RIS2016-05 関連情報
デジタル I&C 規制基盤近代化に関する NRC 統合アクションプランの状況

令和 2 年 10 月 29 日

技術基盤課

要旨

RIS2016-05「安全関連システムに組込まれたデジタル装置」は、第 30 回技術情報検討会（平成 30 年 2 月 21 日）にて、「規制に取り入れるか必要性を判断するために調査を必要とする案件」に分類され、RIS に記載された組み込み型デジタル装置（EDD）を安全系に使用するための規制基盤及び品質保証（QA）プロセス等の改善を目的とした米国原子力規制委員会（NRC）の統合アクションプラン（IAP）の動向を調査することとした。

IAP のビジョンは、「安全性とセキュリティを維持しつつ、実用発電炉におけるデジタル I&C（DIC）の使用を拡大できるように、規制の不確かさを減じた明確な規制基盤をつくること」である。その IAP の成果として、特に EDD に関連する図書（表 1）が発行され、許認可プロセス上の規制の不確かさが減り、米国規制 10CFR50.59「「変更、検査及び試験」の基準に合えば、NRC の事前承認なしに、比較的低いリスク／安全重要度の原子力安全関連系に EDD を使用したデジタル改造を行えるようになった。結果として、米国では、安全系機器に商用グレードの EDD を NRC の事前承認を取得することなく適用するプラントが増加している。表 2 にその他の IAP タスク（未完了含む）を示すが、NRC では今後、未完了タスクは通常業務の中で取り扱うこととしている。

表1 EDD に関連する IAP 成果図書

図書名（発行月）	骨子
RIS2002-22 補足 1 「I&C のデジタル更新設計における NEI ガイダンスのエンドースの明確化」 （2018 年 5 月）	本図書は、RIS2002-22（2002 年 11 月）を明確化するものであり、アナログ機器をデジタル I&C（DIC）に更新する等のデジタル改造によってもたらされる共通要因故障（CCF）を含む故障可能性を評価する際に使用可能な「定性評価」のガイダンスを提供する。なお、本図書は安全関連システム又はコンポーネントのデジタル改造に適用されることを意図しているものの、事業者の裁量により、非安全関連システム等の改造にも適用できる。ただし、原子炉保護システム（RPS）、工学的安全施設作動システム（ESFAS）のデジタル改造等は非対象である。
NEI96-07 付録 D 改訂 1 「デジタル改造に 10CFR50.59 適用するための補足ガイダンス」 （2020 年 5 月）	本図書は、NEI96-07 改訂 1 本体（2000 年 11 月）に含まれるガイダンスをデジタル改造に関わる活動に特化して補足する。主目的は、デジタル改造に関わる活動に 10CFR50.59 プロセスをどのように適用させるかについて、共通のフレームワークと共通の理解を全てのステークホルダーに提供すること。本図書は、RIS2002-22 補足 1 に含まれる 10CFR50.59 関連の定性評価のガイダンスを取り込んでいる。

図書名（発行月）	骨子
RG1.182 改訂 2 「10CFR50.59”変更、検査及び試験”導入ガイダンス」（2020 年 6 月）	本図書は、デジタル改造の際の 10CFR50.59 要求適合に関するガイダンスを提供する。特に、いくつかの確認項目があるが、NEI96-07 付録 D 改訂 1 のガイダンスがデジタル改造の際に 10CFR50.59 に適合するアプローチを提供していることを認めるものである。

表 2　その他の主要な IAP タスク（ドラフト段階含む）

図書名（発行月）	骨子
SECY-18-0090 「DIC の潜在的 CCF 対処計画」（2018 年 9 月）	CCF 発生可能性のさらなる検討を不要とするための基準に対する NRC の現状ポジションを評価するもの。
BTP7-19 改訂 8 「DIC システムの潜在的 CCF 評価のためのガイダンス」（ドラフト段階）	潜在的 CCF に関連する D3 解析の評価方法に関するガイダンス（BTP7-19）を改訂する。RIS2002-22 補足 1 に書いてあるように、許認可審査において、設計属性、設計プロセスの品質と運転経験の使用を審査するのを助ける。
NEI17-06 改訂 B 「デジタル装置の CGD に関する IEC61508 を用いた SIL 認定ガイダンス」（ドラフト段階）	NEI は、IEC61508 に基づく第三者認証の仕組みを取り入れた追加ガイダンス（NEI17-06）を策定し、NRC によるエンドースを期待している。
DI&C ISG-06 改訂 2 「許認可プロセス、スタッフガイダンス」（2018 年 9 月）	工場出荷試験や申請補助書類を含む許認可申請書の審査からの教訓を含め、許認可審査の効率と効果を高めるための方策として、DI&C ISG-06 を更新した。この活動のゴールは、提出許認可図書のスコープを減らすことと、デジタル設計の工場出荷試験前の早期許認可を可能にすることである。

国内原子力発電所においても、技術基準にて、「安全設備は、全ての環境条件において、その機能を発揮することができる」ことを求めており、商用グレードの EDD を安全設備に用いる場合は性能認証を要するが、現状、商用グレード EDD を安全設備に適用する機会が少なく、RIS2016-05 に記載された規制基盤に関わる課題は顕在化していない。したがって、米国 IAP 成果を直ちに国内原子力規制に反映させる必要性はないと考えられる。

しかし、近い将来、国内も米国と同様な課題が顕在化する可能性があることから、国内原子力発電所の安全設備に商用グレードの EDD を適用する将来計画の有無ならびに EDD の性能認証における潜在的な課題について、事業者の見解を聴取することが必要である。さらに、米国 IAP タスクの中には実質終了していないものもあるので、米国動向を継続して注視することは、デジタル機器に関する国内規制技術や規制基盤の将来構想に役立つと考えられる。

1. はじめに

RIS2016-05[a]によると、米国では、組込み型デジタル装置（EDD）[b]を実用発電炉に用いる際には、汎用品グレード格上げ（CGD）プロセスを含む品質保証（QA）プロセス[c]にのっとった、ソフトウェア品質管理や共通要因故障（CCF）分析等が必要とされている。しかしながら、EDDを用いたデジタル改造すべてに、前記 QA プロセスを適用することは現実的ではないことから、デジタル機器を安全系に使用するための規制基盤及び QA プロセス等の改善を統合アクションプラン（IAP）[d]に含めて検討することとした（2016 年）。

規制庁では、第 30 回技術情報検討会（平成 30 年 2 月 21 日）にて、RIS2016-05 を「規制に取り入れるか必要性を判断するために調査を必要とした案件」に分類し、米国の IAP 動向をウォッチすることとした[e]。

2. IAP の状況

NRC のビジョンは、「安全性とセキュリティを維持しつつ、実用発電炉におけるデジタル I&C（DIC）の使用を拡大できるように、規制の不確かさを減じた明確な規制基盤をつくること」である[f]。そのビジョン達成のため、IAP には以下の 4 つの近代化プラン（MP）があり、NRC と産業界のステークホルダーとのやり取りを通じて更新されている。

MP#1　CCF に対する防護〈protection〉

MP#2　10CFR50.59[g]に準じた DIC の考慮〈considering〉

MP#3　デジタル機器の CGD

MP#4　I&C 規制基盤の近代化〈modernization〉

---

[a] RIS2016-05, 安全関連システムに組込まれたデジタル装置〈Embedded Digital Devices in Safety-Related Systems〉, April 29, 2016, https://www.nrc.gov/docs/ML1511/ML15118A015.pdf.

[b] ソフトウェア、ファームウェアの使用を必要とする電子機器が装置に組み込まれているもの。例：デジタル保護リレー、スマート検出器、デジタル電圧計、デジタルタイマリレー。

[c] 10CFR50 付録 B, 原子力発電所と燃料再処理施設の品質保証基準〈Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants〉, https://www.nrc.gov/reading-rm/doc-collections/cfr/part050/part050-appb.html.

[d] デジタル I&C の規制基盤を近代化するための統合アクションプラン〈Integrated Action Plan to Modernize Digital Instrumentation and Controls Regulatory Infrastructure〉, Revision 3, January 2019, https://www.nrc.gov/docs/ML1902/ML19025A312.pdf.

[e] 資料 30-1-2（3） RIS2016-05「安全関連システムに組み込まれたデジタル装置」（案）、https://www.nsr.go.jp/data/000220533.pdf.

[f] SECY-19-0112, NRC の DIC 規制基盤近代化統合戦略年報〈Annual Update on The Integrated Strategy to Modernize The U.S. Nuclear Regulatory Commission's Digital Instrumentation and Control Regulatory Infrastructure〉, November 4, 2019, https://www.nrc.gov/docs/ML1926/ML19261B629.html.

[g] 10CFR50.59, 変更、検査及び試験〈Changes, tests and experiments〉 https://www.nrc.gov/reading-rm/doc-collections/cfr/part050/part050-0059.html.

(1) MP#1：CCF に対する防護

この MP には、以下の 4 つのタスクがある。

#1A　CCF の影響分析[h]とともに故障発生可能〈the likelihood of failures〉の定性評価〈qualitative assessments〉を効果的に使用する NRC ガイダンスの作成、

#1B　さらなる検討〈further consideration〉を不要とする防御設計手段〈defensive design measures〉の使用、

#1C　CCF 防御に対する NRC 現状ポジションの評価、

#1D　NRC ポジションのフォローアップ。

MP#1A：完了／RIS2002-22 補足 1[i]（2018 年 3 月発行）

米国原子力エネルギー協会（NEI）が策定した NEI01-01[j]は、DIC を使用したプラント改造（デジタル改造と呼ぶ。）の設計／導入／許認可申請のガイダンスであり、NRC スタッフによりエンドースされている[k]。これには、10CFR50.59 下で NRC 事前承認なしでのデジタル改造の可否を判断するガイダンスが含まれている。しかし、NRC 検査において、事業者のデジタル改造の評価図書において、不整合や技術根拠の不備が散見されたことから、NRC スタッフは NEI01-01 を明確化する目的で追加のガイダンス（RIS2002-22 補足 1）を作成した。

これは、比較的低いリスク重要度〈lower risk-significant〉の安全系補助／サポートシステム（例：主制御室冷凍機制御系）をデジタル改造する際に、「設計属性〈design attributes〉」、「設計プロセスの品質〈quality of the design processes〉」と「運転実績〈operating history〉」を評価／図書化することで、CCF 発生可能性を定性評価するためのガイダンスである。なお、このガイダンスは、比較的高いリスク重要度の原子炉保護系（RPS）や工学的安全施設起動系（ESFAS）に関係する潜在的 CCF に対処することは意図していない。それらは、BTP7-19[l]と NUREG/CR-

---

[h] CCF を想定した影響分析結果が許容範囲であることを示す対策分析（coping analysis）と既往解析範囲内であることを示す境界分析〈bounding analysis〉の総称。

[i] RIS2002-22, Supplement 1, I&C システムのデジタル更新に関する NEI ガイダンスのエンドースの明確化〈Clarification on Endorsement of NEI Guidance in Designing Digital Upgrades in I&C Systems, Revision 1〉, May 2018, https://www.nrc.gov/docs/ML1814/ML18143B633.pdf .

[j] NEI01-01,10CFR50.59 規則への変更を反映した EPRI TR-102348 の改訂：デジタル更新許認可ガイダンス〈A Revision of EPRI TR-102348 to Reflect Changes to the 10CFR50.59 Rule: Guideline on Licensing Digital Upgrades〉, EPRI TR-102348 Revision 1, March 2002, https://www.nrc.gov/docs/ML0208/ML020860169.pdf.

[k] RIS2002-22, EPRI/NEI 合同タスクフォース報告書の使用〈Use of EPRI/NEI Joint Task Force Report, "Guideline on Licensing Digital Upgrades: EPRI TR-102348, Revision 1, NEI01-01: a Revision of EPRI TR-102348 to Reflect Changes to the 10CFR50.59 Rule,"〉 November 2002, https://www.nrc.gov/reading-rm/doc-collections/gen-comm/reg-issues/2002/ri200222.pdf.

[l] BTP7-19, DIC システムの潜在的 CCF 評価のためのガイダンス〈Guidance for Evaluation of Potential

6303[m]で扱われている。

MP#1B：完了（中止）／NEI16-16[n]作成中止

NEI16-16 は、CCF を防止〈preventing〉／制限〈limiting〉／緩和〈mitigating〉する設計対応〈design measures〉を開発プロセス中に組み込むことをベースとして、CCF に対処するためのガイダンスである。NRC スタッフは、具体的な防護設計手段がとられていれば、D3 解析要求を除外〈preclude〉できることを、NEI16-16 が技術的に十分正当化しているかどうか評価する計画であった。しかし、NEI16-16 の作成は中止され、NEI は新たなガイダンス（NEI20-07ドラフト段階[o]）を作成し、提出予定である。

MP#1C：完了／SECY-18-0090[p]（2018 年 9 月発行）

NRC 現状ポジションqは、「D3 解析〈Diversity and Defense-in-Depth Analyses〉において、ソフトウェア CCF の発生可能性のさらなる検討を不要とする手段は、十分な多様性を持たせ、完全試験〈complete testability〉が可能なシンプル設計〈simple designs〉を使用すること。」である。しかし、現状のガイダンスは、CCF 発生可能性のさらなる検討を不要とするための影響分析や防御設計手段を使用するための基準が不明確である。そこで、NRC スタッフは現状ポジションを次の 2 項目について評価した。(1)取り扱われるシステムのスコープについて、(2)リスク／安全重要度に基づくグレーデッドアプローチの技術的適用性。

評価結論（SECY-18-0090）：CCF 防御に関する NRC ポジションの矛盾のない適用のために、NRC スタッフはガイド方針（下枠参照）を用いて許認可ガイダンスを更新し、明確化する。さらに、MP#4 に示された規制基盤活動において、いかに CCF を取り扱うかについても評価する計画である。

Common Cause Failure in Digital Instrumentation and Control Systems〉, Revision 8, draft, June 2020, https://www.nrc.gov/docs/ML1923/ML19231A332.pdf.

[m] NUREG/CR-6303, 原子炉保護系の D3 解析手法〈Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems〉, December 1994, https://www.nrc.gov/docs/ML0717/ML071790509.pdf.

[n] NEI16-16 (Draft 2), デジタル CCF 対処ガイダンス〈Guidance for Addressing Digital Common Cause Failure〉, May 2017, https://www.nrc.gov/docs/ML1713/ML17135A253.pdf.

[o] NEI20-07, 安全重要度の高い DIC 設備のソフトウェア CCF 対処ガイダンス〈Guidance for Addressing Software CCF in High Safety-Significant Safety-Related Digital System〉

[p] SECY-18-0090, DIC の潜在的 CCF 対処計画〈Plan for Addressing Potential Common Cause Failure in Digital Instrumentation and Controls〉, September, 2018, https://www.nrc.gov/docs/ML1817/ML18179A067.pdf.

[q] SRM-SECY-93-087,改良発展軽水炉（ALWR）設計に関する戦略、技術、許認可課題〈Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs〉, July 1993, https://www.nrc.gov/docs/ML0037/ML003708056.pdf.

ガイド方針（抜粋）

[1] 事業者は、継続して、DIC のソフトウェアに起因する CCF を評価し対処すべきである。
[2] RPS と ESFAS の D3 解析を実施して、CCF に対する脆弱性が特定され、適切に対処されていることを示さなくてはならない。
[3] 解析は系統の安全重要度に見合っていなくてはならない。その故障が安全機能に悪影響しないような比較的低い安全重要度の I&C には、そうした解析が不要な場合がある。
[4] 想定 CCF により安全機能が不能となった場合、多様化手段が機能発揮しなければならない。関連する事象条件下で確実に機能発揮するに十分な品質を持つならば、その多様化機能は、安全系でも非安全系でもよい。許容可能時間内で起動可能ならば、自動または手動起動も多様化起動手段とみなせる。D3 解析によって、CCF がその他の手段で合理的に緩和されることが示されるならば、多様化手段は必要ではない場合がある。
[5] 潜在的 CCF 対処手段の技術的正当性レベルは、DIC の安全重要度に見合っていなくてはならない。比較的高い安全重要度の系統に、多様性やテスタビリティに代わる手段を使用するならば、その正当性を示す技術的説明が必要である。

MP#1D：進行中／BTP7-19 改訂 8 ドラフト（2020 年 8 月発行）

潜在的 CCF に関連する D3 解析の評価方法に関するガイダンス（BTP7-19）を改訂する。このガイダンスは、RIS2002-22 補足 1 に書いてあるように、許認可審査において、設計属性、設計プロセスの品質と運転経験の使用を審査するのを助ける。

(2) MP#2：10CFR50.59 に準じた DIC の考慮

この活動は、デジタル改造に対して 10CFR50.59 評価を実施するにあたって、NRC ガイダンスが適切に解釈されて産業界の活動に組み込まれていることを、NRC と産業界が相互に確認する目的で行われている。従来の NEI ガイダンス（NEI01-01）では、ソフトウェア CCF に対して定性評価を認めているが、どのように定性評価を展開するかが示されていない。別の NEI ガイダンス（NEI96-07 改訂 1[r]、RG1.187 改訂 0[s]でエンドース）は、10CFR50.59 の一般的ガイダンスであり、DIC にとっては十分に詳しくない。産業界ステークホルダーから、規制の不確かさゆえに、10CFR50.59 下で DIC 改造を実施するのはためらわれると表明されている。

MP#2A：完了／RG1.187 改訂 2[t]（2020 年 6 月発行）

NRC と産業界とのやり取りの末、NEI96-07 に RIS2002-22 補足 1 を取り込んだ NEI96-07

[r] NEI 96-07, Revision 1, 10CFR50.59 導入ガイドライン〈Guidelines for 10CFR50.59 Implementation〉, November 2000, https://www.nrc.gov/docs/ML0037/ML003771157.pdf.
[s] RG1.187, Revision 0, 10CFR50.59 導入ガイダンス〈Guidance for Implementation of 10CFR50.59, “Changes, Tests, and Experiments,”〉 November 2000, https://www.nrc.gov/docs/ML0037/ML003759710.pdf.
[t] RG1.187, Revision 2, 10CFR50.59 導入ガイダンス〈Guidance for Implementation of 10CFR50.59, “Changes, Tests, and Experiments,”〉 June 2020, https://www.nrc.gov/docs/ML2012/ML20125A730.pdf.

付録 D[u]が発行され、RG1.187 改訂 2 によってエンドースされた。

MP#2B：完了／ワークショップ（2018 年、2019 年）、検査官トレーニング（2019 年 7 月）

ガイダンス（RIS2002-22 補足 1 と NEI96-07 付録 D）を使用／解釈／適用するにあたって、共通の理解をすすめるため、NRC スタッフは、検査官トレーニングを計画、実施した。目的の一つは、検査における 10CFR50.59 ガイダンスの矛盾のない導入である。NRC スタッフは、NEI 主催の RIS2002-22 補足 1 ワークショップに参加し、検査官トレーニングに生かした。

(3) MP#3：デジタル機器の CGD

市場で入手可能な EDD 等のデジタル機器は、原子力施設での使用を目的としておらず、NRC の品質保証基準に適合して、設計、開発、製造されていない。商用グレード品（CGI）を安全系に使用することを評価、許容するために必要となるステップを明確にした産業界のガイダンス（例：EPRI 3002002982 改訂 1[v]）が策定され、RG1.164[w]でエンドースされている。

この MP では、第三者認証を許容するかどうか判断するために、NEI の追加ガイダンスと産業界合意標準〈industry consensus standards〉（例：IEC61508[x]）の適切性を評価する。もとは原子力仕様ではないが、第三者認証された EDD を利用することにより、許容プロセス〈acceptance process〉における NRC 負担も事業者許認可リスクも下がると考えられている。

MP#3：進行中／NEI17-06 改訂 B ドラフト（2019 年 9 月発行）

NEI は、第三者認証の仕組みを取り入れた追加ガイダンス（NEI17-06[y]）を策定し、NRC によるエンドースを期待している。

(4) MP#4：I&C 規制基盤の近代化

この MP は、2 つのタスクに分かれている。以下に各々の概要と状況を合わせて示す。

---

[u] NEI 96-07, Appendix D, デジタル改造への 10CFR50.59 適用ガイダンス補足〈Supplemental Guidance for Application of 10CFR50.59 to Digital Modifications〉, Revision 1, May 2020, https://www.nrc.gov/docs/ML2013/ML20135H168.pdf.

[v] EPRI3002002982, プラントエンジニアリング：商用グレード品の原子力安全系での使用許容ガイドライン〈Plant Engineering: Guideline for the Acceptance of Commercial-Grade Items in Nuclear Safety-Related Applications〉, Revision 1 to EPRI NP-5652 and TR-102260, September 2014, https://www.nrc.gov/docs/ML1819/ML18199A161.pdf.

[w] RG-1.164, 商用グレード品の原子力発電所での使用格上げ〈Dedication of Commercial-Grade Items for Use in Nuclear Power Plants〉, June 2017, https://www.nrc.gov/docs/ML1704/ML17041A206.pdf

[x] IEC61508, 電気・電子・プログラマブル電子安全関連系の機能安全〈Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems〉。この中で、安全性の目標として、安全度水準（SIL）が定義されている。JIS C0508 が等価。

[y] NEI17-06, 〈Guidance on Using IEC 61508 SIL Certification to Support the Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Related Applications〉, Revision B, September 2019, https://www.nrc.gov/docs/ML1927/ML19273A007.pdf.

MP#4A：完了／DI&C ISG-06 改訂 2[z]（2018 年 9 月発行）

NRC スタッフは、工場出荷試験や申請補助書類を含む許認可申請書の審査からの教訓を含め、許認可審査の効率と効果を高めるための方策として、DI&C ISG-06 を更新した。この活動のゴールは、提出許認可図書のスコープを減らすことと、デジタル設計の工場出荷試験前の早期許認可を可能にすることである。

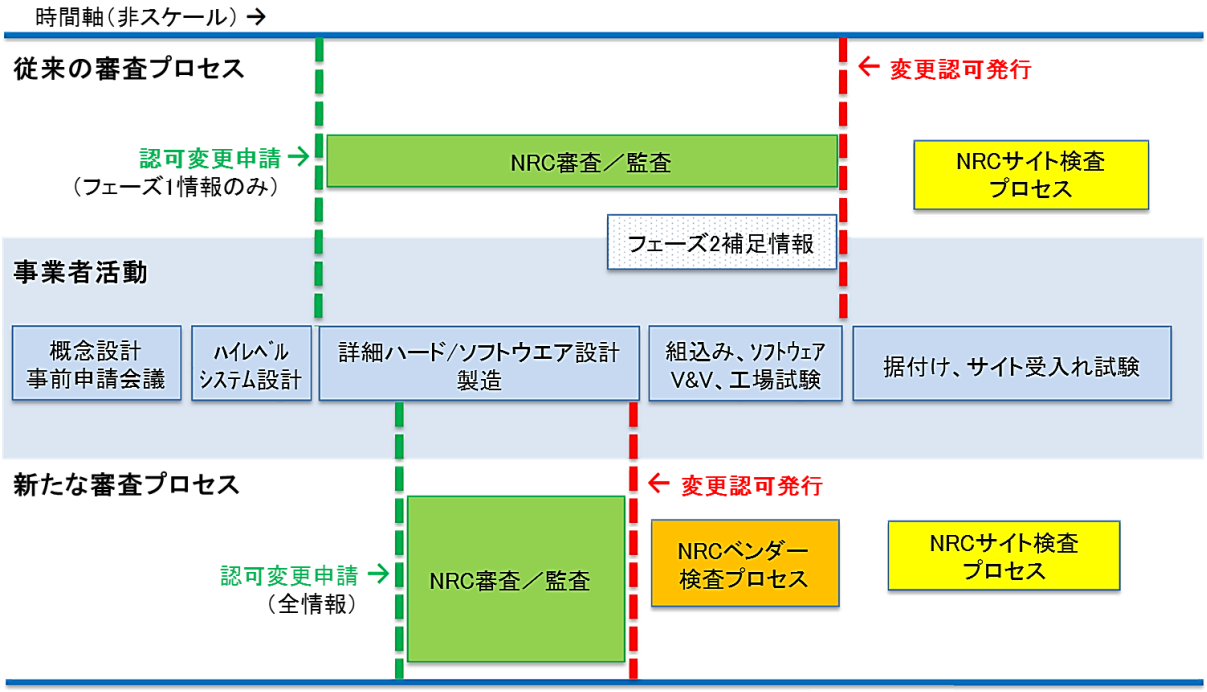

図 ISG-06 改訂 2 に示された新しい NRC 審査プロセスの概念

MP#4B：最終報告書作成中

NRC スタッフは、広範囲に DIC 規制基盤の評価を実施する。その目的は、現在の I&C 規制基盤概要とそれを裏付ける技術根拠をレビュー・評価することと、見落としがないことを確認すること。例えば、過去の審査経験、進行中の許認可審査や調査研究、運転経験からの教訓、他の安全を重視する産業、国際的な観点（IEC 基準）を評価する。そして、長期的に規制基盤を近代化（改善）するため、それらから改善点を特定し優先度をつけ、推奨案を提示する。

3. IAP 年報（SECY-19-0112）の結論

NRC スタッフは、産業界ステークホルダーとともに、DIC の規制基盤を近代化する IAP の策定と遂行に従事してきた。IAP の遂行により、不必要な障害が取り除かれ、規制の不確かさが減じたので、DIC 規制基盤が大きく改善された。結果として、事業者は 10CFR50.59 下でデジタル改造を導入することができ、DI&C ISG-06 に示された新たな NRC 審査プロセスによる認可を求

[z] DI&C-ISG-06, 許認可プロセス、スタッフガイダンス〈Licensing Process, Interim Staff Guidance Revision 2〉, December 2018, https://www.nrc.gov/docs/ML1826/ML18269A259.pdf.

めて、より広範囲なデジタル変更申請を行うことを計画している。こうした許認可活動の状況を踏まえ、NRC スタッフは IAP 年報を今後発行しないこととした。

4. まとめと今後の対応

RIS2016-05 に関連した IAP の遂行により、米国では、許認可プロセス上の規制の不確かさが減り、10CFR50.59 基準に合えば NRC の事前承認なしに、比較的低いリスク／安全重要度の原子力安全関連系に EDD を使用したデジタル改造を行えるようになった。実際に、安全系機器に商用グレードの EDD を適用するプラントが増加している。

一方で、原子力安全系ではない系統にデジタル改造を施す際にも、条件によっては、事業者は RIS2002-22 補足 1 や NEI96-07 付録 D のガイダンスに従った CCF に関わる定性評価を行うこととなった。また、商用グレードの EDD を原子力安全関連系に用いる CGD において、第三者認証を用いたプロセスの検討が行われているが、追加ガイダンス（NEI17-06）は未だドラフト段階で、NRC によるエンドースは行われていない。

国内原子力発電所においても、技術基準にて、「安全設備は、全ての環境条件において、その機能を発揮することができる」ことを求めており、商用グレードの EDD を安全設備に用いる場合は性能認証を要するが、現状、商用グレード EDD を安全設備に適用する機会が少なく、RIS2016-05 に記載された規制基盤に関わる課題は顕在化していない。したがって、米国 IAP 成果を直ちに国内原子力規制に反映させる必要性はないと考えられる。

しかし、近い将来、国内も米国と同様な課題が顕在化する可能性があることから、国内原子力発電所の安全設備に商用グレードの EDD を適用する将来計画の有無ならびに EDD の性能認証における潜在的な課題について、事業者の見解を聴取することが必要と考えられる。さらに、米国 IAP タスクの中には実質終了していないものもあるので、米国動向を継続して注視することは、デジタル機器に関する国内規制技術や規制基盤の将来構想に役立つと考えられる。

添付資料

① RIS2002-22 補足 1 抜粋「I&C のデジタル更新設計における NEI ガイダンスのエンドースの明確化」
② RG1.182 改訂 2 抜粋「10CFR50.59”変更、検査及び試験”導入ガイダンス」
③ NEI96-07 付録 D 改訂 1「デジタル改造に 10CFR50.59 適用するための補足ガイダンス」

添付資料①

RIS2002-22 補足 1 抜粋
「I&C のデジタル更新設計における NEI ガイダンスのエンドースの明確化」

令和 2 年 10 月 29 日

技術基盤課

意図

RIS2002-22 補足 1[a]は、RIS2002-22[b]を明確化するものであり、NEI01-01[c]を引き続きエンドースする。具体的には、NEI01-01 の§4 と 5、付録 A と B にあるガイダンスを NRC スタッフがエンドースしていることを明確にし、共通要因故障（CCF）の可能性〈likelihood〉を含む、デジタル改造〈digital modification〉の故障可能性〈the likelihood of failure〉を評価する際に使用可能な「定性評価〈qualitative assessments〉」の方法と図書化のガイダンスを提供するものである。事業者〈licensees〉は、これらの定性評価を使用して、デジタル I&C（DIC）改造による故障発生可能性は十分に低い〈sufficiently low〉とする結論を裏付けることが可能である。なお、この結論と根拠〈reasons〉は、図書化されなければならない。

RIS2002-22 と整合して、本補足 1 は、安全関連〈safety-related〉システム又はコンポーネントのデジタル更新に適用されることを意図しているものの、事業者の裁量により、非安全関連〈non-safety related〉システム又はコンポーネントの改造にも適用できる。ただし、本補足 1 は、原子炉保護システム（RPS）、工学的安全施設作動システム（ESFAS）の DIC 更新、又はこれらのシステムの内部ロジック部分（例：多数決ロジック、バイステーブル入力、信号調整・処理等）の改造／更新については、追加の考慮事項があるため、対象としない。

背景情報

2002 年 11 月、NRC スタッフは RIS2002-22 を発行して、原子力発電所の I&C システムのデジタル更新の設計及び使用のガイダンスとして NEI01-01 を使用することをエンドースした。その後、運転認可されている事業者は、そのガイダンスと RG1.187 改訂 0（2000 年 11 月発行）とを併せて、デジタル設計改造の裏付けのために使用してきた。しかし、NEI01-01 のガイダンスを使用して事業者が作成した DIC プラント改造に関する図書に対する NRC 検査で、事業者のエ

[a] RIS2002-22, Supplement 1, Clarification on Endorsement of NEI Guidance in Designing Digital Upgrades in I&C Systems, Revision 1, May 31, 2018

[b] RIS2002-22, Use of EPRI/NEI Joint Task Force Report, 'Guideline on Licensing Digital Upgrades: EPRI TR-102348, Revision 1, NEI01-01: A Revision of EPRI TR-102348 To Reflect Changes to the 10 CFR 50.59 Rule.

[c] NEI 01-01, A Revision of EPRI TR-102348 to Reflect Changes to the 10 CFR 50.59 Rule: Guideline on Licensing Digital Upgrades, EPRI TR-102348 Revision 1, March 2002,

学的評価〈engineering evaluations〉のやり方において不整合が指摘され、10CFR50.59 基準の評価についても課題が特定された。「工学的評価」とは、DIC 改造を設計する際の10CFR50.59 以外の評価（例：NRC が承認した事業者の品質保証プログラム（QAP）に基づいて実施する評価）である。本補足 1 は、事業者が「工学的評価」と「定性評価」を実施し、図書化するためのガイダンスを明確化している。

2016 年 10 月の NRC スタッフ要件メモ SECY-16-0070[a]を受け、NRC スタッフは、I&C 規制インフラを近代化するための取り組みの一環として、10CFR50.59 を適用するためのガイダンスを改善するため、公衆、NEI、産業界の代表と協議を開始した。その統合行動計画（IAP）で、DIC 改造がもたらす故障発生可能性が十分に低いという結論を裏付ける定性評価図書作成のための具体的なガイダンス（本補足 1）を近く発行することが述べられている。

実用発電子炉以外の事業者への適用可能性

本補足 1 で示された事例と具体的な説明、及び参照されたガイダンス（NEN01-01、RIS2002-22）は、主として実用発電炉に焦点を当てているが、他の事業者もまた、RIS2002-22 と本補足 1 のガイダンスを適用して、10CFR50.59 基準に対する評価を行うことは可能である。しかし、ガイダンスの一部では、これらの事業者に適用されない規制要件を論じていることに留意すること。

概要

一般に、DIC 技術の導入〈implementation〉により、総合信頼性〈dependability〉と安全性が提供される。特に、デジタル技術は、プラントの内部システム〈internal systems operation〉の運転健全性〈integrity〉とその可用性〈availability〉に関する連続診断情報〈continuous diagnostic information〉を提供する。しかし、DIC 技術の導入により、ソフトウェア CCF や相互接続性〈interconnectivity〉がもたらす故障など、潜在的なハザードをもたらす可能性はある。しかし、ソフトウェア CCF などのいくつかのハザードは、定性評価によって対処できる可能性がある。

定性評価は、DIC 改造〈DIC modification〉によって、事故発生頻度〈the frequency of occurrence of accidents〉[b]又は機能不良発生可能性〈the likelihood of occurrence of malfunctions〉[c]が有意に増加しない〈more than a minimal increase〉という結論〈conclusion〉を裏付けるのに使用可能である。定性評価はまた、DIC 改造は、更新最終安全解析書（UFSAR）

[a] SECY-16-0070, INTEGRATED STRATEGY TO MODERNIZE THE NUCLEAR REGULATORY COMMISSION'S DIGITAL INSTRUMENTATION AND CONTROL REGULATORY INFRASTRUCTURE, October 25, 2016
[b] 10CFR50.59(c)(2)(i)
[c] 10CFR50.59(c)(2)(ii)

において従前に評価されたものとは異なるタイプの事故〈an accident of a different type〉[a]又は異なる結果をもたらす機能不良〈malfunction with a different result〉[b]の発生可能性〈the possibility〉をもたらさないという結論を裏付けるのにも使用可能である。これらの結論は、DIC 改造が、十分に低い故障可能性〈a sufficiently low likelihood of failure〉を持つ場合に満足されるものである。

デジタル変更による故障発生可能性が十分に低いとする判断の根拠は、次に示す定性評価のファクタから得られる。すなわち、設計属性〈design attributes〉、用いられた設計プロセスの品質〈the quality of the design processes used〉及び、ソフトウェアとハードウェアが統合されたもの〈the integrated software and hardware〉の運転経験〈operating experience〉の評価。事業者は、こうしたファクタや判断論理根拠〈rationale〉を図書化するために定性評価を使用することができる。その際、これらのファクタの情報を集約すること。本補足 1 の添付は、相互接続性のハザードに対処するためのアプローチを含む定性評価と工学的評価の方法と図書化の枠組みを示している。

[a] 10CFR50.59(c)(2)(v)
[b] 10CFR50.59(c)(2)(vi)

RIS2002-22 補足 1 添付「定性評価と故障解析」

1. 目的

- RIS2002-22[a]（2002 年 11 月）は、NEI01-01[b]（2002 年 3 月）をエンドース〈endorse〉する。NEI01-01[c]は、デジタル更新〈upgrade〉の導入と認可に関するガイダンスであり、デジタル計装制御系（DIC）の総合信頼性〈dependability〉を定性評価〈qualitative assessment〉するためのガイダンスでもある。
- NEI96-07 改訂 1[d]（2000 年 11 月）は、10CFR50.59 基準[e]に対して、定性評価が可能であることを認めている。本添付は、DIC 改造〈modification〉に対する適正な定性評価を行う方法を明確に示す補足ガイダンスである。RIS2002-22 と NEI01-01 に従えば、事業者〈licensees〉は、「第三者による検証が十分可能なほど詳細に」定性評価を図書化〈document〉できる。
- NEI01-01 は、「定性評価」と「総合信頼性評価」を同義で使っている。本補足 1 では、10CFR50.59 評価と関連付けて、「定性評価」と「十分に低い〈sufficiently low〉」という言葉を使っている。「総合信頼性評価」は、工学的評価〈engineering evaluation〉の観点からのみ使用する。なお、工学的評価は、DIC 改造を展開する際に、NRC が承認〈approve〉した事業者の品質保証プログラム（QAP）に従って実施されるものである。
- もし、定性評価により潜在的故障〈potential failure〉（ソフトウェア CCF など）の頻度が十分に低いことが示されたら、故障の影響〈effect〉を 10CFR50.59 評価する必要はない。

2. 規制明確化－10CFR50.59 に対する定性評価の適用

- 設備[f]の変更〈change〉を行うと決めた際は、事業者はプラント手順に従って工学的、技術的評価を実施する。それらの評価で許容されれば、事業者は 10CFR50.59 プロセスに入る。10CFR50.59 は、規制審査要否のしきい値〈threshold〉を与える。すなわち、NRC の事前承認なし〈without prior NRC approval〉で事業者が施設もしくは手順に変更を加えられる、もしくは、検査や試験を実施できる条件を与えている。

---

[a] RIS2002-22, Use of EPRI/NEI Joint Task Force Report, 'Guideline on Licensing Digital Upgrades: EPRI TR-102348, Revision 1, NEI01-01: A Revision of EPRI TR-102348 To Reflect Changes to the 10 CFR 50.59 Rule.

[b] Use of EPRI/NEI Joint Task Force Report, 'Guideline on Licensing Digital Upgrades: EPRI TR-102348, Revision 1, NEI 01-01: A Revision of EPRI TR-102348 To Reflect Changes to the 10 CFR 50.59 Rule

[c] NEI 01-01, A Revision of EPRI TR-102348 to Reflect Changes to the 10 CFR 50.59 Rule: Guideline on Licensing Digital Upgrades, EPRI TR-102348 Revision 1, March 2002.

[d] NEI96-07, Revision 1, Guidelines for 10 CFR 50.59 Implementation.

[e] 10CFR50.59, Changes, tests, and experiments, (c)(2) (i)~(viii)

[f] 更新最終安全解析書（UFSAR）に記載された設備。

- こうした工学的、技術的評価は、変更のすべての要素〈element〉について実施しなければならない。ある要素は、構造、システム、コンポーネント（SSC）故障頻度について正あるいは負の効果を与えるかもしれない。それらの要素が相互依存するならば、正負の効果を一緒に考慮し、相互依存しないなら、独立評価しなければならない。

2.1. 定性評価

- 適切に図書化された定性評価は、UFSAR で用いられた解析仮定のもとで DIC 改造は十分に低い故障頻度を持つと結論付ける助けとなる。
- 「DIC 改造が十分に低い故障頻度を持つ」ことは、次の 3 つのファクタ〈factor〉の定性評価から得られる：①設計属性〈design attribute〉、②適用した設計プロセスの品質〈quality of the design process〉、③ソフトウェアとハードウェアを統合した運転経験〈operating experience〉（製品成熟度、供用経験）。定性評価図書には、DIC 改造が十分に低い故障頻度をもつことを判断するためのファクタ、論理根拠〈rationale〉、理由〈reasoning〉（工学的判断含む）を含める。
- 故障頻度の判断には、上記のファクタ全てを検討するほうがよい。あるファクタは、他の領域の弱点を補う可能性もある。例えば、シンプルで高度に検査可能〈testable〉なデジタル機器は、運転経験の不足を補える。

「十分に低い」という結果

- 定性評価の一つのアプローチは、概念〈concept〉の採用、すなわち、（1）故障頻度が十分に低い、（2）故障頻度が十分に低くない、の二者択一とすること。NEI01-01 の § 4.3.6 は、「十分に低いとは、UFSAR で検討されている故障頻度（単一故障など）よりずっと低く、UFSAR では言及されていない他の CCF（設計欠陥、保守ミス、校正ミスなど）の頻度に匹敵する」と言っている。この「十分に低い」のしきい値は、想定可能／不能〈credible/not credible〉事象を区別するしきい値とは別物である。想定可能／不能しきい値は、UFSAR で仮定している機能不良〈malfunction〉と同頻度〈as likely as〉かどうかである。
- もし、定性評価が潜在的故障（ソフトウェア CCF など）の頻度は十分に低いと判定したら、故障の影響を検討するための 10CFR50.59 評価は必要ではない。

2.2. 10CFR50.59 基準 i, ii, v, vi の頻度のしきい値

- デジタル改造、特にソフトウェア改造の場合は、故障頻度は潜在的に上昇する可能性が

ある。多重化 SSC では、故障頻度の潜在的な上昇は、CCF 発生頻度の上昇をもたらす可能性がある。

- NRC は、「十分に低い」しきい値の議論の中で、NEI96-07 改訂 1 や NEI01-01 から得た基準を使ってきた。NRC は、10CFR50.59 を明確化する意図で、こうした議論をおこなっており、事業者は、これらの議論を NRC の新たな見解や見解の変更とはみなしてはならない。

基準

- 以下に示すように、「十分に低い」ことを示す定性評価結果があるならば、10CFR50.59(c)(2)の基準(i), (ii), (v), (vi)によって NRC 事前承認は要求されない。

基準 i「事故頻度」

- 事故発生頻度〈frequency〉に関して、最小限以上の増加をもたらすか。

  「十分に低い」しきい値：事故の発生頻度は、事故の起因となる機器の故障発生可能性〈likelihood〉に直接関連する（例：SG の伝熱管不良発生可能性の増加は、SG 伝熱管破断事故の発生可能性の増加と関連する）。もし、定性評価の結果が「十分に低い」ならば、UFSAR で従前に評価された事故発生頻度の増加は最低限未満であることになる。

基準 ii「機能不良頻度」

- 安全上重要[a]な SSC の機能不良発生可能性に関して、最小限以上の増加をもたらすか。

  「十分に低い」しきい値：安全上重要な SSC の機能不良発生可能性は、意図した設計機能[b]〈design function〉を発揮する SSC の故障を引き起こす機器の故障発生可能性に直接関連する（例：補助給水（AFW）ポンプの故障可能性の増加は、AFW ポンプと AFW 系統の SSC の機能不良発生可能性の増加を伴う）。もし、定性評価の結果が「十分に低い」ならば、UFSAR で従前に評価された安全上重要な SSC の機能不良発生可能性の増加は最低限未満であることになる。

---

[a] NEI96-07 改訂 1 § 3.9 によると、安全上重要な SSC の機能不良とは、「UFSAR に記載されている意図した設計機能〈design function〉を発揮する SSC の故障」とされている。Appendix B による「安全関連」の分類とは異なる。

[b] NEI96-07 改訂 1 によると、UFSAR に記載された設計基準機能〈design bases function〉及び設計基準機能を助けるもしくは設計基準機能に影響を与える UFSAR に記載されたその他の SSC の機能。

基準 v「異なるタイプの事故」

- UFSAR で従前に評価されたものと異なるタイプの事故が発生する可能性があるか。

  「十分に低い」しきい値：NEI96-07 改訂 1 § 4.3.5 によると、「異なるタイプの事故とは、UFSAR において従前に評価された事故と同程度の起こりやすさを持つ事故に限定される」。異なるタイプの事故は、その事故の起因となる機器の故障によって発生する。もし、変更による故障頻度が「十分に低い」と定性評価されるならば、変更によって、異なるタイプの事故を引き起こす可能性のある故障の発生可能性も同等（十分低い）となる。もし、潜在的故障（ソフトウェア CCF など）の発生可能性が十分低くないと定性評価されるならば、故障の影響について 10CFR50.59 評価が必要となる。

基準 vi「異なる結果をもたらす機能不良」

- UFSAR で従前に評価されたものと異なる結果をもたらす安全上重要な SSC の機能不良が発生する可能性があるか。

  「十分に低い」しきい値：NEI96-07 改訂 1 § 4.3.6 によると、「異なる結果をもたらす機能不良とは、UFSAR にある機能不良と同程度の起こりやすさを持つものに限定される」。安全上重要な SSC の機能不良とは、意図した設計機能を発揮する SSC の故障を引き起こす機器故障のことである。もし、変更による故障発生可能性が「十分に低い」と定性評価されるならば、変更は、UFSAR に書いてある故障と同等の頻度で起こる故障をもたらさないことになる。もし、潜在的故障（ソフトウェア CCF など）の発生可能性が十分低くないと定性評価されるならば、UFSAR と整合した手法を使って、故障の影響について 10CFR50.59 評価が必要となる。

- なお、潜在的なソフトウェア CCF の影響が、UFSAR で従前に評価されたものと異なる結果をもたらさない場合もある。

3. 定性評価

- 以下に、適切な定性評価図書を使うことで、NRC 事前承認なしで導入可能な DIC 変更の例を示す。
  - アナログリレー（タイマー含む）をデジタルリレーに置き換え
  - 安全関連補助系統（冷凍機、HVAC、潤滑油冷却器など）のアナログ制御器の置き換え

- 非常用ディーゼル発電機（EDG）補助系統や補機系統（電圧制御）のアナログ制御器の置き換え
- 組込み型デジタル機器（EDD）を使用する回路遮断器の据え付け
- アナログレコーダーや指示器をデジタル機器に置き換え
- 非安全系制御系統のデジタル更新

- チャンネル・系統・区分間での相互接続性がなく、UFSAR に記載された設計機能における多重性・多様性・分離・独立性が低下しないならば、変更の評価はむずかしくない。しかし、デジタル変更が、①異なる系統間のネットワークや設計機能の合体、②チャンネル・系統・区分間での相互接続性または、③リソースの共有をもたらす場合は、UFSAR に記載された設計機能における多重性・多様性・分離・独立性を減じることがないよう設計属性が適切に取り入れられていることを、注意深くレビューする必要がある。
- デジタル改造内で異なる設計機能を合体するとは、同じデジタル機器内で直接、異なる系統の設計機能を合体するか、間接的に共有リソースを通じて合体するかである。共有リソースには、双方向デジタル通信／ネットワーク、共通制御器、電源もしくは多機能表示・制御ステーションが含まれる。デジタル改造で導入された共有リソースは、UFSAR に記載された設計機能における多重性・多様性・分離・独立性を減じることになる。

3.1. 定性評価要素

- ここでは、NEI01-01 と整合させて、3 ファクタ：（1）設計属性、（2）設計プロセスの品質、（3）運転経験について説明する。これらのファクタを個別に、また、全体として定性評価し、図書化することによって、事業者は、「第三者による検証が十分可能なほど詳細に」定性評価を図書化できる。なお、設計属性と設計プロセスの品質は相互関連する（つまり、設計プロセスの品質は、設計属性の適切な導入を保証する）。だから、これら 2 つの要素は定性評価に必須である。このガイダンスは、安全関連系統やコンポーネントの改造に適用されるが、事業者の裁量で、非安全関連系統やコンポーネントの改造にも適用可能である。
- 表 1 には、設計属性、設計プロセスの品質と運転経験の例が示されている。このリストが全てではないし、各項目に定性評価が必要というわけではない。

3.1.1. 設計属性

- NEI01-01 § 5.3.1 は、「デジタルシステムが十分に総合信頼でき〈dependable〉、故障発

生可能性が十分に低いと判定するためには、評価しなければならない重要な特性がある。（中略）こうした特性とは、高い総合信頼性に寄与するハードウェアとソフトウェアの機能仕様〈design feature〉を含む。機能仕様の例は、組込み式の不良検知・故障管理スキーム、内部多重性・内部診断、故障影響を最小化し問題診断を容易にするよう設計されたソフトウェアとハードウェア・アーキテクチャの使用である。」と言っている。

- 変更の設計属性によって、故障の発生を防いだり限定したりできる。設計属性は、主には、不良検知・故障管理スキーム、内部多重性、統合ソフトウェア・ハードウェア・アーキテクチャの診断といった組込み式機能仕様に重点を置いている。しかし、改造の外側にある機能仕様（弁の機械式閉止機能、ポンプ速度制限器など）も考慮すべき場合がある。
- 多くの系統設計属性、系統設計手順、系統設計実務（practices）が、CCF 等の故障発生可能性の低減に寄与する。事業者は、変更内の想定故障モード（CCF など）を通して、脆弱性評価し、脆弱性に対処する設計属性を適用することによって、故障発生可能性が低いことを説明できる。故障発生可能性の適切な定性評価により、変更がもたらすかもしれない潜在的故障が示され、その潜在的故障を解消するための設計属性が特定される。
- 多様性は、デジタル技術を使って改造された SSC において、潜在的 CCF によって設計機能が喪失することを防ぐ設計属性の一例である。なお、プラントの設計ベースがすでに設計の一部として多様性を記述している場合もある。とにかく、多様性は、設計機能に影響する故障発生を減少させる強力な手段である。

3.1.2. 設計プロセスの品質

- NEI01-01 § 5.3.3 は、「デジタル機器では、品質と総合信頼性の前提条件は、「プロジェクト管理、ソフトウェア設計、開発、実装、検証〈validation〉、妥当性確認〈verification〉、ソフトウェア安全解析、変更管理と構成管理」のための明確なプロセスと経験豊富なソフトウェア工学専門家の組み合わせである。」と言っている。
- こうしたプロセスには、ソフトウェア開発、ハードウェアとソフトウェアの統合プロセス、系統設計、開発に組み込まれた妥当性検証と試験プロセスが含まれる。安全関連のデジタル機器向けの開発プロセスは図書化され、定性評価の参考情報として使用可能である。しかし、商用品格上げ（CGD）製品や非安全関連デジタル機器においては、開発プロセ

スの図書化は一般的ではない。こうした場合、定性評価は設計属性とそうした機器の運転経験（成功例）に重きを置く場合もある。

- 設計プロセスの品質は、改造の総合信頼性を判断するための重要項目である。適用可能な産業合意標準〈applicable industry consensus standards〉を使用すれば、設計プロセスの品質に寄与するし、従前に許容されたアプローチの使用となる。標準の例：IEEE 1074-2006[a]。
- 品質標準は、QAP や品質保証手順と混同してはならない。品質標準は、設計において達成される基準（benchmarks）を記したものである。品質標準は、合意に基づき作成され、公認の標準策定機関によって認証されなければならない。例えば、IEEE。品質標準は、必ずしも NRC スタッフによってエンドースされたものである必要はない。定性評価図書には、適用される標準が使用される環境下で有効であることを示さなければならない。
- 非安全関連の SSC に対しては、一般に許容されている商用標準に合致していることで十分な場合がある。定性評価には、機器開発に使用されたこうした一般に許容されている商用標準のリストを載せること。もし、NRC がエンドースした産業標準が、設計プロセスもしくは製造プロセス、または、その両方に適用されている場合は、これらの標準を定性評価図書に含め、品質の証拠として使うこともできる。

3.1.3. 運転経験

- NEI01-01 § 5.3.1 は、「豊富で適用可能な運転経緯は、十分な総合信頼性を証明する上での不確かさを減少させる。」と言っている。
- 関連する運転経験は、改造に用いられたデジタル機器が十分な総合信頼性を持つことを評価したり、示したりする助けとなる。改造されたシステムやコンポーネントが、原子力発電所で、もしくは、非原子力適用ではあるが匹敵する性能基準と運転環境下で使用された豊富な経験があることを示す情報を図書化してもよい。そうした機器の供給者が、不断のプロセス改善や教訓の組込みといった品質プロセスを取り入れ、十分な機器総合信頼性を示す方法を図書化していることを追加してもよい。
- 改造 DIC と運転経験で担保された DIC の間に差異が存在する場合がある。そういう場合でも、リファレンス機器のアーキテクチャとソフトウェアは、変更機器のそれとほとんど

[a] IEEE std. 1074-2006, IEEE Standard for Developing a Software Project Life Cycle Process
これは、RG1.173“Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plant” でエンドースされている。

同等でなくてはならない。

- さらに、リファレンス機器の設計条件と機器の運転モードも、改造 DIC のそれとほとんど同等でなくてはならない。解析者は、運転条件（環境雰囲気、連続負荷など）を理解していないといけない。他の施設での運転経験を担保とする場合は、運転経験が担保されているのは、どの設計機能仕様であるかを理解しておく必要がある。関連する運転経験として参考にされる設計において、潜在的な CCF を防止し、制限するのに寄与する設計機能仕様は、図書化され、改造にも取り入れるべきである。そうすることで、改造設計の総合信頼性が、リファレンスと同等であると判断する助けとなる。

表 1　定性評価ファクタの例

ファクタ	例
設計属性	• 深層防護、多様性、独立性、多重性（該当する場合） • 統合ソフトウエア・ハードウェアもしくはアーキテクチャ/ネットワークの固有の設計特性（例：独立したソフトウェアを動かすウォッチドッグ、隔離機器、分散ネットワークのセグメンテーション、自己検査、自己診断機構） • ノンコンカレント・トリガー（非同時並行トリガー） • 充分にシンプル（NEI01-01 § 5.3.1） • 試験性（例：試験可能） • 故障解析で特定された故障の解消法
設計プロセスの品質	<u>安全関連機器</u> • 適用可能産業界コンセンサス標準 • その他の標準 • Appendix B 供給者の利用（Appendix B 供給者を用いていない場合は、どの品質プログラムが適用されているか分析要） • EPRI TR-106439 にしたがった CGD プロセスの利用 • IEEE Std. 7-4.3.2[a]の Annex D と EPRI TR-107330[b]の例にしたがった CGD プロセスの利用 • SSC が設計機能を発揮することを担保できる環境条件に対する性能認証図書（例：EMI、RFI、地震） • 広範囲な評価や試験を通じて示されたカスタム・ソフトウェア・コード（アプリケーション・ソフトウェア用）の総合信頼性 <u>非安全関連機器</u> • 一般に許容された商用標準の遵守 • 交換される機器（オリジナル）と匹敵するもしくは凌駕する設計仕様を示す調達または製造者図書、もしくは両方。 • 設計要求と仕様の検証

[a] IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations
[b] TR-107330, Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants

ファクタ	例
運転経験	• 変更と類似の製品、運転環境、負荷サイクル、負荷、かつ同等構成（ラインアップ）における運転経験 • 現場経験から得られた設計に言及した教訓の経緯 • DIC 改造に用いられる機器と同等として参照される関連する運転経験： ➢ 参照機器とソフトウエア（OS とアプリケーション）のアーキテクチャ ➢ 設計条件と運転モード ➢ 他の適用先で使われた運転経験を持つ高品質商用品 ソフトウェアの場合、限定使用のソフトウェアやカスタム・ソフトウェア、ユーザー変更可能なソフトウエア・アプリケーションは課題が多い ➢ 構成ファイルを作成するために用いるソフトウェア開発ツールの経験

3.2. 定性評価の図書化

- NEI96-07 改訂 1 の § 5.0 と NEI01-01 の付録 B は、NRC がエンドースした 10CFR50.59 評価を図書化するためのガイダンスである。両者とも、図書には、「見識ある専門家が同じ結論を導きだせる」ように、「結論の根拠を十分に示す説明」を含めることを強調している。
- そのためには、検討された項目ならびに、それらの定性評価への影響（個々および全体）を詳細に明確に図書化しないといけない。他の図書を参照する場合は、図書名と情報の場所（セクション、ページなど）を含めなければならない。
- 定性評価ファクタが使われている場合は、表 1 に示された例にならって、肯定否定の両面を考慮しつつ、各ファクタについて考察する（図書の中で）。どのカテゴリがどの程度定性評価の結論に寄与したかも考察する（図書の中で）。

4. 工学的評価：故障解析

- NEI01-01 の § 4.4.2 と 5.1 のとおり、故障解析は、変更〈change〉が多重性、多様性、分離、独立性を減じたかどうか[a]を判断するのに必要な洞察を与える。ソフトウェアによる故障に加えて、デジタル改造の他の影響は新たな機能不良（機能結合、他のシステムとの新たな相互作用、応答時間の変化など）をもたらす場合があることに注意すべきである。設計は、こうした他の影響も対処すべきである。例えば、従前は別々だった機能が単一のデジタル機器に統合された場合、以前は個々の設計機能にのみ影響していた単一故障が、複数の設計機能に影響し得る。潜在的な相互接続ハザードが特定されるような場所では、適切な設計属性の組込みによって、こうしたハザードに対処すべきである。将

[a] いずれも、機能不良発生可能性の最低限以上の増加をもたらすとみなされる。

来のプラント設計変更でも、こうしたハザードに適切に対処できるように、潜在的ハザードの解析と解消法について丁寧に図書化しておくことが重要である。

4.1. 故障解析

- 故障解析を使用して、CCF の潜在的な脆弱性を特定し、設計のさらなる改造の必要性を評価できる。設計機能と設計属性を使用することで、さらなる潜在的故障の検討を除外できる場合もある。内部多様性〈internal diversity〉やセグメンテーションなどの設計属性や機能を使用する改造は、CCF の可能性を最小にするのに役立つ。同様に、他のシステムによるバックアップ能力は、CCF に対処できる。CCF 脆弱性の源は、多重チャネルに導入した同一ソフトウェア、共有リソースの使用、または異なる設計機能を果たす相互接続されたシステムにわたる共通のハードウェア／ソフトウェアの使用が含まれる。他の検討項目は、望ましくない挙動は、必ずしも SSC 故障が原因ではなく、誤操作（偽起動、誤った制御など）が原因である可能性があること。したがって、CCF 源を可能な範囲で特定し、設計プロセス中にそれらに対処することが不可欠であり、そうすることが、改造に対する技術根拠をサポートすることにもなる。
- 複数の SSC に影響を与える可能性のある CCF 源を持つデジタル設計は、従前に UFSAR で評価されたものとは異なるタイプの事故または異なる結果をもたらす機能不良を発生させないことが確かであることをレビューする必要がある。これはまさに、CCF の共通の源が、共通のトリガーにさらされるケースである。例えば、改造された SSC と、同一のハードウェアとソフトウェア、電源、またはヒューマンマシンインターフェイスを使用する他の SSC とのインターフェイスは、丁寧にレビューして、潜在的な共通トリガーは既に対処済みであることを確かめる必要がある。
- 事業者の UFSAR が「最適評価」手法を組み込んでいない限り、UFSAR で評価されたものと異なる結果を評価するために、「最適評価」を使用することはできない。
- 故障解析により、ソフトウェア開発および構成ツールを通じて導入された CCF の潜在的な源も明らかになり得る。CCF の潜在的な源として、個々のプログラマブルロジックデバイスまたはユーザー設定が可能なデバイスについて、注意深い検討を要する。

デジタル通信

- SSC の独立性への影響を除外するために、デジタル通信の故障解析に注意を払うべきである。デジタル通信は、新しいタイプの故障モードにつながる相互作用をもたらす可能

性がある。デジタルネットワークもしくはチャンネル間、区分間、異なる系統間の相互接続性をもたらすようなデジタル改造には、設計属性を適切に取り入れて、多重性、多様性、分離、独立性を減じることがないようにしなくてはならない。IEEE7-4.3.2[a]のような産業基準に適合していれば、設計属性が非安全系 SSC の変更も含めて、デジタル通信の改造に伴う潜在的な故障モードに対処していることの説明となる。

設計機能の統合と共有リソース

- 潜在的な故障モードを特定するのがより困難になる新たな相互依存性や相互作用をもたらす可能性があるため、異なる安全系もしくは非安全系の SSC における設計機能の統合は、故障解析で取り扱う必要がある。統合した設計機能もしくは共有リソースの故障は、1）UFSAR で評価された事故もしくは SSC の機能不良に影響する、または、2）異なる深層防護レベルに関わることが懸念される。
- 分離されたコンポーネント機能の統合は、より総合信頼性が高いシステムパフォーマンスをもたらす。なぜなら、コンポーネント間の結合性が高まり、複雑さが低減するためである。安全関連もしくは非安全関連 DIC 改造において、設計機能の統合もしくは共有リソースの取り入れを事業者が提案しているのならば、事業者は新たな故障可能性に重きを置く必要がある。故障解析や制御システムのセグメンテーション解析は、潜在的課題を特定するのに役立つ。セグメンテーション解析は、とりわけ非安全系の分散型ネットワークの評価に役立つ。

深層防護解析

- 深層防護原理を適用することは、CCF 脆弱性の対処方法となり得る。NEI01-01 では、原子炉保護系や工学的安全施設起動系（ESFAS）のデジタル交換に限定して、深層防護解析の必要性を述べている。しかし、深層防護解析は、共有リソース、共通のハードウェア・ソフトウエアもしくは設計機能の統合によってもたらされる新たな潜在的な CCF の影響を明らかにするため、いかなるデジタル変更の評価に用いることが可能である。さらに、深層防護解析は、既存の SSC とのインターフェイスへの直接的／間接的影響を明らかにすることも可能である。この種の解析は、変更によりもたらされる CCF 脆弱性の効果が、既存の SSC や手順によって緩和され得ることを示すことも可能である。

[a] IEEE 7-4.3.2-2016 - IEEE Standard Criteria for Programmable Digital Devices in Safety Systems of Nuclear Power Generating Stations

4.2. 故障解析による解消法とその図書化

- 事業者は、NRC が承認した QAP にしたがって、DIC 変更に関する図書を作成し維持しなければならない。故障解析図書は、設計に持ち込まれた脆弱性と脆弱性による故障の影響を特定するものである。さらに、NEI01-01 § 5.1.4 に書かれているように、故障解析図書は、特定された故障を解消する設計仕様や手順を特定する。図書の詳細は、安全重要度や改造の複雑さに関連しているべきである。
- 事業者は、故障解析を展開し、図書化する際には、表 2 を使うこともできる。図書には、レビューワが同じ結論にたどり着けるように、故障が除外される、もしくは故障が限定される根拠が適切に示されるべきである。

表 2　例：故障解析による解消法とその図書化

ステップ	記述
ステップ 1 **特定**	• 他の SSC との相互接続や共有特性も含めた変更のスコープ、境界を記述する。 • 変更によって影響を受ける設計機能（UFSAR に記載されたもの）をリストアップする。 • 変更された設計がもたらす新しい設計機能（オリジナルにない）を記述する。 • 変更された設計によって取り除かれた設計機能を記述する。 • 変更によって統合される前の設計機能を記述する。 • 手動制御に移行される自動操作を記述する。 • 自動制御に移行される手動操作を記述する。 • 運転モード及びある運転モードから別のモードへの推移を記述する。
ステップ 2 **故障モード比較**	• 新たなデジタル機器の故障モードと交換前の機器の故障モードを比較する。 • 故障モードが異なる場合、UFSAR に記載された設計機能に対する機器故障の影響を記述する。潜在的な故障をもたらしたかもしれない。 ➢ 特定された潜在的故障モードもしくは望ましくない挙動を記述する。 例：ハードウェア、ソフトウェア、統合機能、共有リソースの使用、ソフトウエアツール、プログラマブル・ロジック機器もしくは共通ハードウェア/ソフトウェアに関係する故障モード ➢ 変更されていない他の SSC の CCF と共通のトリガー機構にもさらされ、変更によりもたらされる CCF の潜在的原因を記述する。 • 特定された潜在的故障が、どのように解消されるか説明する。（NEI01-01 § 5.1.4 参照）
ステップ 3 **機器の総合信頼性と CCF 頻度の決定**	• 表 1 の定性評価ファクタに基づいて、新しいデジタル機器は、少なくとも交換前の機器と同等の信頼性（reliable）を有するか？

ステップ	記述
ステップ 4 機器の総合信頼性と CCF 頻度の結果評価	• もし、ステップ 3 が YES もしくは、新しいデジタル機器の総合信頼性（dependability）のレベルが許容可能と判断されるならば、 ➢ 結論の根拠を記述する。 ➢ ステップ 5 に進む。 • もし、ステップ 3 が NO なら、設計変更を検討するか、既存の設計機能のバックアップ能力に頼る。
ステップ 5 図書化	• 結果と到達した結論をまとめる。UFSAR に記載された設計機能に影響があるならば、変更がもたらす影響を考察する。機器故障モードに関する相違ならびに、UFSAR に記載された設計機能への異なる故障モードの影響について考察する。潜在的 CCF 脆弱性を解消する取り入れた設計属性を記述する。 • 関係図書の例: ➢ 設計に適用する規格・基準 ➢ 機器環境条件（例：雰囲気温度、電磁波妨害（EMI）、無線周波妨害（RFI）、地震） ➢ 使用されている品質設計プロセス（例：NQA-1 のパート II、サブパート 2.7[a]） ➢ 汎用品格上げ（CGD）図書（例：EPRI TR-106439[b]に記載のもの、該当する場合） ➢ 故障モードと影響解析（該当する場合） ➢ ソフトウェア・ハザード解析（該当する場合） ➢ クリティカル設計レビュー（例：EPRI TR-1011710[c]に記載のもの、該当する場合） ➢ 機器の運転経験の図書
ステップ 6 故障解析結果の 10CFR50.59 評価基準への適用	• 10CFR50.59 評価の質問に対して、工学的結論を適用する。

[a] Quality Assurance Requirements for Computer Software for Nuclear Facility Applications
[b] TR-106439, Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications
[c] TR-1011710, Handbook for Evaluating Critical Digital Equipment and Systems

添付資料②

RG1.182 改訂 2 抜粋
「10CFR50.59”変更、検査及び試験” 導入ガイダンス」

令和 2 年 10 月 29 日

技術基盤課

1. 解説

改訂理由〈Reason for Revision〉

RG1.187 改訂 2[a]は、デジタル計装制御（DIC）改造〈modification〉の際の 10CFR50.59[b]要求適合に関するガイダンスを提供している。特に、この改訂 2 は、いくつかの確認項目があるが、NEI96-07 付録 D 改訂 1[c]のガイダンスが DIC 改造の際に 10CFR50.59 に適合するアプローチを提供していることを認めるものである。

背景

10CFR50.59 に基づき、事業者〈licensees〉は NRC の変更認可なしで、更新最終安全解析書（UFSAR）に記載された施設〈facility〉や手順〈procedures〉を変更〈changes〉または、UFSAR に記載されていない検査〈tests〉や試験〈experiments〉を実施することが許されている。1999 年に 10CFR50.59 が改訂された後、米国原子力エネルギー協会（NEI）は 10CFR50.59 の導入ガイダンス NEI96-07 改訂 1[d]を発行した。2000 年 11 月に、NRC は RG1.187 改訂 0 を発行し、NEI96-07 改訂 1（以降 NEI96-07 と呼ぶ。）をエンドースした。

NRC は 2001 年と 2007 年に、10CFR50.59 に影響する 2 つの規則を発布し、2019 年 5 月に RG1.187 改訂 1 を発行し、NEI96-07 改訂 1 の § 4.3.5 にある「異なるタイプの事故」の意味と § 4.3.8 にある「評価手法からの逸脱」の定義を明確化した。同時に、NEI96-07 付録 D 改訂 0（2019 年 1 月発行）に対して、いくつかの除外と追加を行うことでエンドースする RG1.187 改訂 2 ドラフト（DG-1356）を発行した。2020 年 5 月に、NEI は NEI96-07 付録 D 改訂 1（以降付録 D と呼ぶ。）を発行し、DG-1356 で指摘された除外事項を解消した。

---

[a] RG1.187, Rev. 2, GUIDANCE FOR IMPLEMENTATION OF 10CFR50.59, “CHANGES, TESTS, AND EXPERIMENTS,” June 2020

[b] 10CFR50.59：「PART 50—DOMESTIC LICENSING OF PRODUCTION AND UTILIZATION FACILITIES」のセクション 59「Changes, tests and experiments.」

[c] NEI96-07, Appendix D, Supplemental Guidance for Application of 10CFR50.59 to Digital Modifications, Revision 1, May 2020

[d] NEI96-07, Rev. 1, GUIDELINES FOR 10CFR50.59 IMPLEMENTATION, November 2000

デジタル改造に関する背景

I&C 設備の改造には、デジタル技術を使用する新しい設備、又は機器の導入、アナログ機器のデジタル技術への更新、あるいは既存デジタル機器の更新が含まれる。NEI は、そうした変更により発生する可能性のある課題に対処するために、2002 年 3 月に NEI96-07 改訂 1 を補足する DIC に特化したガイドラインとして、NEI01-01[e]を発行し、NRC は、2002 年 11 月に RIS2002-22[f]を発行し、NEI01-01 をエンドースした。

RIS2002-22 の発行を受けて、事業者は NEI01-01 を使用して DIC 更新を実施したところ、NRC 検査において、10CFR50.59 に記載された NRC 認可を要する「変更、検査及び試験」の基準（表 1）の解釈に事業者と NRC の間で相違があることがわかった。

表 1 10CFR50.59 に記載された NRC 認可を要する「変更、検査及び試験」の基準

「変更、検査及び試験」が以下に該当する場合は、それを実施する前に 10CFR50.90 にしたがい、事業者は NRC から変更認可を得なくてはならない。	
i)	UFSAR で従前に評価した事故発生頻度〈the frequency of occurrence of an accident〉に関して、最小限以上の増加〈more than a minimal increase〉をもたらす場合
ii)	UFSAR で従前に評価した安全上重要な SSC の機能不良〈the likelihood of occurrence of a malfunction〉に関して、最小限以上の増加をもたらす場合
iii)	UFSAR で従前に評価した事故の影響〈the consequences of an accident〉に関して、最小限以上の増加をもたらす場合
iv)	UFSAR で従前に評価した安全上重要な SSC の機能不良影響〈the consequences of a malfunction〉に関して、最小限以上の増加をもたらす場合
v)	UFSAR で従前に評価したどれとも異なるタイプの事故〈an accident of a different type〉をもたらす可能性〈possibility〉がある場合
vi)	UFSAR で従前に評価したどれとも異なる結果〈with a different result〉をもたらす安全上重要な SSC の機能不良が発生する可能性がある場合
vii)	UFSAR に記載された核分裂生成物（FP）境界の設計基準限界〈a design basis limit〉を超過または、改めるような結果をもたらす場合
viii)	設計基準を構築する際または、安全解析を行う際に用いられた UFSAR に記載された評価方法からの逸脱〈a departure from a method of evaluation〉をもたらす場合

[e] NEI 01-01, A Revision of EPRI TR-102348 to Reflect Changes to the 10 CFR 50.59 Rule: Guideline on Licensing Digital Upgrades, EPRI TR-102348 Revision 1, March 2002

[f] RIS2002-22, Use of EPRI/NEI Joint Task Force Report, "Guideline on Licensing Digital Upgrades: EPRI TR-102348, Revision 1, NEI01-01: a Revision of EPRI TR-102348 to Reflect Changes to the 10 CFR 50.59 Rule," November 2002

これを受け、NRC は、2018 年 5 月に RIS2002-22 補足 1[g]を発行して、NEI01-01 を継続してエンドースするとともに追加のガイダンスを提供した。特に、RIS2002-22 補足 1 は、共通要因故障（CCF）発生可能性を含むデジタル変更の故障可能性を評価する際に使用可能な「定性評価〈qualitative assessments〉」の方法と図書化に関するガイダンスを提供している[h]。

2. NRC スタッフ規制ガイダンス

(1) NEI96-07

NRC スタッフは、NE96-07 のガイダンスを、10CFR50.59 要求に適合する 1 手段として使用することを概ねエンドースする。しかし、NEI96-07 に記載の以下の事項を明確化〈clarification〉する。

A) § 4.3.8 に記載の評価方法からの逸脱とみなさい変更の例

事業者が認められている評価方法の改訂は、10CFR50.59(a)(2)に書かれている以下のどちらかの場合である：（1）UFSAR に記載の方法の要素に対する変更、（2）UFSAR に記載の方法から他の方法への変更。もし、評価方法の改訂が（2）の場合は、10CFR50.59(a)(2)(i)に示された「解析結果は保守的もしくは本質的に同じである」は、適用されない。

B) § 4.3.5 に記載の異なるタイプの事故について

UFSAR は、広範囲の過渡と事故または起因事象を評価しており、事故はプラントへの影響に基づくタイプで分類されている。タイプによって事故を分類することで、事象同士の比較が可能となり、限界ケース〈the limiting cases〉かどうかの特定と評価の根拠が得られる。異なるタイプの事故を特定する助けとして、UFSAR 解析は既往機器の想定可能な故障モード〈credible failure modes〉に基づいていることを考慮すること。さらに、提案されている変更が限界シナリオ〈the most limiting scenario〉の根拠を変えることになるかどうか特定すること。また、限界ケースでない事故は、UFSAR では議論されていないことにも留意すること。

異なるタイプの事故は新しい事故であり、UFSAR で従前に評価されたものと異なるが、頻度と重要度〈significance〉は類似している。こうした異なるタイプの事故では、既存の解析の改訂ではなく、異なる事故解析が必要となる。

---

[g] RIS2002-22, Supplement 1, Clarification on Endorsement of NEI Guidance in Designing Digital Upgrades in I&C Systems, Revision 1, May 2018

[h] 本補足 1 は、原子炉保護システム、工学的安全施設作動システム（ESFAS）の DIC への更新、又はこれらのシステムの内部ロジック部分（例：多数決ロジック、双安定入力、信号調整・処理等）の変更・交換については対象としていない。本補足を適用すると、他にも考慮すべき事項が出てくるためである。

C) 参照図書と事例

NEI96-07 で参照されている図書は、NRC によりエンドースされているとは限らない。NEI96-07 のガイダンスを補足する目的の事例は、すべての事業者に適用できるとは限らない。事業者は、事例に示されたガイダンスを導入する前に、事例が適用されている環境条件を確かめる必要がある。

D) 許認可更新向けの FSAR 補足のガイダンス

NEI96-07 と本 RG のガイダンスは、FSAR に加えられた情報の変更にも適用可能である。

E) 実用発電炉以外の事業者への適用性

実用発電炉以外の事業者も、NEI96-07 のガイダンスを使用することができる。ただし、いくつかの項目は、こうした事業者には完全に適用されない規制要求を扱っていることに留意。

(2) 付録 D

付録 D は、デジタル改造にのみ適用可能であり、NRC は、一般適用可能とはみなしていない。NRC は、付録 D につき、以下の項目を明確化する。

a） NEI01-01 との関係

- 付録 D には、それは NEI01-01 に置き換わるものと述べられているが、NRC は、RIS2002-22 補足 1 に明記されているように、NEI01-01 改訂 1 も引き続き使用可能とみなしている。
- 事業者が、NEI01-01 改訂 1 か付録 D のどちらを使用するか選択可能。ただし、両者から、一部を選択して使用することは付録 D にも書かれていないし、NRC もエンドースしない。

b） NEI96-07 改訂 1 からの変更

i. ヒューマンシステムインターフェイス（HSI）

付録 D には、HSI に対するスクリーニング・ガイダンスも提供している。NEI96-07 では、HSI の変更は、設計機能を働かすもしくは制御する既往の手段を基本的に変えることになることから、自動的にスクリーンインとされている。一方で、NEI01-01 では、HSI の変更は必ずしも設計機能を働かすもしくは制御する既往の手段を基本的に変えることにはならないと述べている。付録 D も NEI01-01 と同様である。NRC スタッフは、付録 D で示されるように HSI への変更をスクリーニングすることに賛成する。

ii.　評価結果としての許容基準〈acceptance criteria〉の使用

付録 D では、改訂した安全解析が許容基準を満たさない場合は、デジタル変更には、異なる結果をもたらす安全上重要な SSC の機能不良発生可能性があると述べられている。一方、NEI96-07 では、異なる結果をもたらす安全上重要な SSC の機能不良発生可能性を判定する目的での許容基準の使用について言及していない。NEI96-07 では、SSC の故障モードのタイプと結果を特定し、機能不良が事故解析の中で評価されたかどうかに留意することと述べられている。NRC の見解は、「NEI96-07 のガイダンスに加えて、付録 D のガイダンスを用いることができる」である。

c） 十分に低いソフトウェア CCF 頻度

RIS2002-22 補足 1 が、現状唯一の NRC が発行した「ソフトウェア CCF 発生可能性が十分低い」ことを示すためのガイダンスであり、付録 D と併せて用いることができる。

d） 付録 D の § 4.3.6 ステップ 6「基本過程と許容基準」

ステップ 6 には、「変更により、異なる結果をもたらす安全上重要な SSC の機能不良発生可能性」を判断する上で、下記の2段階判定法が示されている。

① 基本的仮定が無効となったこと（例：単一故障仮定が維持されない）により、安全上重要な SSC の機能不良に関わる従前の評価が無効になったかどうか。

② 既安全解析が無効になったかどうか（安全解析上の許容基準を満足しなくなったかどうか）。

①に関して、事業者は、既往安全解析結果とデジタル変更にともなう安全解析への影響分析結果を適切に比較しなければならない。そのために、NRC スタッフは以下を明確にする。まず、付録 D には、「基本的仮定」が定義されていない。NRC の理解は、「基本的仮定」とは、設計の適切性〈adequacy〉を証明する際に機能すると仮定する SSC の設計機能である。それには、安全解析では特に特定されていないが、担保された設計機能が含まれる。§ 4.3.6 では、基本的仮定の例として単一故障仮定が示されているが、他にも、（1）担保されたプラント／原子炉保護系機能が働くこと、（2）担保された工学的安全系機能が働くこと、（3）担保されたプラントシステム機能と関連する I&C 機能が働くことが含まれる。

②に関して、もし FSAR に、SSC の一機能に対して複数の許容基準が示されていたら、既存の安全解析が変更に対しても紐づけされることを示すためには、全ての許容基準に満足していることを示す必要がある。

一方で、許容基準が FSAR に直接述べられていない場合があるので、事業者は FSAR で参照されている図書にあたる必要がある。さらに、安全解析の結論において、想定事象に対する安全解析結果のみが示され、許容基準に言及していない場合もある。そのため、ステップ 6 を実施するには、事業者は全ての適用される許容基準を特定する必要がある。

添付資料③

NEI96-07 付録 D 改訂 1
「デジタル改造に 10CFR50.59 適用するための補足ガイダンス」

令和 2 年 10 月 29 日

技術基盤課

エグゼキュティブサマリー

2020 年に発行された NEI96-07 付録 D 改訂 1[a]（以降、付録 D と呼ぶ。）は、NEI96-07 改訂 1 本体[b]（2000 年発行、以降、NEI96-07 と呼ぶ。）に含まれるガイダンスをデジタル改造〈digital modification〉に関わる活動〈activities[c]〉に特化して補足するものである[d]。付録 D の主目的は、デジタル改造に関わる活動に 10CFR50.59[e]プロセスをどのように適用させるかについて、共通のフレームワークと共通の理解を全てのステークホルダーに提供すること。付録 D は、NEI01-01[f]に含まれる 10CFR50.59 関連のガイダンスを置き換える[g]ものであり、RIS2002-22 補足 1[h]に含まれる 10CFR50.59 関連の「定性評価〈qualitative assessment〉ガイダンスも取り込んでいる。

1. 序論

デジタル改造に関わる活動には、10CFR50.59 プロセスに沿った特別な考慮が必要となる。こうした考慮の対象は、改造前の機器とは異なる潜在的故障モード〈potential failure mode〉、前は独立していた複数機器の機能が、コンポーネント／系統レベル、もしくは、複数系統レベルで統合された影響〈effect〉、ソフトウェア共通要因故障（CCF）の可能性である。

1.1. 背景

事業者は、既存設備の陳腐化によるトラブル増加、交換部品の入手困難、及び保守費増加等から、性能や信頼性向上が見込めるデジタル計装制御（DIC）の利用を必要としている。このため、NEI01-01 が 2002 年に発行され、NRC が RIS2002-22[i]でエンドースしたが、2002 年以降デ

---

[a] NEI 96-07, Appendix D, Supplemental Guidance for Application of 10CFR50.59 to Digital Modifications, Revision 1, May 2020。NRC が RG1.187 改訂 2 で、改訂 D に含まれるガイダンスをエンドースした。

[b] NEI 96-07, Revision 1, GUIDELINES FOR 10CFR50.59 IMPLEMENTATION, November 2000

[c] 10CFR50.59 の「change, test, or experiment」を総称したもの。

[d] 付録 D では使い易さを考慮し、NEI96-07 の構成（セクション構成）を踏襲する。

[e] 10CFR50.59：「PART 50—DOMESTIC LICENSING OF PRODUCTION AND UTILIZATION FACILITIES」のセクション 59「Changes, tests and experiments.」

[f] NEI 01-01, A Revision of EPRI TR-102348 to Reflect Changes to the 10 CFR 50.59 Rule: Guideline on Licensing Digital Upgrades, EPRI TR-102348 Revision 1, March 2002

[g] NRC の見解は異なり、NEI01-01 改訂 1 は引き続き適用可能としている。

[h] RIS2002-22, Supplement 1, Clarification on Endorsement of NEI Guidance in Designing Digital Upgrades in I&C Systems, Revision 1, May 2018

[i] RIS2002-22, Use of EPRI/NEI Joint Task Force Report, "Guideline on Licensing Digital Upgrades: EPRI TR-102348, Revision 1, NEI01-01: a Revision of EPRI TR-102348 to Reflect Changes to the 10 CFR 50.59 Rule," November 2002

ジタル改造が広がり、バラエティに富んだことから、10CFR50.59 ガイダンスとして NEI01-01 の記載内容が不十分になってきた。

2018 年に RIS2002-22 補足 1 が発行され、NRC が NEI01-01 に含まれるガイダンスをエンドースしていることを再確認するとともに、デジタル改造がもたらすソフトウェア CCF を含む故障発生可能性〈likelihood of failure〉を「定性評価〈qualitative assessment〉」するためのガイダンスが示された。

RIS2002-22 補足 1 は、定性評価は、「DIC 改造の結果、事故発生頻度〈the frequency of occurrence of accidents〉、もしくは、機能不良発生可能性〈the likelihood of occurrence of malfunctions〉が有意に増加しない〈more than a minimal increase〉」という結論をサポートする目的で使用可能であることを示した。定性評価はまた、「改造によって、更新最終安全解析書（UFSAR）の中で従前に評価されたものと異なるタイプの事故〈an accident of a different type〉、もしくは、異なる結果をもたらす機能不良〈a malfunction with a different result〉が発生する可能性〈possibility〉がもたらされない」という結論をサポートする目的でも使用可能である。

1.2. 目的

付録 D は、デジタル改造に特化して、事業者が 10CFR50.59 のスクリーニングと評価を行うためのガイダンスであり、NEI96-07 に含まれるガイダンスを変えるものでも、異なる解釈を与えるものでもない。

デジタル改造に関わるものの例は、コンピューター、コンピュータープログラム、データ、組み込み型デジタル装置（EDD）、ソフトウェア、ファームウェア、ヒューマンーシステム・インターフェイス（HSI）、マイクロプロセッサ使用機器、プログラマブルデジタル機器である。付録 D の適用対象は、スタンドアローンの I&C システムに限定されない。もし、機械もしくは電気機器がデジタル技術を使っているなら、それらにも適用される（例：組み込み型マイクロプロセッサ制御系を含む換気空調（HVAC）設計）。本ガイダンスは、安全関連にも非安全関連システム／コンポーネントにも適用される。デジタルからデジタルへの変更もカバーする。

1.3. 10CFR50.59 プロセスの概要

追加のガイダンスなし。

1.4. 10CFR72.48[a]の適用性

追加のガイダンスなし。

1.5. 本ガイダンス図書の内容

添付 D と NEI96-07 の関係

- 添付 D の§3 と 4 で NEI96-07 を参照している。

ガイダンスの焦点

- §4.2 と 4.3 では、特定の観点に焦点をあて、その他の観点を意図的に除外している。特に関心の高い観点に絞るためであり、その他の観点が関係しないわけではない。

事例

- 事例は、そのセクションに書かれている観点のみに対応するものである。意図的に除外された観点から、結論が変わる場合もある。

2. 深層防護設計思想、及び 10 CFR 50.59

追加のガイダンスなし。

3. 用語の定義

§3.1~3.14 は、NEI96-07 と同じ。

3.15. 定性評価〈Qualitative Assessment〉

定義

- 10CFR50.59(c)(2)に書かれた基準の(i) (ii) (v) (vi)[b]に対する 10CFR50.59 評価に有効な技術に基づく工学的評価〈technical-based engineering evaluation〉である。

解説

- 定性評価の目的は、ソフトウェア CCF の発生可能性〈the likelihood of a software CCF〉の大きさ〈magnitude〉を判定〈determine〉することだが、それは、「十分に低い〈sufficiently low〉」か、「十分に低くない〈not sufficiently low〉」かのどちらかである。
- 定性評価は、通常、10CFR50.59 評価全体より前、もしくは、並行して実施される。
- 一般に、ソフトウェア CCF による故障の発生可能性が低いことは、(1)改造された構造／システム／コンポーネント(SSC)の設計属性〈design attribute〉、(2)設計プロセスの品質

---

[a] PART 72—LICENSING REQUIREMENTS FOR THE INDEPENDENT STORAGE OF SPENT NUCLEAR FUEL, HIGH-LEVEL RADIOACTIVE WASTE, AND REACTOR-RELATED GREATER THAN CLASS C WASTE
72.48 Changes, tests, and experiments.

[b] 本付録 D の§4.3.1~4.3.8 のセクションタイトルが基準である。なお、基準(iii) (iv) (vii) (viii) には、NEI96-07 のガイダンスが適用される。

〈quality of design process〉、及び(3)ソフトウェア／ハードウェアの運転経験〈operating experience〉に関わるファクターの定性評価から得られる。

- 定性評価は、DIC 改造に付随するソフトウェア CCF による故障発生の可能性を判定するためのファクターや論理根拠〈rationale〉を記録するために使われる。
- 故障の発生可能性を判定するには、上記のファクターを全て考慮する必要がある。例えば、あるファクターが他のファクターの弱点を相殺する場合があるから。
- なお、定性評価は、原子炉保護系統(RPS)や工学的安全施設作動系統(ESFAS)の DIC 更新、あるいは、それらの系統の内部ロジック回路(競売回路〈voting logic〉、バイステーブル入力、及び信号処理等)の改造／更新には適用すべきではない。

3.16. 十分に低い〈Sufficiently Low〉

定義

- 「十分に低い」とは、更新最終安全解析書(UFSAR)で考慮している故障(単一故障など)の発生可能性より非常に低く〈much lower〉、UFSAR では考慮していない他の CCF(設計欠陥、保守エラー、及び較正エラー等)と同等〈comparable〉であること。

解説

- 「十分に低い」のしきい値は、想定可能事象〈credible event〉と非想定可能事象〈not credible〉を区別するしきい値と異なる。想定可能のしきい値は、UFSAR で想定している機能不良発生と同程度〈as likely as〉であり、非常に低い〈much lower than〉とは異なる。

4. 実施ガイダンス

4.1. 適用性

追加のガイダンスなし。

4.2. スクリーニング[a]

注意:本ガイダンスは、NEI96-07 の§4.2 に記載されている一般的なスクリーニングガイダンスを補うものである。つまり、デジタル改造に対しては、付録 D も NEI96-07 も適用される。

序論

- 変更〈proposed activity[b]〉の影響〈impact〉を判定する上でベースとなるのは、UFSAR に

[a] 変更の結果、改悪となる可能性の有無でふるい分けること。改悪可能性あり(スクリーニングイン)の場合は、次のステップの定性評価が必要となる。

[b] 「Activity」は、10CFR50.59 の「change, test, or experiment」を総称したもの。ここでは、以降「変更」と呼ぶ。

記載されている設計機能[a]〈design functions〉に対する影響である。付録 D は、以下の 2 項目のデジタルに特化したガイダンスを追加している。

デジタルからデジタルへの更新と同等性

- デジタルからデジタルへの変更は、必ずしも同等ではない。応答時間や故障モード等が異なる場合があるため。こうした非同等デジタルーデジタル更新に対しては、本付録 D を適用するべきである。

ヒューマンーシステム・インターフェイス（HSI）

- 他と同様、人間工学（HFE）によって変更の影響と結果は評価される。10CFR50.59 評価においても、変更前と後の影響と結果を比較する。

4.2.1. UFSAR に記載された施設〈facility〉又は手順〈procedures〉に対する変更か？

序論

- 以下のようなデジタル改造は、デフォルトで改悪〈adverse〉となるわけではない。
  - ソフトウェアあるいはデジタル機器の導入
  - ソフトウェア／デジタル機器の異なるソフトウェア／デジタル機器への更新
  - アナログ機器に代わるソフトウェアを使用した演算処理あるいは制御信号を発生させるデジタルプロセッサの使用
  - ハードワイヤード機器（押しボタン、スイッチなど）からタッチスクリーンへの更新
- デジタル改造による影響を記録するため、工学／技術情報を図書化すべきである。この情報が、「改悪か非改悪か〈adverse or not adverse〉」の結論付けに使われる。

デジタル改造のスコープ

- 一般に、デジタル改造は次の 3 領域からなる。（1）ソフトウェア関連、（2）ハードウェア関連、（3）HSI 関連。
- NEI96-07 § 4.2.1.1 は、「SSC 設計機能」もしくは「設計機能の動作／制御方法」に関する変更に対するガイダンスである。§ 4.2.1.2 は、「SSC 設計機能の動作／制御」（手順、運転員操作、応答時間など）に関する。
- 上記（1）と（2）は、SSC、SSC の設計機能、設計機能の動作／制御方法に関わることか

[a] 設計機能とは、1）UFSAR に記載された設計基準機能〈design bases functions〉と、2）設計基準機能をサポートしたり影響したりする UFSAR に記載されたその他の SSC の機能のこと。設計基準機能とは、(1) 規制や許認可条件や技術仕様で要求されたり、適合要求されたりする SSC の機能、または、(2) NRC 要求を満足するために安全解析で担保された機能。

ら、「施設」スクリーニングの中で評価される。(3)は、動作／制御に関わることから、「手順」スクリーニングである。

4.2.1.1. 施設スクリーニング

スコープ

- 潜在的な悪影響の有無を判定するため、下記の観点でスクリーニングする。
  - ソフトウェアあるいはデジタル機器を使用
  - コンポーネント／システムと機能の組合せ、または複数の機能の組合せ

ソフトウェアあるいはデジタル機器を使用

- ソフトウェアの導入によって、それを使った SSC 故障発生の可能性が潜在的に増加し、改悪影響がある可能性があるが、だからと言って、このデジタル改造が自動的にスクリーニングインされる(定性評価が必要)とは限らない。
- 多重の安全系統の場合、こうした故障発生の可能性の増加は、多重化した系統の共通故障発生の可能性の増加とみなされるので、ほとんどのデジタル改造が改悪である。
- しかし、こうしたデジタル改造(比較的簡単なもの)の工学／技術情報に、ソフトウェア CCF を防ぐ設計属性が含まれている場合がある。このようなデジタル改造は、改悪ではない。
- 「非改悪」という結論を導くためには、以下のような検討項目がある。
  - デジタル改造の物理的仕様
    - 変更のスコープが限定的(例:アナログ伝送器をデジタルに更新)
    - 比較的簡単なデジタル・アーキテクチャの使用(例:1 入力信号を得るためのシンプルプロセス、1 出力の設定、簡単な診断を行うもの)
    - 限定された機能(例:監視パラメータ用の信号駆動に使われる伝送器)
    - 総合試験可能(100%組合せ試験である必要はない)
  - 工学評価アセスメント
    - 用いられている設計プロセスの品質
    - デジタル機器の単一故障が、既存のアナログ機器の故障に包絡される(例:新たな故障モードをもたらす機器間のデジタル通信がない。)
    - 広範囲に及ぶ適用実績
- SSC の 2 つ以上のチャンネル、トレイン、回路で、異なるソフトウェアを用いていれば、非改悪である。ソフトウェア導入によって、新たな機能不良をもたらすメカニズムがないため。

- 潜在的に改悪をもたらすと考えられる例は、以下のものである。どちらも、スクリーニングの結論を出すためには、その条件下での設計機能への影響（改悪／非改悪）を評価する必要がある。
  - 不感帯〈dead band〉の追加もしくは削除
  - 即時計測を時間平均計測で更新（または、その逆）

事例

事例 4-1	比較的簡単なデジタル改造において設計機能への改悪影響がない
変更	多重の ESFAS チャンネルによって監視されているパラメータを駆動するために、伝送器が使用されている。このアナログ伝送器をマイクロプロセッサ内蔵のデジタル伝送器で置き換える。変更は限定的で、既存の 4-20 mA 計装回路は維持され、伝送器以外の変更はない。デジタル伝送器は、監視パラメータを駆動するために使用され、ESFAS の設計機能に関する機能は限定的である。
スクリーニング結果	このデジタル伝送器は比較的簡単なデジタル・アーキテクチャを用いていて、その故障はアナログ機器の故障に含まれる。工学／技術情報（設計プロセスの品質、ハードウェアとソフトウェアの運転経験）に基づくと、このデジタル機器は従前のものと同等の信頼性〈reliable〉がある。さらに、機器の単純さから、総合試験済みである。多数の動作実績からも高い信頼性を示している。よって、本デジタル改造は、改悪はない。

事例 4-2	ソフトウェアとデジタル機器の使用に関連する設計機能への改悪影響がある
変更	非安全系の 2 台の主給水ポンプ（MFWP）は、各々流量制御弁を具備している。各々にアナログ制御系があるが、物理的にも機能的にも同じものである。アナログ制御系は、それぞれデジタル制御系で置き換えられる。各デジタル制御系のハードウェア・プラットフォームは同じ供給元であり、ソフトウェアは全く同じである。新たなコンポーネント／システムと機能の組合せ、または複数の機能の組合せはない。
スクリーニング結果	このデジタル改造は比較的簡単ではない。両方のデジタル制御系に全く同じソフトウェアが使われているので、以前は考慮しなくてよかったソフトウェア CCF を考慮しなくてはいけないので、主給水制御系の設計機能に改悪影響がある。

事例 4-3	コンポーネントと機能の組み合わせにより設計機能に (1)改悪影響がないと(2)改悪影響がある
変更	非安全系の 2 台の MFWP は、各々流量制御弁を具備している。各々のアナログ制御系は、物理的にも機能的にも同じものであるが、多くのサブコンポーネントから成る。(1)各制御系において、全てのアナログ・サブコンポーネントが単一のデジタル機器(コンポーネントも機能も統合)で置き換わる。各デジタル制御系は、個別〈discrete〉で相互接続はない。(2)デジタル制御系は一つで、コンポーネントと機能を合体している。
スクリーニング結果	(1)2 つの給水制御系が維持されているので、主給水制御系の設計機能への改悪影響はない。(2)一つのデジタル機器の喪失が複数の設計機能の不作動をもたらし得るので、主給水制御系の設計機能への改悪影響がある。

事例 4-4	コンポーネントと機能の組み合わせにより設計機能に改悪影響がない
変更	緊急対策室用クーラーがある部屋の温度監視制御器は、空調ダンパーの入力信号を出している。両アナログ制御器が単一のデジタル制御器で置き換わることになっている。機能(温度監視制御とダンパー制御)に変更はない。
スクリーニング結果	スクリーニング:デジタル機器の故障は複数の故障をもたらすが、室温調整機能の喪失しかもたらさない。それは現行設計と同様であり、設計機能への改悪影響はない。

事例 4-5	コンポーネントと機能の組み合わせにより設計機能に改悪影響がある
変更	非安全系のアナログ蒸気バイパス制御系(SBCS)と非安全系の主タービン蒸気入口弁アナログ制御系が、単一のデジタル制御系で置き換わる。
スクリーニング結果	新しい単一デジタル機器の故障は複数の設計機能の喪失をもたらすので、このデジタル改造は改悪影響がある。

4.2.1.2. 手順スクリーニング

スコープ

- デジタル改造が HSI 要素を含まない場合(単体アナログリレーの単純デジタルリレーへの更新等)は、本セクションは適用されない。
- このスクリーニングの焦点は、使用者と機器のインターフェイスの改造による潜在的な改悪／非改悪を評価すること。なお、使用者とは、制御室運転員、他のプラント運転員、保守要員、技術者、技師などである。

人間工学評価

- HSI の基本要素は、次の 3 つ。①表示器、②制御器、③ユーザーインターフェイス(UI)相互作用と管理(入力を与え、出力を受け取り、情報のアクセスと制御に関係するタスクを管理する手段)

- 原子力発電所では、特に、以下の 4 つのタスクがある。
  - 監視と検知（環境から情報を引き出し、何か変わった場合に認識する）
  - 事態評価（状態を評価する）
  - 対応計画（事態を打開するための措置を決める）
  - 対応実施（措置を実施する）

表 1　HSI 基本要素ごとの HSI 改造例

要素	典型的改造	説明、例
表示器	パラメータ数	例：複数パラメータを合体して単一にする。システムのパフォーマンスに関する情報を追加する。
	パラメータタイプ	例：従前は表示されていた情報を取り除く。その逆。
	表示情報	情報の視覚表示を変更する。
	情報構成	例：フローパスごとの表示をチャンネル／トレインごとの表示に変更する。
制御器	入力方法	入力機器のタイプや機能を変更する。 例：押しボタンをタッチスクリーンに変更する。
	フィードバック	操作に応じたフィードバック形式を変更する。 例：触覚フィードバックから聴覚へ変更する。
UI 相互作用と管理	シークエンス	決定や措置のステップ数やタイプを変更する。 例：1 ステップで操作できるアナログ制御器を UI 上で呼び出して、操作するタイプのデジタル制御器に変更する。
	情報／データ収集	情報／データの読み取り方法を変更する。 例：連続表示のアナログメータから多目的表示デジタルパネルに変更する。
	機能配分	機能の手動起動から自動起動に変更する。 例：手動ポンプ起動から自動起動に変更する。

- HSI 改造が設計機能にもたらす潜在的改悪影響を判定するためには、2 ステップ HFE 評価が必要である。
  - ステップ 1：変更により潜在的に影響される主要タスクを特定する。
  - ステップ 2：それら主要タスクごとに、変更が個人のタスク遂行パフォーマンスに悪影響を与えるかどうかを評価する。設計機能に悪影響もたらす個人のタスク遂行パフォーマンスへの影響例は以下の通り。
    - 操作ミスの可能性の増加

- 状態評価の困難性の増加
- 措置実施における困難性の増加
- 反応時間の増加
- 新たな潜在的故障モードの発生

ガイダンス

- 上記の 2 ステップ HFE 評価後に、通常のスクリーニングを行う。

HSI 事例

事例 4-6	UFSAR に記載の設計機能に改悪影響のない改造の評価
変更	現在、流量制御弁を 1%ずつ開くためにスイッチノブを時計回りに回し、閉じるときは反時計回りに回す。このノブを 2 つの矢印が表示されるタッチスクリーンで置き換える。UP をタップすれば、1%ずつ流量制御弁が開き、DOWN をタップすれば、1%ずつ閉まる。
スクリーニング結果	UFSAR に記載された設計機能の作動、制御方法を維持しつつ、主制御室にある手動制御器を使って、流量制御弁の開け閉めが可能であることに対して影響がないので、この改造は改悪影響がない。

事例 4-7	設計機能に改悪影響のない HSI に関わるデジタル改造
変更	現在は、多重化システムのチャンネル／トレインの情報、状態が制御室に表示されている。チャンネル／トレインごとに、いくつものアナログ計装が、システム状態を示しており、アナログ表示は運転員が見やすいように流路ごとに並べられている。現在の HSI は、多重のハードワイヤードスイッチ、表示灯とアナログメータで構成されている。新しい HSI では、情報や状態を 2 つのフラットパネル（タッチスクリーン）に集約する。表示される情報は変わらない。各フラットパネルは、1 スクリーンのみで一つのトレインの情報しか表示されない。表示配列は、アナログのものを再現している。新しい HSI では、運転員はフラットパネルで適切な画面選択、制御されるコンポーネントの画面、制御操作画面を順次選んでから、操作実施しないといけない。
スクリーニング結果	新しい HSI で表示される情報と構成は既存のものと同じであることから、設計機能への悪影響はない。また、タッチスクリーンを用いた操作により設計機能も動作させられる。HFE 評価により、運転員は適宜、現状とそん色なく操作できることが示されているので、設計機能を動作させる点でも悪影響はない。

事例 4-8	設計機能に改悪影響のある HSI に関わるデジタル改造
変更	事例 4-7 に加えて、各フラットパネル表示のパラメータや構成は、運転員の好みに応じてカスタマイズ可能。さらに、フラットパネルには、多数の表示オプションも用意されている。
スクリーニング結果	表示がカスタマイズ可能であるため、逆に、緊急状態表示が失われる可能性があり、この変更は、設計機能への改悪影響がある。ただし、HFE 評価により、運転員は適宜、現状とそん色なく操作できることが示されているので、設計機能を動作させる点では悪影響はない。

4.2.1.3. UFSAR に記載されている評価方法に対する変更のスクリーニング

- UFSAR に記載されている評価方法とは、解析や数値計算モデルのことである。NEI96-07 § 4.2.1.3 が適用される。

4.2.2. UFSAR に記載されてない検査〈Test〉や試験〈Experiment〉を実施するのか？

- デジタル改造に伴い必要となる検査や試験には、NEI96-07 § 4.2.が適用される。

4.3. 評価

注意：本ガイダンスは、NEI96-07 の § 4.3 に記載されている一般的な評価ガイダンスを補うものである。つまり、デジタル改造に対しては、付録 D も NEI96-07 も適用される。

4.3.1. 変更により事故の発生頻度が有意に増加するか？

序論

- 事故とは、NEI96-07 § 3.2 に、想定される運転過渡〈operational transients または Anticipated Operational Occurrences〉と設計基準事故〈design basis accidents または Postulated Accidents〉と定義されている。
- デジタル更新〈digital upgrades〉に対する評価基準の重要項目は、事故につながる起因事象の頻度が増加するかどうかである。
- 全ての起因事象は、次のどちらかに分類される：①機器関連〈equipment-related〉、②人的〈personnel-related〉。デジタル改造の影響評価では、①も②も考慮しなくてはならない。
- ①には、デジタル特有のものと特有でないものがある。前者の例は、ソフトウェア CCF がもたらす事故発生頻度への影響。後者の例は、デジタルシステムの据え付け先環境との相性がもたらす事故発生頻度への影響。ただし、デジタル特有でないものに対しては、NEI96-07 § 4.3.1 が適用される。
- 事故発生頻度は事故の起因となる機器の故障可能性と直接関連することから、改造機器の故障可能性が増加すれば、事故発生頻度も増加することになる。（例：蒸気発生器（SG）

の伝熱管の故障可能性が増加すれば、SG 伝熱管破断事故の頻度も増加する。）

ガイダンス

定性評価結果

- 定性評価結果が「十分に低い」場合は、UFSAR で従前に評価された事故発生頻度は、有意に増加しない。

無視できる〈negligible〉

- 事故発生頻度の変化が小さすぎて、合理的に頻度が変化するという結論を導き出せないとき（明らかな頻度の増加傾向がない場合）。

認識可能〈discernable〉

- 明らかな頻度の増加傾向がある場合、ソフトウェア CCF の可能性は、十分に小さいとは言えない。この場合は、工学／技術情報を用いて事故発生頻度の大きさを定性評価しなければならない。
- 定性評価の一部として、相互依存性〈interdependence〉を考慮すること。例えば、ソフトウェア CCF 発生可能性への負の影響は、対象のデジタルシステムそのものやその設計仕様がもたらす正の影響で相殺されるかもしれない。
- 工学／技術情報に基づく定性評価の結論を得るためには、変更は、全ての適用可能な NRC 要求ならびに、事業者がコミットした設計、材料、建設標準も満足していなくてはならない。適用可能な要求や標準には、当該デジタル改造の開発や図書化に使用されるものも含まれる。

事例[a]

事例 4-9	**事故発生頻度に有意な増加がない**
変更	非安全系の 2 台の MFWP は、各々流量制御弁を具備している。各々にアナログ制御系があるが、物理的にも機能的にも同じものである。アナログ制御系は、それぞれデジタル制御系で置き換えられる。各デジタル制御系のハードウェア・プラットフォームは同じ供給元であり、ソフトウェアは全く同じである。
結論	改造した SSC によりもたらされる故障発生の可能性が十分に低いので、UFSAR で従前に評価した事故の発生頻度に有意な増加はない。

[a] 同じ変更事例でも、工学／技術情報（具体的記載はない）によっては結論が異なることを示す目的で、2事例を挙げていると考えられる。

事例 4-10	事故発生頻度に有意な増加がある
変更	事例 4-9 と同じ。
結論	この変更に適用された設計プロセスや運転経験情報は、設計属性の弱点を補うに不十分。改造された SSC によってもたらされる故障可能性が十分に低くなく、設計属性の弱点を補うことも不可能であるので、UFSAR で従前に評価した事故の発生頻度に有意な増加がある。

4.3.2. 変更により安全上重要な SSC の機能不良発生可能性が有意に増加するか？

序論

- デジタル改造に対する評価基準の重要項目は、デジタル機器により、その機器の機能不良につながる起因事象の発生可能性が増加するかどうかである。
- 全ての起因事象は、次のどちらかに分類される：①機器関連〈equipment-related〉、②人的〈personnel-related〉。デジタル改造の影響評価では、①も②も考慮しなくてはならない。
- ①には、デジタル特有のものと特有でないものがある。前者の例は、ソフトウェア CCF がもたらす機能不良発生可能性への影響。後者の例は、デジタルシステムの据え付け先環境との相性がもたらす機能不良発生可能性への影響。ただし、デジタル特有でないものに対しては、NEI96-07 § 4.3.2 が適用される。
- 安全上重要な SSC の機能不良発生可能性は、意図した設計機能を果たす SSC の故障の起因となる機器の故障可能性と直接関連することから、改造機器の故障可能性が増加すれば、機能不良発生可能性も増加することになる（例：補助給水（AFW）ポンプの故障可能性の増加は、AFW ポンプや AFW 系の機能不良発生可能性を増加させる。）。
- ネットワーク、他のシステムの設計機能との合体、チャンネル／システム／区分間の相互接続性及び共有リソースに関わるデジタル改造では、UFSAR に記載された設計機能における多重性、多様性、分離、独立性を減少させることがないか、注意深くレビューすることが重要である。
- デジタル改造により異なる機能を合体させると、異なるシステムの設計機能を合体することになるが、同じデジタル機器の中で直接合体する場合と、共有リソースを通じて間接的に合体する場合がある。デジタル改造で共有リソース（例：双方向通信、電源、制御器、多機能表示制御ステーション）が用いられたら、UFSAR に記載された設計機能における多重性、多様性、分離、独立性を減少させる場合がある。

ガイダンス

- 設計機能における多重性、多様性、分離、独立性を減少させる変更は、機能不良の発生可能性を有意に増加させるので、事前の NRC 承認が必要となる。しかし、事業者は、UFSAR で担保されているレベルまでなら、過剰な多重性、多様性、分離、独立性を減じてもよい。
- デジタル改造によって、従前は起こらないとされていた CCF が、起こり得る事象となる場合もある。

事例

事例 4-11	機能不良発生可能性に影響がある事例a
変更	2 台の安全系格納容器冷却器は、各々アナログ制御系を持っているが、それらは物理的にも機能的にも同一である。各アナログ制御器は、それぞれデジタル制御器で置き換えられる。両デジタル制御器のハードウェア・プラットフォームは同じ供給者からのものであり、使われているソフトウェアは全く同じである。
結論	安全関連冷却器制御系は、UFSAR で特定されている起因事象ではないが、デジタル制御器によって新たな共通機能不良原因がもたらされた。よって、デジタル改造は、機能不良発生可能性に影響する。

定性評価結果

- 定性評価結果が「十分に低い」場合は、UFSAR で従前に評価された安全上重要な SSC の機能不良発生可能性は、有意に増加しない。

無視できる〈negligible〉

- 機能不良発生可能性の変化が小さすぎて、合理的に可能性が変化するという結論を導き出せないとき（明らかな発生可能性の増加傾向がない場合）。

認識可能〈discernable〉

- 明らかな発生可能性の増加傾向がある場合、ソフトウェア CCF の可能性は、十分に小さいとは言えない。この場合は、工学／技術情報を用いて機能不良発生可能性の大きさを定性評価しなければならない。
- 定性評価の一部として、相互依存性〈interdependence〉を考慮すること。例えば、ソフトウェア CCF 発生可能性への負の影響は、対象のデジタルシステムそのものやその設計仕様がもたらす正の影響で相殺されるかもしれない。

[a] アナログ制御器が 2 台とも故障（CCF）する起因事象はないと評価されていたが、デジタル制御器では CCF が起こり得ると評価が変わった事例である。

- 工学／技術情報に基づく定性評価の結論を得るためには、変更は、全ての適用可能な NRC 要求ならびに、事業者がコミットした設計、材料、建設標準も満足していなくてはならない。適用可能な要求や標準には、当該デジタル改造の開発や図書化に使用されるものも含まれる。

事例

事例	機能不良発生可能性に有意な増加がない
変更 4-12	非安全系の 2 台の MFWP は、各々流量制御弁を具備している。各々にアナログ制御系があるが、物理的にも機能的にも同じものである。アナログ制御系は、それぞれデジタル制御系で置き換えられる。各デジタル制御系のハードウェア・プラットフォームは同じ供給元であり、ソフトウェアは全く同じである。
結論	改造した SSC によりもたらされる故障発生の可能性が十分に低いので、UFSAR で従前に評価した事故の発生頻度に有意な増加はない。

事例 4-13	機能不良発生可能性に有意な増加がある
変更	安全系の 2 台の主制御室冷却器は、各々のアナログ制御系は物理的にも機能的にも同じものである。アナログ制御系は、それぞれデジタル制御系で置き換えられる。各デジタル制御系のハードウェア・プラットフォームは同じ供給元であり、ソフトウェアは全く同じである。安全注入系ポンプの起動／運転のためのロジック系と制御系は、その主制御室境界内にあり、それらの要求環境は、主制御室冷却系統（前記冷却器含む）の許容限度内で維持されている。
結論	単一故障基準を満足する故障なので、デジタル改造による安全注入ポンプの機能不良発生可能性に有意な増加はない。しかし、改造された SSC による故障発生可能性が十分に低いとは判定されないし、設計属性における弱点を補うこともできないので、UFSAR 従前に評価された機能不良発生可能性に有意な増加がある。

4.3.3. 変更により事故影響に有意な増加があるか？

- NEI96-07 § 4.3.3 が適用される。

4.3.4. 変更により機能不良の影響に有意な増加があるか？

- NEI96-07 § 4.3.4 が適用される。

4.3.5. 変更により異なるタイプの事故を発生させる可能性はあるか？

ガイダンス

- NEI96-07 § 4.3.5 によれば、この評価には 2 つの検討項目がある：起こりやすさ〈as likely to happen as〉と異なるタイプの事故〈accident of a different type〉。

「起こりやすさ」の判断

- 定性評価結果が十分に低い場合は、変更は、UFSAR で評価した異なるタイプの事故を引

き起こす可能性のある故障と同等の起こりやすさの故障をもたらさない。

「異なるタイプの事故」の判断

- 定性評価結果が十分に低くない場合は、異なるタイプの事故を以下のように判定しなくてはならない。
  - 既存の事故解析の改訂〈revision〉が行われることになるなら、変更は異なるタイプの事故を発生させる可能性はない。
  - 新たな〈new〉事故解析が必要になるなら、変更は異なるタイプの事故を発生させる可能性がある。

事例

事例 4-14	異なるタイプの事故を発生させる可能性はない
変更	非安全系の 2 台の MFWP は、各々流量制御弁を具備している。各々にアナログ制御系があるが、物理的にも機能的にも同じものである。アナログ制御系は、それぞれデジタル制御系で置き換えられる。各デジタル制御系のハードウェア・プラットフォームは同じ供給元であり、ソフトウェアは全く同じである。
結論	改造した SSC によりもたらされる故障発生の可能性が十分に低いので、UFSAR で評価した異なるタイプの事故を引き起こす可能性のある故障と同等の起こりやすさの故障をもたらさない。

事例 4-15	異なるタイプの事故を発生させる可能性がある
変更	非安全系の 2 台のアナログ給水制御系と非安全系の主タービン蒸気入口弁アナログ制御系が、単一のデジタル制御系に合体される。
結論	既往の安全解析では、単一のデジタル制御系の機能不良によりもたらされ得る次の 4 事象を考慮していない：①給水喪失とタービントリップの組み合わせ、②給水喪失と過剰蒸気デマンドの組み合わせ、③過剰給水とタービントリップの組み合わせ、④過剰給水と過剰蒸気デマンドの組み合わせ。これらの新たな安全解析が必要となるので、異なるタイプの事故の発生する可能性がある。

4.3.6. 変更により異なる結果をもたらす安全上重要な SSC の機能不良が発生する可能性はあるか？

ガイダンス

- NEI96-07 § 4.3.6 によれば、この評価には 2 つの検討項目がある：起こりやすさ〈as likely to happen as〉と機能不良への影響〈impact on the malfunction〉。

「起こりやすさ」の判断

- 定性評価結果が十分に低い場合は、変更は、UFSAR で評価したものと異なる結果をもたらす安全上重要な SSC の機能不良が発生する可能性はない。

事例

事例 4-16	異なる結果をもたらす機能不良が発生する可能性はない
変更	多様な系統で用いられている多くのアナログ伝送器がデジタルに置き換わる。これらの伝送器の機能は多様であり、安全解析上担保されている自動起動装置の制御も含まれる。
結論	改造した SSC によりもたらされる故障発生の可能性が十分に低いので、安全上重要な SSC の機能不良が UFSAR で評価したものと異なる結果をもたらす可能性はない。

「機能不良への影響」の判断

- 定性評価結果が十分に低くない場合は、安全上重要な SSC の機能不良結果への影響（結果が異なるかどうか）を判断しなくてはならない。一般的な評価ステップ（6 ステップ）は以下の通り。

ステップ 1 変更に直接的または間接的に関連する機能を特定する。適切な SSC のスコープや機能を特定する際に、以下の 3 つのガイダンスがある。

1. UFSAR に直接記載されたレベルに限定することなく、SSC が関わる機能を考慮すること。
2. 変更が UFSAR に直接記載されていないサブコンポーネント等に関わる場合は、変更によるそのサブコンポーネントを含んでいるシステムへの影響を考慮すること。
3. 変更が UFSAR に記載されていないサブコンポーネント等に関わる場合は、変更によるそのサブコンポーネントがサポートするシステムへの影響を考慮すること。

影響評価では以下に示す設計機能の要素を考慮すること。

- 設計機能の意味に暗に含まれるのは、意図した機能の発揮のために要求される条件で、例えば、機器応答時間、プロセス[a]条件、機器性能認証、単一故障。
- 安全関連または非安全関連 SSC によって発揮される設計機能で、もし、その機能が発揮されなければ、プラント過渡や事故の起因となる可能性があるもの。

[a] 水、蒸気等の作動流体

ステップ 2 ステップ 1 で特定された機能のうち、設計機能もしくは設計基準機能を特定する。

まず、ステップ 1 で特定された機能が、非設計機能か設計機能か分類する。

非設計機能の場合、異なる結果をもたたらす安全上重要な SSC の機能不良の発生可能性はない。非設計機能は、安全上重要な SSC の機能と無関係だから。

設計機能の場合、各々以下により分類する。

1） 設計基準機能:

1a. 規制や許認可条件や技術仕様で要求されたり、適合要求されたりする SSC の機能、

1b. NRC 要求を満足するために安全解析で担保された機能。

2) 設計機能:

2a. 1a.をサポートまたは 1a.に影響する機能、

2b. 1b.をサポートまたは 1b.に影響する機能。

3) 設計基準機能に関係しないが、それが機能しないと、プラントが耐えることが要求されている過渡／事故の起因となるもの。

上記 1a.と 1b.を区別する一つの方法は、要求（規制、許認可条件、技術仕様書）、または、関連する GDC、特に施設ごとの最重要設計基準〈Principle Design Criteria: PDC〉を特定すること。例えば、設計機能が GDC の要求に直接関わっていれば、1a.、サポートや影響のレベルだったら、1b。

ただし、機能は安全解析で取り上げられている SSC のものに限定しないこと。例えば、高圧安全注入系の弁制御系の変更の場合、安全解析で高圧安全注入系を担保しているが、弁自身は取り上げていない。

SSC の分類において、安全関連か非安全関連かは、設計機能を特定する上で決め手とならない。非安全関連でも、安全解析上で担保しているものがあるため。

もし、設計機能に関わるものがない場合は、ステップ 5 に進む。（注:より厳しい事故の起因可能性はステップ 5 で議論されるが、このような設計は、上記 3)に分類されるべきである。）

ステップ 3 新たな故障モード影響解析（FMEA）の必要性の有無を判断する。

関連する設計基準機能への影響が明確で、新たな FMEA が不要な場合は、ステップ 4 に進む。

新たな FMEA を行うにあたって、設計機能への潜在的な有害な影響を緩和する SSC の設計や運転（手順）オプションがあるかどうか特定するために、既存／相互依存に関連する変更手順の遵守と既存の機器の使用を仮定する。

既存／相互依存に関連する変更とは、例えば、新しいデジタル機器とその制御操作を反映させるために、既存の手順に変更を加えること。制御系の再起動操作オプションといった新しい機能仕様が含まれる。

ステップ 4 各設計基準機能が継続して働くか／満足するか判断する。

もし、全ての設計基準機能が継続して働き、満足され、他に関連する設計機能がなければ、変更による、異なる結果をもたらす安全上重要な SSC の機能不良発生可能性はない。機能不良が発生しないならば、異なる結果ももたらし得ない。

設計基準機能が継続して働かず、満足しないならば、または、他の設計機能が関連するならば、ステップ 5 に進む。

ステップ 5 UFSAR で従前に評価した安全上重要な SSC の全ての機能不良を特定する。

ステップ 2 で、1a.や 2a.と分類された設計機能と設計基準機能に関連する UFASR の既往評価を全て特定する。さらに、従前に 10CFR50.59 適合評価が行われていれば、その結論を再検討する。設計機能に関連した他の要求があるかもしれないため（例：規制の変更、技術仕様書の変更、規制指示、運転許可の変更）。

ステップ 2 で、1b.や 2b.と分類された設計機能と設計基準機能に関連して、設計基準機能に直接／間接的に依存している全ての安全解析を特定することによって、UFSAR で従前に評価された安全上重要な SSC の機能不良を全て特定する。

事故または過渡の起因に影響を与える可能性のあるその他の設計機能に関係するすべての安全解析を特定する。このような設計機能があれば、ステップ 2 の 2b.か 3 に分類されるべきである。

ステップ 6 特定された各機能不良に対して、予見される結果と既往の評価結果と比較する。

ステップ 2 で 1a.または 2a.と分類された設計機能について、既往の UFSAR 評価結果〈the results of all pre-existing UFSAR evaluations〉と変更がもたらす改訂必要性〈potential for any revision〉について評価する〈assess〉。変更がもたらす

改訂評価結果が、「規制、許認可条件、規制指示、技術仕様書」と整合していない場合は、変更により、異なる結果をもたらす安全上重要な SSC の機能不良発生の可能性があることになる。

その他の分類や設計機能の組合せに対して、もし、基本的な仮定が無効になる場合（例：単一故障基準が守られない）、既往安全解析がもはや紐づけされない場合（例：許容基準を満足しない）、変更により、異なる結果をもたらす安全上重要な SSC の機能不良発生の可能性がある。許容基準を満足し、基本仮定が有効な場合は、例え機能不良により UFSAR に記載された入力パラメータが変わることになっても、異なる結果は生じない。

機能不良発生評価の結果が引き続き紐づけされるかどうかを特定するためには、起因条件の重大度への影響と関連する安全解析で仮定された起因条件への影響を含めること。特に、機能しないと、事故や過渡をもたらすような設計機能を考慮すること（ステップ 2 の分類 3）。

事例

事例 4-17	**異なる結果をもたらす機能不良が発生する可能性はない**
変更	給水制御系の一つをアナログからデジタルに更新する。現在、給水流量制御弁 4 台の 1 台のみが、アナログ制御系の故障が起こればフェイルクローズする。更新後、デジタル制御系のソフトウェア CCF により、4 台とも同時にフェイルクローズする可能性がある。
結論	ソフトウェア CCF 発生可能性は十分に低いとは判定されないが、給水喪失事故解析で仮定された起因重大度（4 台故障）、故障モード（弁閉止）と給水流量喪失メカニズム（制御信号喪失）は変わらない。さらに、既往安全解析の事象タイプ（圧力上昇）も全ての許容基準〈acceptance criteria〉（最大許容 RCS ピーク圧力と最大許容 2 次系圧力）も満足したままである。よって、この変更によって、異なる結果をもたらす安全上重要な SSC の機能不良が発生する可能性はない。

事例 4-18	**異なる結果をもたらす機能不良が発生する可能性はない**
変更	給水制御系の一つをアナログからデジタルに更新する。現在、給水流量制御弁 4 台の 1 台のみが、過剰給水事象の発生によりフェイルオープンする。更新後、デジタル制御系のソフトウェア CCF により、4 台とも同時にフェイルオープンする可能性がある。
結論	ソフトウェア CCF 発生可能性は十分に低いとは判定されないし、起因故障の重大度も増加したが、最小 DNBR の比較により、関連する許容基準を満足しているので、安全解析は有効である。よって、この変更によって、異なる結果をもたらす安全上重要な SSC の機能不良が発生する可能性はない。

事例 4-19	異なる結果をもたらす機能不良が発生する可能性はない
変更	多様な場所のエリア放射線モニター（高線量用）の完全更新が提案されている。老朽化したアナログ放射線モニターはデジタルに置き換わる。新しいモニターのハードウェア・プラットフォームは同じ供給者のもので、用いられているソフトウェアはすべてのモニターで同じである。
結論	ソフトウェア CCF 発生可能性は十分に低いとは判定されないが、放射線モニターの更新評価結果は GDC64[a]を満足したままであり、UFSAR で従前に評価されたものと異なる結果をもたらす安全上重要な SSC の機能不良が発生する可能性はない。さらに、放射線モニターの設計基準機能を直接／間接的に担保としている安全解析はないし、放射線モニターから／への応答を含んだ安全解析もない。よって、この変更によって、異なる結果をもたらす安全上重要な SSC の機能不良が発生する可能性はない。

事例 4-20	異なる結果をもたらす機能不良が発生する可能性はない
変更	主制御室換気系統（MCRVS）を冷やす 2 台の冷却器が更新される。MCRVS は MCR と隣接するリレー室も冷却する。リレー室には、複数の計装ラックがあり、RPS と ESFAS の両方を制御している。更新によって、各々の冷却器のアナログ制御系がデジタルに置き換わる。運転機能（自動／手動、起動／停止、設定、警報など）に変わりはない。2 台のデジタル制御系のハードウェア・プラットフォームは同じ供給業元であり、ソフトウェアはまったく同じものである。
結論	ソフトウェア CCF 発生可能性は十分に低いとは判定されないが、設計基準機能は維持され、安全解析にも影響がない。よって、この変更によって、異なる結果をもたらす安全上重要な SSC の機能不良が発生する可能性はない。

事例 4-21	異なる結果をもたらす機能不良が発生する可能性はない
変更	現在、非安全系の蒸気バイパス制御系（SBCS）と非安全系の加圧器制御系は、別々のアナログ制御系である。SBCS と加圧器制御系をアナログからデジタルに更新する。更新によって、これらは分散制御系（DCS）内の同じデジタル制御器に合体される。同じソフトウェアが、蒸気バイパス機能と加圧器圧力制御機能を制御する。
結論	ソフトウェア CCF 発生可能性は十分に低いとは判定されないが、主蒸気流量増大事故解析で仮定する起因重大度（4 弁影響）、故障モード（弁閉止）と蒸気流量増大メカニズム（制御信号エラー）は変わらない。事象タイプ（減圧）は変わらず、全ての許容基準（最大ピーク RCS 圧力、最大二次側圧力、最小 DNBR、最大ピーク線出力と線量影響）は満足することから、既往の安全解析は有効である。よって、この変更によって、異なる結果をもたらす安全上重要な SSC の機能不良が発生する可能性はない。

[a] 10CFR50 付録 A—General Design Criteria for Nuclear Power Plants
Criterion 64—Monitoring radioactivity releases. Means shall be provided for monitoring the reactor containment atmosphere, spaces containing components for recirculation of loss-of-coolant accident fluids, effluent discharge paths, and the plant environs for radioactivity that may be released from normal operations, including anticipated operational occurrences, and from postulated accidents.

事例 4-22	異なる結果をもたらす機能不良が発生する可能性がある
変更	アナログベースの RPS をデジタルベースに更新する。この更新により、AOO を検知し、原子炉トリップ信号を発信するすべてのソリッドステート基板が交換される。これらの基板を用いる多重チャンネルでは、単一故障基準は満足。
結論	ソフトウェア CCF 発生可能性は十分に低いとは判定されないし、単一故障基準に関する基本仮定が無効であり、既往の安全解析が有効でなくなった。よって、この変更によって、異なる結果をもたらす安全上重要な SSC の機能不良が発生する可能性がある。

事例 4-23	異なる結果をもたらす機能不良が発生する可能性がある
変更	両トレインの非常用ディーゼル発電機（EDG）のアナログ電圧調整器がデジタルに変更される。
結論	ソフトウェア CCF 発生可能性は十分に低いとは判定されないし、単一故障基準に関する仮定が無効、関連する許容基準を不満足、既往の安全解析も有効ではない。よって、この変更によって、異なる結果をもたらす安全上重要な SSC の機能不良が発生する可能性がある。

事例 4-24	異なる結果をもたらす機能不良が発生する可能性がある
変更	加圧器逃し弁（PORV）用の低温過加圧防護系を制御するためのアナログ圧力伝送器と関連回路をデジタル機器で更新する。
結論	ソフトウェア CCF 発生可能性は十分に低いとは判定されないし、関連する許容基準を満足しないので、PORV は作動しないし、既往の安全解析は有効ではない。よって、この変更によって、異なる結果をもたらす安全上重要な SSC の機能不良が発生する可能性がある。

4.3.7. 変更により FP 境界の設計基準限界を超過したり、改めたりするような結果をもたらすか？

- NEI96-07 § 4.3.7 が適用される。

4.3.8. 変更により設計基準を構築する際または安全解析を行う際に用いられた UFSAR に記載の評価手法からの逸脱をもたらすか？

- NEI96-07 § 4.3.8 が適用される。

参考図書

[1] NEI 96-07, Appendix D, Supplemental Guidance for Application of 10CFR50.59 to Digital Modifications, Revision 1, May 2020

[2] NEI 96-07, Revision 1, GUIDELINES FOR 10CFR50.59 IMPLEMENTATION, November 2000