資料 1-2

原子力発電所におけるデジタル安全保護回路のソフトウェア共通要因故障緩和対策に関する技術要件書（ATENA 20-ME05 Rev.1）

改定前後比較表

本文

<table>
<tr><th>No</th><th>改定前</th><th>改定後</th><th>変更理由</th></tr>
<tr><td>1.</td><td>改定履歴

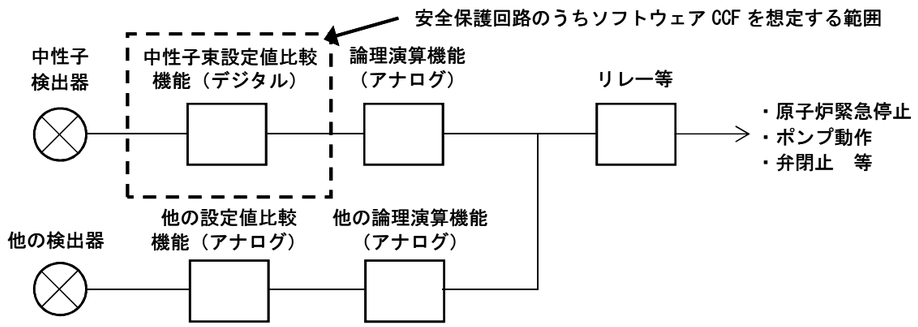
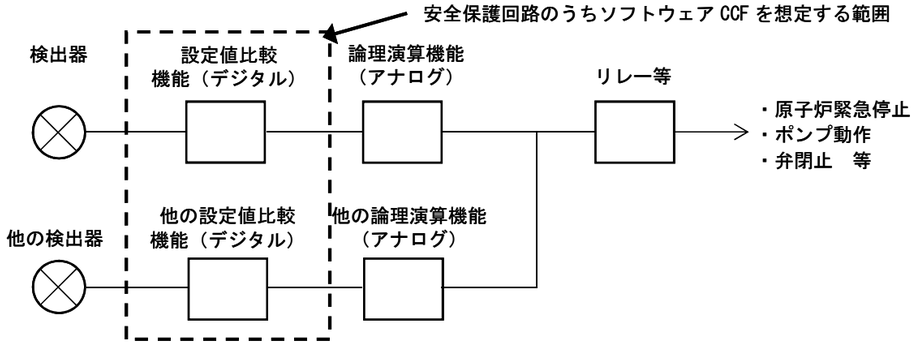
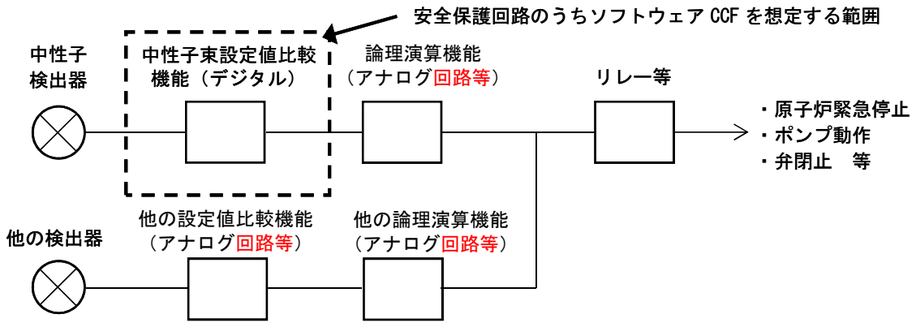
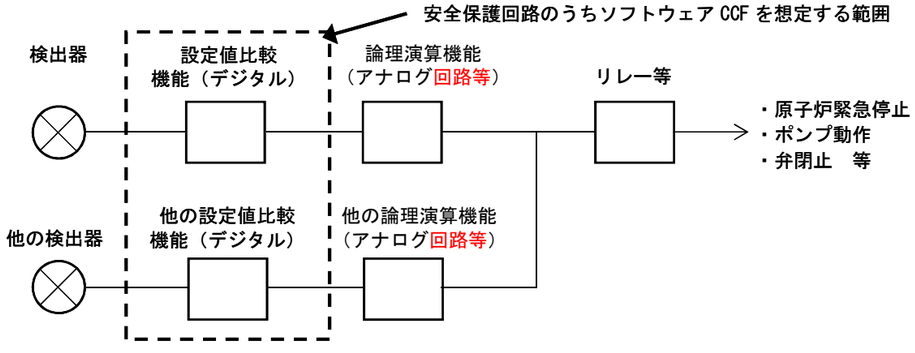
<table><tr><th>改定年月</th><th>版</th><th>改定内容</th><th>備考</th></tr><tr><td>2020 年 12 月 24 日</td><td>Rev.0</td><td>新規制定</td><td></td></tr></table></td><td>改定履歴

<table><tr><th>改定年月</th><th>版</th><th>改定内容</th><th>備考</th></tr><tr><td>2020 年 12 月 24 日</td><td>Rev.0</td><td>新規制定</td><td></td></tr><tr><td>2022 年 10 月 5 日</td><td>Rev.1</td><td>国内外の規格・基準の更新及びこれに伴う参考文献及び関連する記載の見直し，記載の適正化。</td><td></td></tr></table></td><td>改定来歴の反映</td></tr>
<tr><td>2.</td><td>【はじめに】
国内の原子力発電所においては，設備の信頼性及び保守性の向上を目的として，1980 年代頃から常用系設備にデジタル計算機を適用してきており，その良好な運転実績を踏まえ，1990 年代頃からは安全保護回路にもデジタル計算機を適用する事例が増えてきている。デジタル計算機では，設計上の要求機能がソフトウェアによって実現されることから，安全保護回路に適用するソフトウェアの信頼性を確保する取り組みとして，「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」にて引用されている日本電気協会「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）」（以下，「JEAC4620」という。）及び日本電気協会「ディジタル安全保護系の検証及び妥当性確認に関する指針（JEAG4609-2008）」（以下，「JEAG4609」という。）に基づき，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を実施してきた。</td><td>【はじめに】
国内の原子力発電所においては，設備の信頼性及び保守性の向上を目的として，1980 年代頃から常用系設備にデジタル計算機を適用してきており，その良好な運転実績を踏まえ，1990 年代頃からは安全保護回路にもデジタル計算機を適用する事例が増えてきている。デジタル計算機では，設計上の要求機能がソフトウェアによって実現されることから，安全保護回路に適用するソフトウェアの信頼性を確保する取り組みとして，「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」にて引用されている日本電気協会「安全保護系へのディジタル計算機の適用に関する規程（JEAC4620-2020）」（以下，「JEAC4620」という。）及び日本電気協会「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（JEAG4609-2020）」（以下，「JEAG4609」という。）に基づき，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を実施してきた。</td><td>引用文献 JEAC4620/JEAG4609 の改正情報反映</td></tr>
<tr><td>3.</td><td>1.2 概要
しかしながら，特定できない不具合がソフトウェアに内在することを想定した場合に，同一のプラットフォームの使用下においては，ソフトウェア CCF が顕在化することにより，多重化されたデジタル安全保護回路が同時に故障し，安全保護機能が喪失するという可能性は否定できない。</td><td>1.2 概要
しかしながら，特定できない不具合がソフトウェアに内在することを想定した場合に，同一のプラットフォームの使用下においては，ソフトウェア CCF が顕在化することにより，多重化されたデジタル安全保護回路が同時に故障し，安全機能が喪失するという可能性は否定できない。</td><td>記載の適正化（「安全保護機能」を「安全機能」に統一）</td></tr>
</table>

No	改定前	改定後	変更理由
4.	1.4 用語の定義 デジタル安全保護回路　：安全保護回路とは，運転時の異常な過渡変化又は設計基準事故を検知し，これらの事象が発生した場合において，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設備で，多重化されたものをいう。デジタル安全保護回路とは，安全保護回路のうち，ソフトウェアにより設定値比較機能，論理演算機能の全部又は一部を作動させるものをいう。 多様化設備　：運転時の異常な過渡変化又は設計基準事故が発生し，かつソフトウェア CCF により多重化されたデジタル安全保護回路がその安全保護機能を喪失した場合においても，安全保護回路の代替機能として，原子炉停止系統，工学的安全施設等を自動，又は手動により作動させ，設計基準事故の判断基準を概ね満足しながら事象を収束させるために必要となる設備をいう。	1.4 用語の定義 安全保護回路　：安全保護回路とは，運転時の異常な過渡変化又は設計基準事故を検知し，これらの事象が発生した場合において，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設備で，多重化されたものをいう。 デジタル安全保護回路　：デジタル安全保護回路とは，安全保護回路のうち，デジタル計算機のソフトウェアにより安全機能の全部又は一部を作動させるものをいう。なお，安全保護回路に適用するデジタル計算機としては，マイクロプロセッサや FPGA を含む PLD が考えられる。 PLD（Programmable Logic Device）　：内部の論理回路の構造を再構築できる半導体チップの総称をいう。 FPGA（Field Programmable Gate Array）　：PLD の一種で，現場で書き換え可能な論理回路をいう。 多様化設備　：運転時の異常な過渡変化又は設計基準事故が発生し，かつソフトウェア CCF により多重化されたデジタル安全保護回路がその安全機能を喪失した場合においても，安全保護回路の代替機能として，原子炉停止系統，工学的安全施設等を自動，又は手動により作動させ，設計基準事故の判断基準を概ね満足しながら事象を収束させるために必要となる設備をいう。	(1) 用語の定義の適正化。 ✓ 安全保護回路の定義を独立させる。安全保護回路は，検出器から操作端までを含む範囲とし，安全保護系と同等の範囲を指す。 ✓ デジタル安全保護回路は，安全保護回路のうちデジタル計算機を適用したものを指す。改正前の記載では，「設定値比較機能と論理演算機能」だけがデジタル安全保護回路と受けと取られる可能性があった。また，デジタル計算機の適用例としてマイクロプロセッサー，FPGA を含む PLD を記載した。 ✓ デジタル安全保護回路の定義にでてくる FPGA と PLD の定義を追加した。 (2) 記載の適正化（「安全保護機能」を「安全機能」に統一）
5.	2.2 ソフトウェア CCF 発生時の安全保護回路故障モード想定 デジタル安全保護回路のソフトウェアに不具合が潜在しているところで，運転時の異常な過渡変化又は設計基準事故が発生しデジタル安全保護回路の自動作動が要求された時に，その不具合が顕在化しソフトウェア CCF が発生することにより，原子炉停止系統及び工学的安全施設を自動起動する信号が出力されず，安全保護機能が喪失する状態を故障モードとして想定する。 なお，ソフトウェア CCF の発生により安全保護機能が喪失する場合においても，それ以前にデジタル安全保護回路の信号により起動，運転しているポンプ等の機器は，ソフトウェア CCF の影響を受けないものとして機器の作動状態の変化は想定しない。	2.2 ソフトウェア CCF 発生時の安全保護回路故障モード想定 デジタル安全保護回路のソフトウェアに不具合が潜在しているところで，運転時の異常な過渡変化又は設計基準事故が発生しデジタル安全保護回路の自動作動が要求された時に，その不具合が顕在化しソフトウェア CCF が発生することにより，原子炉停止系統及び工学的安全施設を自動起動する信号が出力されず，安全保護回路の安全機能が喪失する状態を故障モードとして想定する。 なお，ソフトウェア CCF の発生により安全保護回路の安全機能が喪失する場合においても，それ以前にデジタル安全保護回路の信号により起動，運転しているポンプ等の機器は，ソフトウェア CCF の影響を受けないものとして機器の作動状態の変化は想定しない。	記載の適正化（「安全保護機能」を「安全保護回路の安全機能」に統一）

No	改定前	改定後	変更理由
6.	3.1 設置要求 ただし，ソフトウェア CCF が発生するおそれがない場合，若しくは運転時の異常な過渡変化又は設計基準事故が発生し，かつ安全保護回路の一部がソフトウェアにより作動するものがある場合で，当該ソフトウェアが機能しない場合を想定しても，他の安全保護機能が作動することにより設計基準事故の判断基準を概ね満足することが有効性評価により確認できる場合には，多様化設備を設けなくてもよい。	3.1 設置要求 ただし，ソフトウェア CCF が発生するおそれがない場合，若しくは運転時の異常な過渡変化又は設計基準事故が発生し，かつ安全保護回路の一部がソフトウェアにより作動するものがある場合で，当該ソフトウェアが機能しない場合を想定しても，他の安全保護回路の安全機能が作動することにより設計基準事故の判断基準を概ね満足することが有効性評価により確認できる場合には，多様化設備を設けなくてもよい。	記載の適正化（「安全保護機能」を「安全保護回路の安全機能」に統一）
7.	3.2 機能要求 多様化設備は，運転時の異常な過渡変化又は設計基準事故が発生し，かつソフトウェア CCF により安全機能が喪失した場合においても，設計基準事故の判断基準を概ね満足できるよう，原子炉停止系統，工学的安全施設等を自動，又は手動で作動させることができなければならい。 さらに，原子炉停止系統，工学的安全施設等を手動により作動させる場合には，運転員が必要な時間内に操作を開始し，判断基準を概ね満足した状態で事象を収束させることができるよう，運転時の異常な過渡変化又は設計基準事故の発生時に安全保護機能動作の異常の発生を認知し，必要な操作の判断を行える機能を設けなければならない。	3.2 機能要求 多様化設備は，運転時の異常な過渡変化又は設計基準事故が発生し，かつソフトウェア CCF により安全機能が喪失した場合においても，設計基準事故の判断基準を概ね満足できるよう，原子炉停止系統，工学的安全施設等を自動，又は手動で作動させることができなければならない。 さらに，原子炉停止系統，工学的安全施設等を手動により作動させる場合には，運転員が必要な時間内に操作を開始し，判断基準を概ね満足した状態で事象を収束させることができるよう，運転時の異常な過渡変化又は設計基準事故の発生時に安全保護回路の安全機能動作の異常の発生を認知し，必要な操作の判断を行える機能を設けなければならない。	(1) 誤記訂正 (2) 記載の適正化（「安全保護機能」を「安全保護回路の安全機能」に統一）
8.	5.1 手順書の整備 運転時の異常な過渡変化又は設計基準事故が発生した際に，デジタル安全保護回路の安全保護機能の喪失によって，原子炉停止系統及び工学的安全系施設が自動作動していないことを運転員が認知した場合に，その要因がソフトウェア CCF の重畳によることを判断した上で，必要な運転操作を実施し，判断基準を概ね満足した状態で事象を収束することができるための手順書を整備すること。	5.1 手順書の整備 運転時の異常な過渡変化又は設計基準事故が発生した際に，デジタル安全保護回路の安全機能の喪失によって，原子炉停止系統及び工学的安全系施設が自動作動していないことを運転員が認知した場合に，その要因がソフトウェア CCF の重畳によることを判断した上で，必要な運転操作を実施し，判断基準を概ね満足した状態で事象を収束することができるための手順書を整備すること。	記載の適正化（「安全保護機能」を「安全機能」に統一）
9.	7. 参考文献 本技術要件書を作成するにあたり，参考とした文献を以下に示す。 (1) U.S. Nuclear Regulatory Commission, “Guidance for evaluation of diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems,” NUREG-0800, Standard Review Plan Chapter 7, Branch Technical Position 7-19, Revision7, AUGUST 2016. (11) 日本電気協会，安全保護系へのディジタル計算機の適用に関する規程（JEAC4620-2008） (12) 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に関する指針（JEAG4609-2008）	7. 参考文献 本技術要件書を作成するにあたり，参考とした文献を以下に示す。 (1) U.S. Nuclear Regulatory Commission, “Guidance for evaluation of diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems,” NUREG-0800, Standard Review Plan Chapter 7, Branch Technical Position 7-19, Revision8, JANUARY 2021. (11) 日本電気協会，安全保護系へのディジタル計算機の適用に関する規程（JEAC4620-2020） (12) 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（JEAG4609-2020） (15) 原子力規制委員会，人間工学設計開発に関する審査及び検査ガイド（令和 3 年 4 月 7 日原規技発第 2104072 号原子力規制委員会決定）	(1) 参考文献の改正情報反映（(1), (11), (12)） (2) 参考文献(15)の追加

解説

No	改定前	改定後	変更理由
10.	解説 2.1 ソフトウェア CCF 想定の範囲 安全保護回路の一部にデジタル計算機を適用した場合は，デジタル計算機を適用した範囲に対してソフトウェア CCF を想定するものとする。 （例－1） 中性子計装にデジタル技術を適用した例を解説図 2.1－1 に示す。安全保護回路のうち，デジタル化された中性子束設定値比較機能に対してソフトウェア CCF の想定を行う。  解説図 2.1－1 中性子計装にデジタル技術を適用した場合のソフトウェア CCF を想定する範囲の例 （例－2） 設定値比較機能にデジタル技術を適用した例を解説図 2.1－2 に示す。安全保護回路のうち，デジタル化された設定値比較機能に対してソフトウェア CCF の想定を行う。  解説図 2.1－2 設定値比較機能にデジタル技術を適用した場合のソフトウェア CCF を想定する範囲の例	解説 2.1 ソフトウェア CCF 想定の範囲 安全保護回路の設定値比較機能，論理演算機能の一部にデジタル計算機を適用した場合は，デジタル計算機を適用した範囲に対してソフトウェア CCF を想定するものとする。 （例－1） 中性子計装にデジタル技術を適用した例を解説図 2.1－1 に示す。中性子計装のデジタル化された中性子束設定値比較機能については，ソフトウェア CCF により当該機能が喪失すると，安全保護回路の安全機能の一部が喪失することから，中性子束設定値比較機能に対してソフトウェア CCF の想定を行う。  解説図 2.1－1　中性子計装にデジタル技術を適用した場合のソフトウェア CCF を想定する範囲の例 （例－2） 設定値比較機能にデジタル技術を適用した例を解説図 2.1－2 に示す。安全保護回路のうち，デジタル化された設定値比較機能に対してソフトウェア CCF の想定を行う。  解説図 2.1－2　設定値比較機能にデジタル技術を適用した場合のソフトウェア CCF を想定する範囲の例	(1) 本文 2.1 との整合性確保。 (2) 記載の適正化（「アナログ回路等」への記載の統一）

No	改定前	改定後	変更理由
11.	解説 2.2 ソフトウェア CCF 発生時の安全保護回路故障モード想定 デジタル安全保護回路のソフトウェアの不具合により誤作動信号が出力される場合は，工学的安全施設の機器の作動，原子炉緊急停止等のプラント状態の変化を伴うことにより，運転員等に認知され，適切に対処可能であることから，故障モードとして想定しない。 これに対し，デジタル安全保護回路のソフトウェアの不具合が不作動側の場合は，運転時の異常な過渡変化又は設計基準事故が発生し自動作動要求があるまで，その異常を認知することが困難であり，ソフトウェア CCF 発生まで不具合の潜在が継続する可能性がある。 したがって，デジタル安全保護回路のソフトウェア CCF 影響緩和対策にあたっては，原子炉停止系統及び工学的安全施設を自動作動する信号が出力されず，安全保護機能が喪失する状態を故障モードとして想定するものである。	解説 2.2 ソフトウェア CCF 発生時の安全保護回路故障モード想定 デジタル安全保護回路のソフトウェアの不具合により誤作動信号が出力される場合は，工学的安全施設の機器の作動，原子炉緊急停止等のプラント状態の変化を伴うことにより，運転員等に認知され，適切に対処可能である。 これに対し，デジタル安全保護回路のソフトウェアの不具合が不作動側の場合は，運転時の異常な過渡変化又は設計基準事故が発生し自動作動要求があるまで，その異常を認知することが困難であり，ソフトウェア CCF 発生まで不具合の潜在が継続する可能性がある。 したがって，デジタル安全保護回路のソフトウェア CCF 影響緩和対策にあたっては，原子炉停止系統及び工学的安全施設を自動作動する信号が出力されず，安全保護回路の安全機能が喪失する状態を主たる故障モードとして想定し，誤作動信号が出力される状態は，起因事象に至る故障モードとして想定を行うものである。	(1) 記載の適正化（「安全保護機能」を「安全保護回路の安全機能」に統一） (2) BTP7-19(Revision8) を参考に，ソフトウェア CCF により誤動作信号が出力される不具合を起因事象に至る故障モードとして想定することの記載の追加（解説 4.2 参照）
12.	解説 3.1 設置要求 「ソフトウェア CCF が発生するおそれがない場合」とは，具体的には，安全保護回路がアナログで構成されている場合，あるいは安全保護回路がソフトウェアで構成されている場合で，ソフトウェア自身が多様性を有していること等によってソフトウェア CCF が発生するおそれがない場合をいう。なお，ソフトウェア自身が多様性を有しているとは，多重化されたデジタル安全保護回路内で異なるハードウェア・OS・アプリケーションで構成されたデジタル技術等を適用した場合をいう。 「運転時の異常な過渡変化又は設計基準事故が発生し，かつ安全保護回路の一部がソフトウェアにより作動するものがある場合で，当該ソフトウェアが機能しない場合を想定しても，他の安全保護機能が作動することにより設計基準事故の判断基準を概ね満足することが有効性評価により確認できる場合」とは，安全保護回路の一部がソフトウェアにより作動するものがあるプラントにおける対処方法の一つを示している。 （省略） 中性子計装にデジタル技術を適用した例を解説 2.1 ソフトウェア CCF 想定の範囲（例－1）に示したように，中性子束設定値比較機能（デジタル）以外の機能が，アナログ回路で構成されているので，ソフトウェア CCF の影響を受けることは無く，運転時の異常な過渡変化又は設計基準事故が発生した場合でも，中性子束設定値比較機能（デジタル）に係る中性子束高スクラム機能等以外の安全保護機能は正常に動作するため，有効性評価により事象を緩和できることを確認できる場合は，多様化設備を設けなくてもよい。	解説 3.1 設置要求 「ソフトウェア CCF が発生するおそれがない場合」とは，具体的には，安全保護回路がアナログ回路等で構成されている場合，安全保護回路がソフトウェアで構成されておりソフトウェア自身が多様性を有している場合又は試験によってソフトウェア CCF が発生するおそれがないと評価される場合をいう。なお，ソフトウェア自身が多様性を有しているとは，多重化されたデジタル安全保護回路内で異なるハードウェア・OS・アプリケーションで構成されたデジタル技術等を適用した場合をいう。また，ソフトウェア CCF が発生するおそれがないと評価するための試験要件を添付書類 3 に示す。 「運転時の異常な過渡変化又は設計基準事故が発生し，かつ安全保護回路の一部がソフトウェアにより作動するものがある場合で，当該ソフトウェアが機能しない場合を想定しても，他の安全保護回路の安全機能が作動することにより設計基準事故の判断基準を概ね満足することが有効性評価により確認できる場合」とは，安全保護回路の一部がソフトウェアにより作動するものがあるプラントにおける対処方法の一つを示している。 （省略） 中性子計装にデジタル技術を適用した例を解説 2.1 ソフトウェア CCF 想定の範囲（例－1）に示したように，中性子束設定値比較機能（デジタル）以外の機能が，アナログ回路等で構成されているので，ソフトウェア CCF の影響を受けることは無く，運転時の異常な過渡変化又は設計基準事故が発生した場合でも，中性子束設定値比較機能（デジタル）に係る中性子束高スクラム機能等以外の安全保護回路の安全機能は正常に動作するため，有効性評価により事象を緩和できることを確認できる場合は，多様化設備を設けなくてもよい。	(1) 記載の適正化（「アナログ回路等」への記載の統一） (2) BTP7-19(Revision8) を参考に，100%試験によりソフトウェア CCF が発生するおそれがないと評価されるケースを追加。（添付書類３参照） (3) 記載の適正化（「安全保護機能」を「安全保護回路の安全機能」に統一）

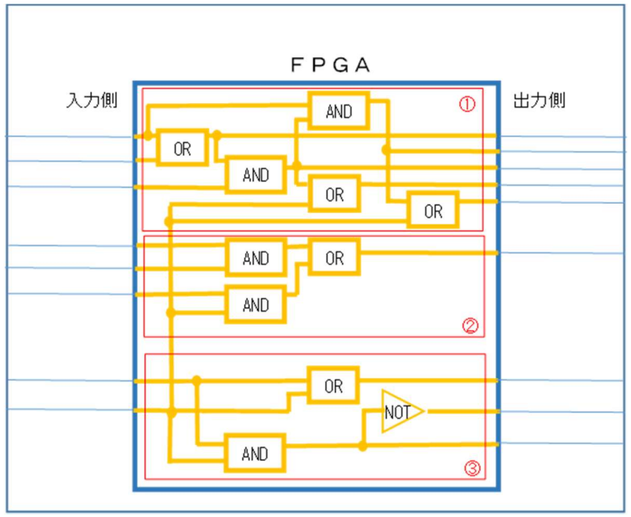
No	改定前	改定後	変更理由
13.	解説 3.3 多様化設備の範囲 多様化設備は，原子炉停止系統，工学的安全施設等を作動させる機能を有する計測制御設備であり，安全保護回路のソフトウェアに対する多様性を含む要求事項を満足した複数の計測制御機能を統合したものであることから，多様化設備の範囲を設計図書で具体的に明確にしておく必要がある。	解説 3.3 多様化設備の範囲 多様化設備は，安全保護回路のソフトウェアにより原子炉停止系統，工学的安全施設等を作動させる機能を代替する計測制御設備であり，安全保護回路のソフトウェアに対する多様性を含む要求事項を満足した複数の計測制御機能が含まれるものであることから，多様化設備の範囲を設計図書で具体的に明確にしておく必要がある。	多様化設備の範囲に関する記載の適正化（多様化設備はソフトウェアによる安全機能を代替する設備であることを明記）
14.	解説 3.5.4 耐震性 多様化設備は，運転時の異常な過渡変化又は設計基準事故が発生し，かつソフトウェア CCF により安全機能が喪失するという設計基準を超える事象に対応する設備であるため，耐震 S クラスは要求しない。しかしながら，ソフトウェア CCF 発生時の安全保護回路の代替機能を有する設備であるため，安全保護回路と同等の基準地震動 Ss に対して機能維持するものとする。	解説 3.5.4 耐震性 多様化設備は，運転時の異常な過渡変化又は設計基準事故が発生し，かつソフトウェア CCF により安全機能が喪失するという設計基準を超える事象に対応する設備であるため，耐震 S クラスは要求しない。しかしながら，ソフトウェア CCF 発生時の安全保護回路の代替機能を有する設備であるため，安全保護回路と同様に基準地震動 Ss に対して機能維持するものとする。	基準地震動に関する記載の適正化
15.	解説 3.5.8 安全保護回路への波及的影響防止 多様化設備は，ソフトウェア以外の共通要因によって安全保護機能と同時にその代替機能が損なわれる恐れがないよう考慮する必要があることから，アイソレータ，切替回路等による物理的方法，又は電気的な方法等により安全保護回路と互いに分離するものとする。 解説図 3.5.8－1～解説図 3.5.8－3 に，多様化設備の機能である主蒸気隔離弁（MSIV）閉機能，工学的安全施設作動機能，原子炉停止機能喪失（ATWS）緩和機能と安全保護回路の分離例を示す。	説 3.5.8 安全保護回路への波及的影響防止 多様化設備は，安全保護回路への波及的影響を防止するため，アイソレータ，切替回路等による物理的方法，又は電気的な方法等により安全保護回路と互いに分離するものとする。 解説図 3.5.8－1～解説図 3.5.8－3 に，多様化設備の機能である主蒸気隔離弁（MSIV）閉機能，工学的安全施設作動機能，原子炉停止機能喪失（ATWS）緩和機能と安全保護回路の分離例を示す。	多様化設備の安全保護回路への波及的影響防止に関する記載の適正化
16.	解説 3.5.11 操作性 運転時の異常な過渡変化又は設計基準事故とソフトウェア CCF が重畳した事象への対応に必要な手動操作設備及び操作結果を確認できる監視設備を多様化設備として原子炉制御室に設けるものとする。 多様化設備の誤操作防止を考慮した設計例としては，多様化設備の手動操作設備は，運転員が容易に操作可能な場所に設置し，操作器具の配列，形状等の設計条件を同じ場所に設置された他の設備と同様とすることで，操作が円滑に行われるよう留意すること等がある。 また，多様化設備に切替スイッチを設ける場合は，例えば，切替警報，アクセスカバー等を設置することで，誤操作防止を実現するものとする。さらに，盤上に設置した指示計及び警報は，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。 なお，有効性評価により，対応操作までの時間余裕があり，現場での操作で対応可能であることが確認できたものはこれを許容する。	解説 3.5.11 操作性 運転時の異常な過渡変化又は設計基準事故とソフトウェア CCF が重畳した事象への対応に必要な手動操作設備及び操作結果を確認できる動作ランプや指示計などを多様化設備として原子炉制御室に設けるものとする。 多様化設備の誤操作防止を考慮した設計例を以下に示す。 ・手動操作設備は，運転員が容易に操作可能な場所に設置する ・操作器具の配列，形状等の設計条件を近傍に設置された他の設備と同様とする ・安全保護回路からの多様化設備への切替スイッチを設ける場合は，例えば，切替警報，アクセスカバー等を設置する ・盤上に設置した指示計及び警報は，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 なお，有効性評価により，対応操作までの時間余裕があり，事故時環境下において現場での操作で対応可能であることが確認できたものはこの限りではない。	(1) 監視設備の具体化 (2) 誤動作防止具体例に関する記載の適正化（箇条書き） (3) BTP7-19(Revision8) を参考に，現場における操作に関する許容条件（事故時環境下）記載の追加。 (4) 記載の適正化（「これを許容する」を「この限りではない」に修正）

No	改定前	改定後	変更理由
17.	解説 4.2　評価すべき事象 有効性評価においては，運転時の異常な過渡変化及び設計基準事故の全事象を対象とし，具体的には，「発電用軽水型原子炉施設の安全評価に関する審査指針」に基づくものとする。BWR 及び PWR における対象事象は以下のとおりである。 また，有効性評価における評価すべき事象のグルーピングの考え方を添付書類 2 に示す。	解説 4.2　評価すべき事象 有効性評価においては，運転時の異常な過渡変化及び設計基準事故の全事象を対象とし，具体的には，「発電用軽水型原子炉施設の安全評価に関する審査指針」に基づくものとする。BWR 及び PWR における対象事象は以下のとおりである。 また，有効性評価における評価すべき事象のグルーピングの考え方を添付書類 2 に示す。なお，参考文献（1）NUREG-0800，Standard Review Plan Chapter 7，Branch Technical Position 7-19，Revision 8，JANUARY 2021.（以下，BTP7-19）で，ソフトウェア CCF による誤作動事象の評価が明記されたことを考慮し，解説 2.2 で示した安全保護回路のソフトウェア CCF により安全機能の誤作動が生じる事象については，4.2 評価すべき事象に定める運転時の異常な過渡変化又は設計基準事故事象への包絡性を確認することとする。	BTP7-19(Revision8)を参考に，ソフトウェア CCF による誤動作を有効性評価における起因事象として取り扱うことを追記。（解説 2.2 参照）
18.	解説 4.4.4 常用系機能に対する仮定 「起因事象として外部電源の喪失を仮定する事象以外は，外部電源は利用可能」とは，有効性評価において，最も確からしいプラント応答を評価する観点から，常用系設備に対して外部電源喪失等の追加の故障は想定しないことである。 「事象発生前から機能しており，かつ事象発生後も機能し続ける設備は，故障の仮定から除外」とは，ソフトウェア CCF は，デジタル安全保護回路に対して安全保護機能の喪失を想定するものであることから，常用系のデジタル制御装置に対して機能喪失等を想定しないことである。例えば，給水制御の運転継続（BWR/ABWR），制御棒駆動機構パージ水の考慮（BWR/ABWR）等がある。 「常用系機能の喪失が起因となる事象が前提である場合は，当該事象を評価する際にはその機能を期待しない」とは，起因事象及びそれに従属して，ある常用系機能が喪失する場合，当該の常用系設備が復旧し，利用可能となることは想定しないことである。例えば，起因事象及びそれに従属して外部電源が喪失する場合は，外部電源が復旧し利用可能となることを想定しない。	解説 4.4.4 常用系機能に対する仮定 「起因事象として外部電源の喪失を仮定する事象以外は，外部電源は利用可能」とは，有効性評価において，最も確からしいプラント応答を評価する観点から，常用系設備に対して外部電源喪失等の追加の故障は想定しないことを意味する。 「事象発生前から機能しており，かつ事象発生後も機能し続ける設備は，故障の仮定から除外」とは，ソフトウェア CCF は，デジタル安全保護回路に対して安全機能の喪失を想定するものであることから，安全保護回路とは独立の常用系のデジタル制御装置に対して機能喪失等を想定しないことを意味する。例えば，給水制御の運転継続（BWR/ABWR），制御棒駆動機構パージ水の考慮（BWR/ABWR）等がある。なお，事象発生後に自動作動する常用系設備において，作動の有無，作動タイミングの不確かさにより，その後の操作の優先度や余裕時間が変わり得る場合は，その影響を予め把握しておくことが手順書の整備等に有効である。具体例として，ABWR の LOCA 事象においては，原子炉減圧による駆動蒸気喪失によりタービン駆動給水ポンプがトリップした後，給水制御系により電動駆動給水ポンプが自動起動することが想定されるが，タービン駆動給水ポンプトリップ及びその後の電動駆動給水ポンプの自動起動のタイミングは，原子炉減圧の状態等によって変わり得ることから，タイミングが変化した場合の影響を解析により確認することが考えられる。 「常用系機能の喪失が起因となる事象が前提である場合は，当該事象を評価する際にはその機能を期待しない」とは，起因事象及びそれに従属して，ある常用系機能が喪失する場合，当該の常用系設備が復旧し，利用可能となることは想定しないことである。例えば，起因事象及びそれに従属して外部電源が喪失する場合は，外部電源が復旧し利用可能となることを想定しない。	(1) 記載の適正化。（「である」を「を意味する」に修正） (2) 記載の適正化（「安全保護機能」を「安全機能」に統一） (3) 有効性評価における現実的評価条件の適用において，常用系の自動作動に不確かさを伴う場合は，自動の有無や作動タイミングについて感度を確認することを ABWR の LOCA 時の挙動を例として追記。
19.	添付書類 1 多様化設備は，運転時の異常な過渡変化又は設計基準事故が発生し，かつソフトウェア CCF により多重化されたデジタル安全保護回路がその安全保護機能を喪失した場合においても，設計基準事故の判断基準を概ね満足できるよう，原子炉停止系統，工学的安全施設等を自動，又は手動により作動させる機能，及び操作，監視を行うために必要となる指示，警報機能を有するものであり，これらの例を以下に示す。	添付書類 1 多様化設備は，運転時の異常な過渡変化又は設計基準事故が発生し，かつソフトウェア CCF により多重化されたデジタル安全保護回路がその安全機能を喪失した場合においても，設計基準事故の判断基準を概ね満足できるよう，原子炉停止系統，工学的安全施設等を自動，又は手動により作動させる機能，及び操作，監視を行うために必要となる指示，警報機能を有するものであり，これらの例を以下に示す。	記載の適正化（「安全保護機能」を「安全機能」に統一）

<table>
<tr><th>No</th><th>改定前</th><th>改定後</th><th>変更理由</th></tr>
<tr><td>20.</td><td></td><td>
添付書類 3

ソフトウェア CCF が発生するおそれがないと評価するための試験要件

本添付書類では，ソフトウェア CCF が発生する恐れがないことを評価するため，対象とする論理回路の全ての入力の組み合わせに対して，論理回路の不作動や誤作動が無いことの確認を行うための試験要件について記載する。なお，試験要件の検討にあたっては，参考文献(1)BTP7-19 の 3.1.2 Use of Testing to Eliminate Potential Common-Cause Failure from Further Consideration を参照した。
BTP7-19 の記載とそれを参考に具体化した試験要件を次表に対比して示す。次表以下に示す要件で，実際の回路（A／D 変換器の有無，入力点数の大小，シンプル又は多角的な論理構成などを模擬した実回路）に対して試験を行い，下記の要件に適合した結果が得られた場合は，当該デジタル回路にはソフトウェア CCF のおそれがないと評価できる。
<table>
<tr><th>BTP7-19 記載内容</th><th>本技術要件書での試験要件の考え方</th></tr>
<tr><td>a. 試験は，全ての運転モードと運転モード間の遷移状態をカバーし，以下を含むこと</td><td>当該デジタル回路において，全ての運転モードと運転モード間の遷移状態の適切な組み合わせで検証すること。</td></tr>
<tr><td>・全ての入力の組み合わせをカバーすること</td><td>全ての入力信号の組み合わせに対して検証すること。</td></tr>
<tr><td>・アナログ入力に対しては，レンジ逸脱を含む全ての運転範囲での組み合わせをカバーすること</td><td>アナログ信号の量子化ビット数(A/D 変換器の Bit 巾)を考慮した全ての遷移および，レンジ逸脱における挙動(前回値保持や異常状態の出力など)に対して検証すること。</td></tr>
<tr><td>・全ての実行可能な論理パスをカバーすること</td><td>(1)内部の全ての論理パスを検証すること。(全ての論理パスを動作させる(オン・オフさせる)試験を行うこと。(以下全パス試験という)
(2) 論理回路にタイマーなどの時間条件があり，論理回路の一部がそのタイミングで動作する場合，その検証方法の説明性を検討・判断した上で適用可能とする。その場合には，検証方法の説明性について文書化すること。</td></tr>
<tr><td>・全ての運転モードにおける全ての機能の遷移状態をカバーすること</td><td>全ての運転モード(操作スイッチなどの運転モード選択，インターロック等の条件入力)に対する，当該デジタル回路内の論理の遷移状態を検証すること。</td></tr>
<tr><td>・全ての試験ケースで，全てのアウトプットが事前の予測と一致すること</td><td>全ての試験条件で，全ての入力の組み合わせに対する出力結果が事前の予測と一致すること。</td></tr>
<tr><td>b. 実機と同じ機能を正確に模擬したシステムを用いて試験を行うこと</td><td>(1)製品の状態で検証すること。
(2)製品状態で検証できない場合，説明性を検討・判断した上で論理回路のソフトウェアを用いて製品状態をシミュレーター上で模擬したツール等による試験を適用可能とする。その場合には，検証方法の説明性について文書化すること。</td></tr>
<tr><td>c. 試験結果は，誤作動に対しても説明性を有すること。</td><td>全パス試験では，全ての入力信号の組み合わせを模擬し全ての実行経路の動作確認が行えるため，不作動及び誤作動両方の有無の確認が可能になる。</td></tr>
<tr><td>（記載無し）</td><td>回路設計の妥当性については，説明性を考慮し文書化すること。</td></tr>
</table>
</td><td>BTP7-19(Revision8)を参考に，試験によるソフトウェア CCF が発生するおそれがないと評価されるケースの要件と具体例を追加。（解説 3.1 参照）</td></tr>
</table>

No	改定前	改定後	変更理由
		全パス試験とは，対象とする論理回路について，入力信号の全ての組み合わせを模擬することにより，論理回路内の全ての実行経路を動作させる試験である。 例えば，下図のようなFPGAを使用したデジタル回路がある場合，全パス試験とは，対象とするFPGAの内部の論理回路や素子を入力から出力まで（下図の黄染め部）全ての動作を確認する。下図の場合，アナログ入力は無く，かつ，タイマーやタイミング制御などの時間条件は無いことを前提条件とすれば，以下に示すシンプルな検証で全パス試験が実施可能となる。すなわち，試験の組み合わせについては，このFPGAの場合，8入力あるので全入力ケースは2の8乗で256通りとなり，この組み合わせの試験を行う。なお，この例のように，論理回路に関連する赤枠①～③の場合，独立した信号入力でお互いが影響を受けないことから，3つに分けて検証する事で全てのFPGA内の動作を検証した事と同等の結果が得られる（赤枠①の場合は4入力分16通りの検証とし，②,③も同様の考え方。ただし，出力側は当該入力信号に関係する全ての出力信号を監視しておく。）。このような場合には論理構成に着目した分割試験の組み合わせとすることができる。  図　デジタル回路(FPGA)内部の論理回路例	

No	改定前	改定後	変更理由
21.		用語の定義 A/D 変換器 （A/D；Analog/Digital）：アナログ信号をデジタル信号に変換するための電子部品をいう。 運転モード：論理回路がプラントの運転状態などで切り替わる場合，それぞれの論理回路の動作体系を運転モードという。 運転モード間の遷移状態：論理回路が異なる運転モードに切り替わる場合，移行途中に生じる論理回路状態を遷移状態という。 量子化ビット数：アナログ信号からデジタル信号への変換の際に，信号を何段階の数値で表現するかを示す値。 論理パス：論理回路上の実行経路をいう。 （本頁以下余白）	