア製作検証，ハードウェア・ソフトウェア統合検証及び妥当性確認の各作業を行う。 (3)文書管理 検証及び妥当性確認を実施する上で以下の文書化を行う。 (a)設計の文書化 図１に示される各ステップごとに必要な設計・製作に係わる内容を明確にし文書化する。 (b)検証及び妥当性確認作業の文書化 検証及び妥当性確認作業の開始に当たり，検証・妥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」 →「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。 (図１の変更点は別添新旧対照表を参照) 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	

No.	頁	規定番号	変更内容	分類
			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） （略） (d)ソフトウェア設計検証（検証 3） （略） (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	

No.	頁	規定番号	変更内容	分類
			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。 (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」	
		（解説-10）ソフトウェアツール	・適用指針の年版変更 ・ソフトウェアの品質確保に適用する品質保証仕様書の項番号を「7.6 監視機器及び測定機器の管理」から「7.1.5 監視及び測定のための資源」に変更 「(解説-9) ソフトウェアツール ソフトウェアツールの品質の確保とは，「原子力発電所における安全のための品質保証規程（JEAC4111-2003）の適用指針－原子力発電所の運転段階－：JEAG4121-2005[2007 年追補版]」の附属書「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」の「7.6 監視機器及び測定機器の管理」に基づいた品質保証活動の結果として確保することである。」 →「(解説-10) ソフトウェアツール ソフトウェアツールの品質の確保とは，「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]」の附属書－１「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」の「7.1.5 監視及び測定のための資源」に基づいた品質保証活動の結果として確保することである。」	② ③
12	6	4．3 ソフトウェア再利用時の V&V	・表現の明確化 「4．3 ソフトウェア再利用時の検証及び妥当性確認 ソフトウェアの設計・製作の各作業において，既存設計を再利用する際には，再利用範囲及び再利用の妥当性を示す根拠を明確にする。 この場合，既存設計の際の検証結果を利用することにより，4.2 節記載の検証作業をその再利用の範囲において代替することが可能である。但し検証 5 及び妥当性確認は実施する。」 →「4．3 ソフトウェア再利用時の V&V ソフトウェアについて既存設計を再利用する際には，再利用範囲及び再利用の妥当性を示す根拠を明確	①

No.	頁	規定番号	変更内容	分類
			にする。 　この場合，既存設計の際の検証結果を利用することにより，4.2 の検証作業をその再利用の範囲において代替することが可能である。ただし，検証 5 及び妥当性確認は実施する。」	
13	6	5. 変更管理	・表現の明確化 「5. 変更管理 (1)設計要求仕様の変更及びソフトウェアの変更に関する管理方法をあらかじめ文書化し，適切な管理のもとに変更を行う。変更を行う場合には，変更理由，変更箇所等を文書化し，変更の影響範囲を明確にした上で，変更を実施し，必要に応じて，変更箇所及び変更の影響を受ける部分について検証及び妥当性確認作業を再度実施する。 (2) (略)」 →「5. 変更管理 (1)設計要求仕様の変更及びソフトウェアの変更に関する管理方法をあらかじめ文書化し，適切な管理のもとに変更を行う。変更を行う場合には，変更理由，変更箇所等を文書化し，変更の影響範囲を明確にした上で，変更を実施し，必要に応じて，変更箇所及び変更の影響を受ける部分について V&V 作業を再度実施する。 (2) (略)」	①

デジタル安全保護系 V&V 指針 2020

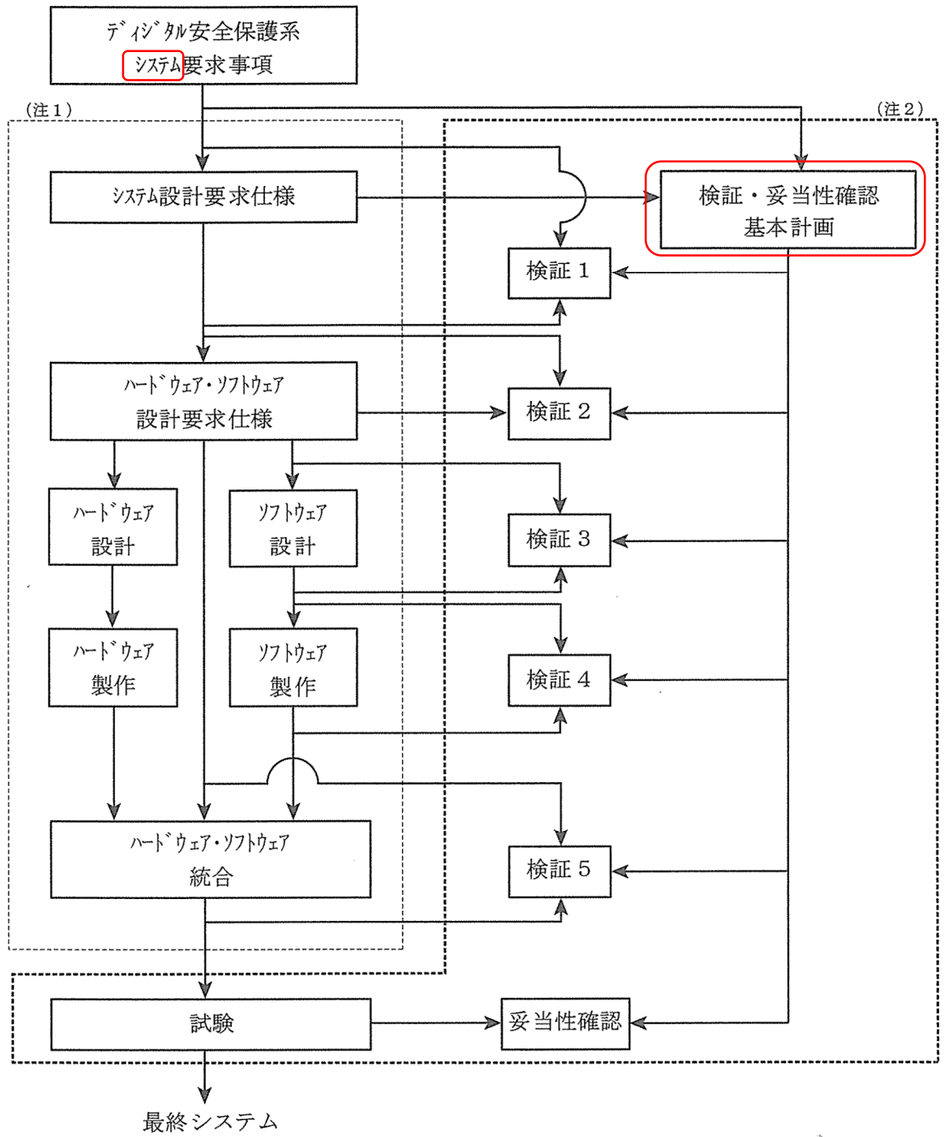


検証１・・・システム設計要求仕様検証
検証２・・・ハードウェア・ソフトウェア設計要求仕様検証
検証３・・・ソフトウェア設計検証
検証４・・・ソフトウェア製作検証
検証５・・・ハードウェア・ソフトウェア統合検証

(注１) は，設計・製作作業の範囲を示す。(解説-6，解説-7)
(注２) は，V&V の範囲を示す。
(注３) ---→ は，設計，製作及び試験の作業段階のつながりを示す。
(注４) ⟶ は，情報の流れを示す。

図１ V&V 概要

デジタル安全保護系 V&V 指針 2008



検証１・・・システム設計要求仕様検証
検証２・・・ハードウェア・ソフトウェア設計要求仕様検証
検証３・・・ソフトウェア設計検証
検証４・・・ソフトウェア製作検証
検証５・・・ハードウェア・ソフトウェア統合検証

(注１) は，設計・製作作業の範囲を示す。
(注２) は，検証・妥当性確認作業の範囲を示す。

図１ 検証・妥当性確認概要

別添

添付資料－２　引用規格の変更に関する確認結果

１．デジタル安全保護系規程 2020 における関連規格のデジタル安全保護系規程 2008 からの変更に関する確認結果

No.	関連規格の名称	規定番号	変更内容	確認結果
1	JEAC 4111-2013 原子力安全のためのマネジメントシステム規程	3.3 V&V （解説-18）品質保証活動 （解説-21）V&V(手順)	（3.3 項及び（解説-21）には追加） 「原子力発電所における安全のための品質保証規程」→「原子力安全のためのマネジメントシステム規程」と名称変更し、年版を 2003 年版→2013 年版に変更	「4.1.9 検証及び妥当性確認（V&V）」にて技術評価
2	JEAG 4121-2015[2018 年追補版] 原子力安全のためのマネジメントシステム規程（JEAC 4111-2013）の適用指針	3.3 V&V （解説-18）品質保証活動 （解説-21）V&V(手順)	（3.3 項及び（解説-21）には追加） 「原子力発電所における安全のための品質保証規程（JEAC 4111-2003）の適用指針 －原子力発電所の運転段階－」→「原子力安全のためのマネジメントシステム規程（JEAC 4111-2013）の適用指針」と名称変更し、年版を 2005[2007 年追補版]→2015[2018 年追補版]に変更	「4.1.9 検証及び妥当性確認（V&V）」にて技術評価
3	JEAG 4608-2007 原子力発電所の耐雷指針	（解説-10）外的要因（関連規格・指針）	2007 年版→削除	「4.1.11 環境条件の考慮」にて技術評価
4	JEAC 4601-2015 原子力発電所耐震設計技術規程	（解説-10）外的要因（関連規格・指針）	「 JEAG 4601・補-1984 原子力発電所耐震設計技術指針[重要度分類・許容応力編]」→「 JEAC 4601-2015 原子力発電所耐震設計技術規程」と名称及び年版変更	「4.1.11 環境条件の考慮」にて技術評価
5	JEAC 4626-2010 原子力発電所の火災防護規程	（解説-10）外的要因（関連規格・指針）	2010 年版(追加)	「4.1.11 環境条件の考慮」にて技術評価
6	JEAG 4607-2010 原子力発電所の火災防護指針		1999 年版→2010 年版	
7	実用発電用原子炉及びその附属施設の火災防護に係る審査基準：平成 25 年 6 月 19 日原子力規制委員会決定	（解説-10）外的要因（関連規格・指針）	(追加)	－(確認不要)

8	原子力発電所の内部溢水影響評価ガイド：平成 25 年 6 月 19 日原子力規制委員会決定	（解説-10）外的要因（関連規格・指針）	（追加）	－（確認不要）
9	JEAG 4609-2020 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	（解説-21）V&V（手順）	「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」→「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」と名称変更し年版を 2008 年版→2020 年版に変更	今回の技術評価対象件名

２．デジタル安全保護系 V&V 指針 2020 における関連規格のデジタル安全保護系 V&V 指針 2008 からの変更に関する確認結果

No.	関連規格の名称	規定番号	変更内容	確認結果
1	JEAC 4111-2013 原子力安全のためのマネジメントシステム規程	3.3 V&V	（追加）	－（用語の定義 3.3 項に記載されているのみであり、技術評価対象外）
2	JEAG 4121-2015[2018 年追補版]原子力安全のためのマネジメントシステム規程（JEAC 4111-2013）の適用指針	3.3 V&V （解説-10）ソフトウェアツール	（3.3 項には追加） 「原子力発電所における安全のための品質保証規程（JEAC 4111-2003）の適用指針 －原子力発電所の運転段階－」→「原子力安全のためのマネジメントシステム規程（JEAC 4111-2013）の適用指針」と名称変更し、年版を 2005[2007 年追補版]→2015[2018 年追補版]に変更	「4.2.1 検証及び妥当性確認（V&V）」にて技術評価
3	JIS Q 9000-2015 品質マネジメントシステム－基本及び用語	3.4 検証	（追加）	－（IS Q 9000-2015 の用語「検証」を除外する意味で記載しており関連規格扱い外）
4	JEAC 4620-2020 安全保護系へのディジタル計算機の適用に関する規程	4．1 V&V の目的と概要 4．2 V&V の実施	2008 年版→2020 年版	今回の技術評価対象件名

添付資料－３　機能的分離（通信の独立性）に関する海外動向との比較

米国においては 2000 年代に高機能統合型の制御室の審査に適用するため、U.S.NRC において DI&C-ISG-04 Highly-Integrated Control Rooms-Communications Issues（HICRc）（以下「ISG」という。）がまとめられ（最新は 2009 年版）、通信の独立性を含む機能的分離はこのガイドの一部として記載されている。また、この内容が民間規格の IEEE Std 7-4.3.2（最新は 2016 年版、以下「IEEE」という）に取り入れられている。これらの最新版とデジタル安全保護系規程 2020 について比較した。

また、デジタル安全保護系規程 2008 の技術評価において参考とした米国 SRP（標準審査指針）7.1（1997 年版）の「計測制御系デジタル計算機を用いた安全系の補足指針[79]」（通信の独立性に関する部分に限る。）についても参考として示した。なお、本 SRP の記載は米国における規制要件ではなく補助ガイドとして記載された部分であり、また米国ではその後削除されている。本 SRP では優先処理回路、機能統合型（多区分型）VDU については記載がないため、①通信の独立性について記載している。

本比較は ISG に記載されたスタッフポジション 35 項目について実施した。比較結果を参考にするにあたっては以下に留意する必要がある。

（１）　ISG 及び IEEE では、これらに記載の 35 の要件全てを考慮する必要があるが、デジタル安全保護系規程 2020 では「(解説-8) 計測制御系との分離」に記載の 4 項目の例示について、何れか１項目の考慮でよいとしている。

（２）　デジタル安全保護系規程 2020 については、対応する項目についてもその要求する内容が大きく異なる場合がある。このため、これに該当する事項について補足を記載した。

また、ISG は高機能統合型の制御室に関するガイドであるため、以下の３区分の要件をまとめている。

①　通信の独立性
②　優先処理回路
③　機能統合型監視操作設備（原文ではステーションと表記）

このため安全保護系を対象とするデジタル安全保護系規程 2020 へ記載すべき範囲とは必ずしも一致しない可能性があるが、①～③は極めて密接に関連する事項であるため、原文の意図を損なわないよう全ての項目について比較評価した。

[79] 平成 17 年 12 月 15 日、原子炉安全小委員会性能規定化検討会配付資料　参考２「原子炉制御室における誤操作防止のための設備面への要求事項及びディジタル計算機の安全保護系への適用に当たっての要求事項について」の資料 10「SRP、国内外の知見を反映した要求事項及び学協会として検討されるべき仕様規定」

① 通信の独立性

米国標準審査指針（SRP） 7.1(1997)[80] 計測制御系デジタル計算機を用いた安全系の補足指針 （通信の独立性に関する部分）	ISG	IEEE	デジタル安全保護系規程 2020
	1.安全機能を他区分に依存しないこと	5.6 独立性	4.5 独立性
	2.他区分の影響を受けないよう保護すること	5.6 独立性	4.5 独立性 4.6 計測制御系との分離
(2)安全グレードのシステムは、試験時を除き、非安全関連グレードのシステムからの情報を受けないこと	3.安全機能を支援強化する場合のみ外部からの通信を許容すること	5.18 単純化*1	(解説-8) 計測制御系との分離(1)～(2)試験時又は保守時を除き計測制御系からの情報を受けない設計とすること、受ける場合には当該チャンネルをバイパス又はトリップとする、（例示）
(4)通信接続の制御装置は発信側システムにあること	4.安全機能と通信の機能を分離すること	5.6.4.1 バッファリング機能	(解説-8) 計測制御系との分離(4) ディ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（例示）
	5.共有メモリのサイクルタイムを考慮すること	5.6.4.1 バッファリング機能	4.3 精度及び応答時間 (解説-8) 計測制御系との分離(4)
(3)双方向情報伝達が適用されている場合、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(handshaking)の失敗によって、ど	6.ハンドシェイク通信を適用しないこと	5.6.4.2 通信の独立性 a)	(解説-8) 計測制御系との分離(3) 発信側のシステムと受信側のシステム間の調整、接続の失敗によって、どちらのシステムも機能的に異常を

[80] U.S.NRC の Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants:LWR Edition - Instrumentation and Controls-Introduction (NUREG-0800,Chapter 7.1 (rev.4, 1997))の II. Acceptance Criteria の No.5

米国標準審査指針（SRP） 7.1(1997)[80] 計測制御系デジタル計算機を用いた安全系の補足指針 (通信の独立性に関する部分)	ISG	IEEE	デジタル安全保護系規程 2020
ちらのシステムも機能的に異常を生じないこと			きたさない設計とする（例示）
	7.受信データを事前に定義し、決定論的振る舞いとすること	5.6.4.2 通信の独立性 b)	－
	8.受信データが他区分の処理に影響しないこと	5.6 独立性	－
	9.受信データの保存は共有メモリの固定位置とすること	5.6.4.2 通信の独立性 c)	
	10.ソフトウエアを改ざんから保護すること	5.6.4.2 通信の独立性 e)～h)	4.18 不正アクセス行為等の被害の防止、(解説-17) 不正アクセス行為等の被害の防止（システム据付以降とされており範囲が限定的)
	11.ソフトウエア命令が送信されないよう保護すること	5.6.4.2 通信の独立性 d)	－
	12.通信障害が悪影響を与えないよう保護すること	5.6.4.2 通信の独立性 i) 1～14	－
	13.受信メッセージの誤り検出、修正をすること	5.6.4.2 通信の独立性 j)	－
(1)冗長安全グレードの装置は一方通行の通信路を介して情報伝達を行うこと	14.重要な(バイタルな)通信は1対1通信とすること	5.6.4.2 通信の独立性 k)	－
	15.固定データセット、定周期の処理とすること	5.6.4.2 通信の独立性 l)	－
	16.接続がない場合にデッドロックとならないこと	5.6.4.2 通信の独立性 m)	－

米国標準審査指針（SRP） 7.1(1997)[80] 計測制御系デジタル計算機を用いた安全系の補足指針 （通信の独立性に関する部分）	ISG	IEEE	デジタル安全保護系規程 2020
	17. 通常時及び事故時の環境条件へ適合すること（放射線・熱を含む）	5.4 機器認定	4.9 外的要因
	18. 不要な機能、複雑な通信を分析し対処すること	5.6.4.2 通信の独立性 n)	－
	19. 全ての機能に必要な通信容量を確保すること	5.6.4.2 通信の独立性 o)	－
	20. 応答時間の計算においてエラー率を考慮すること	5.6.4.2 通信の独立性 p)	－

*1 ISG では安全性向上に寄与する場合に限定して当該区分以外からのデータ伝送を許容するとしており、これが反映された IEEE では、ISG 開発当時の課題であった共通原因故障対策の多様化設備、多区分型監視操作設備について記載(許容)したうえで、一般的な要件として単純化を求めている。

② 優先処理回路

ISG	IEEE	デジタル安全保護系規程 2020
1. 安全系デバイス又はソフトウエアであること	5.5.4 機能優先処理 a)	－
2. 他の部分から独立していること	5.5.4 機能優先処理 b)	－
3, 安全系コマンドを最高の優先順位とし他をオーバライドすること	5.5.4 機能優先処理 c)	－
4. 複数機器を制御する場合には各機器について本要件を適用すること	5.5.4 機能優先処理 d)	－
5. 優先処理モジュール間の通信は区分間通信の要件を満たすこと	5.5.4 機能優先処理 e)	－
6. 設計/試験/保守用ソフトウエアは IEEE7-4.3.2 等の要件を満たすこと	5.5.4 機能優先処理 f)	－
7. 安全機能に係るソフトウエアは、安全系の要件（略）を満足すること	5.5.4 機能優先処理 g)	－
8. 共通原因故障の可能性を最小化するため完全な試験を実施すること	5.16 共通原因故障基準	－

ISG	IEEE	デジタル安全保護系規程 2020
9. 自動試験機能は安全機能を妨げないこと	5.5.4 優先処理回路 h)	－
10. 他の安全区分のコマンド、条件、又は故障によって中断されないこと	5.5.4 優先処理回路	－

③ 機能統合型 VDU

ISG	IEEE	デジタル安全保護系規程 2020
1. 非安全系ステーションと安全系機器との全ての通信は、区分間通信の要件を満たすこと	5.8 情報表示ディスプレイ 5.6 独立性	－
2. 安全系ステーションにおける、自区分以外の機器との全ての通信は、区分間通信の要件を満たすこと	5.8 表示装置ディスプレイ 5.6 独立性	－
3. 非安全系ステーションが安全系機器を制御する場合： ・優先モジュールを介して安全系プラント機器にアクセスすること ・安全系機器が安全機能を実行しているとき影響を与えないこと ・安全区分自身が許可した場合のみ安全機能をバイパスできること ・他区分の機器を制御する安全系ステーションも同様とすること	5.8.1 多区分型監視操作設備の独立性と分離 a) 1)～6)	－
4. 安全系ステーションが他の安全系区分の機器を操作する場合： ・他区分の安全系プラント機器にアクセスする場合の優先モジュールはガイダンスの要件を満たすこと ・他区分の安全系機器の安全機能の実行に影響を与えないこと	5.8.1 多区分型監視操作設備の独立性と分離 b) 1)～6)	－
5. システム間で共有される制御システムリソースの異常・誤動作の結果が安全解析の仮定と一致していること	5.8.2 故障と誤動作	－