参考 1

資料１－１

発電用原子炉施設におけるデジタル安全保護回路のソフトウェアに起因する共通要因故障対策について

令和元年９月１３日
原子力規制庁

本年の原子力規制委員会の重要課題（重点課題と比較すると個別性が強いが、規制上の重要度が高いもの）として、発電用原子炉施設におけるデジタル安全保護系の共通要因故障対策の規制への取り込みが挙げられている。[1]

１．現状と国内外の動向

（1）現状と国内動向

安全保護回路をデジタル化する場合には、アナログ式の場合にはなかった、ソフトウェア起因のCCF（ソフトウェアによって機能する電子計算機の不作動又は誤作動による、多重化された安全保護回路の同時機能喪失）を新たに考慮する必要がある。

この問題は古くから認識されており、現に事業者は、デジタル安全保護回路を設ける場合には、ソフトウェア処理の簡素化や可視化、自己診断機能の実装、ライフサイクルを通じた品質管理、検証及び妥当性確認（V＆V）の実施[2]といった現行基準の要求事項を満たすだけでなく、一部の安全保護機能を代替するハードワイヤード機構（以下「Hw機構」という。）を別途自主的に設けている。

Hw機構の設置が現行基準で求められていないのは、現行基準の要求するソフトウェアの品質確保策が的確に講じられることにより、ソフトウェア起因のCCFが発生する可能性は十分低く抑えられていると考えられるからである。[3]

なお、現行基準の下でSA対策の有効性評価を行う際には、安全保護回路がデジタル式であるかアナログ式であるかを問わず、何らかの理由により原子炉停止系統又は工学的安全施設が自動的に作動しない場合でも、自主設備であるHw機構を用いることなく重大事故等に対処できることを確認している。

ABWRのように当初設計からデジタル式であるものに加え、近年、従来はアナログ式であった安全保護回路をデジタル化して取り替える事例[4]が増えている。このような場合でも事業者は、現行基準の要求事項に加えて、信頼性向上の観点からHw機構を別途自主的に設けている。

しかしながら、安全保護回路に要求される安全保護機能のうち一部の機能のみをデジタル化する事例も見られ、当初設計からデジタル式であるものとは異なる様態でデジタル技術が適用されている場合がある。[5]

---

[1] 平成30年度第53回原子力規制委員会（平成31年1月16日）資料1
[2] 高浜1号機工事計画認可申請書添付書類（デジタル制御方式を使用する安全保護系等の適用に関する説明書）（平成28年5月　関西電力株式会社）
[3] 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（平成23年1月　原子力安全・保安院、独立行政法人原子力安全基盤機構）
[4] 玄海原子力発電所3号炉及び4号炉原子炉安全保護計装盤等の更新について（2019年5月　九州電力株式会社）
[5] 島根原子力発電所2号炉安全保護回路（平成31年2月　中国電力株式会社）

事業者は、自主設備であるHw機構を「合理的な範囲」で設計するとしている[6]が、実態として、そのHw機構がデジタル安全保護回路の安全保護機能をどの程度代替できているか、また、安全保護回路と比べてどの程度の設計グレードとなっているかについては明らかでない。

（2）海外動向

海外においても同様に、デジタル安全保護回路を設ける場合には、ソフトウェア起因のCCFを考慮した設備が別に設けられている。すなわち、多重化されたデジタル安全保護回路に対しては、そのソフトウェアの健全性を確保するためのV＆V等を実施することに加え、デジタル安全保護回路とは別に、その安全保護機能を代替する多様性を有した設備（以下「多様化設備」という。）が設けられている。

多様化設備が代替する機能については、安全保護系が有する機能に比べ限定的であるのが一般的で、低頻度DBAを除外している事例や多様性に関する解析評価を実施して必要な範囲に限定している事例がある。

多様化設備の設計グレードについては、安全系としている事例と非安全系としている事例の両方があるが、いずれの場合でも安全保護回路より低位の設計グレードとなっている。

海外における多様化設備にも日本と同様にHw機構で構成されるものがあるが、近年、特に新設炉において、PLD（Programmable Logic Device：ハードウェア記述言語で設計され、実行段階では、従来型のソフトウェアで論理演算を行うのではなく、ハードウェア上に構成された論理回路で信号処理が行われるデジタル半導体素子）といった新技術を多様化設備に適用しようとする動きも見られる。

（3）IAEAの新ガイド

IAEAは、昨今のデジタル技術の進展や利用の拡大を踏まえ、2016年、旧来の2つのカイドを統合・改定し、新たなガイド（SSG－39[7]）を策定した。

新ガイドは、I＆Cシステムやアーキテクチャの共通要因故障について、「共通要因故障に対する全ての脆弱性を完全に排除することは達成不可能である」とした上で、多様性を確保することによって共通要因故障の影響を緩和できるようにするべきとしている。また、多様性が安全保護系の共通要因故障の影響を緩和するものとして認められるためには、その多様性機構は、実際に影響緩和を達成できることを確認できなければならないとしている。

また、I＆Cの設計クライテリアに係る各国規制機関のプラクティスには多くの差異が認められるとして、新ガイドは、その検討過程で違いが認められた主な規制プラクティスをANNEXにまとめている。その中で、多様化設備については、ハードワイヤード・システムを要求している国、デジタル・システムの利用を禁止まではしていないが実質的に認めていない国、適正な多様性が実証されればデジタル・システムの利用を認めている国があるとしている。

---

[6] 高浜発電所1号機デジタル安全保護系のバックアップ設備について（平成28年6月　関西電力株式会社）

[7] “Design of Instrumentation and Control Systems for Nuclear Power Plants”, SSG-39, IAEA

2. 今後の取組方針（案）

国内では、デジタル安全保護回路を設ける場合には、Hw機構による多様化設備を自主的に整備しているが、最近の国際的な動向も踏まえ、信頼性向上の観点から現行規制の見直しを検討する。

具体的には、現在は自主設備となっている多様化設備を規制要求化することとし、当該設備に係る規制上の要求事項（設計グレードや代替する機能等）を整理するとともに、国内の導入実態や国際動向も踏まえ、規制対象とする~~「~~デジタル安全保護回路~~」~~の範囲~~定義~~について~~再~~検討する。

これらの検討に当たっては、規制委員会の了承を得て検討チームを設置し、国内事業者等からの意見（経過措置の要否等を含む。）も聴取しつつ、今年度内を目途に要求事項の整理等を行うこととしたい。なお、検討チームの設置・メンバー等については、改めて規制委員会にお諮りする。

【参考資料】

参考1. デジタル安全保護系に関する国内調査結果について（平成30年6月20日 原子力規制部）[8]
参考2. デジタル安全保護系の共通要因故障(CCF)対策設備に関する調査結果について（平成30年6月20日　技術基盤グループ）[9]
参考3. 高浜1号機工事計画認可申請書添付書類（デジタル制御方式を使用する安全保護系等の適用に関する説明書）（平成28年5月　関西電力株式会社）（抜粋）
参考4. 玄海原子力発電所3号炉及び4号炉原子炉安全保護計装盤等の更新について（2019年5月　九州電力株式会社）（抜粋）
参考5. 島根原子力発電所2号炉安全保護回路（平成31年2月　中国電力）（抜粋）
参考6. 高浜発電所1号機デジタル安全保護系のバックアップ設備について（平成28年6月　関西電力株式会社）（抜粋）
参考7. デジタル安全保護系に関する海外調査結果について（令和元年9月13日 システム安全研究部門）
参考8. “Design of Instrumentation and Control Systems for Nuclear Power Plants”(SSG-39, IAEA) （抜粋）
参考9. 関連条文

[8] 第32回技術情報検討会（平成30年6月20日） 資料 32-5-2 (1)
[9] 第32回技術情報検討会（平成30年6月20日） 資料 32-5-2 (2)

参考１

デジタル安全保護系に関する国内調査結果について

平成３０年６月２０日
原子力規制部

１．国内におけるデジタル制御系の実態調査

平成３０年３月５日及び１４日に、電気事業者（５日及び１４日）及びメーカ（１４日）に対し、デジタル制御系の国内実態に関するヒアリングを実施。調査対象としては、PWR について、高浜１・２号機（デジタル安全保護系に変更）、泊３号機（当初設計からデジタル安全保護系）、BWR について、柏崎刈羽６・７号機（当初設計からデジタル安全保護系（ABWR））、浜岡４号機（デジタル安全保護系は導入していない（BWR5））を選定。

主な調査結果は、以下のとおり。（別添１）

① 安全保護系（間連系含む。）のデジタル化の考え方

- ✓ デジタル化可能な範囲は原子炉停止系及び工学的安全施設の設定値比較部及び論理回路部（検出器からの信号をデジタルに変換する多重伝送盤から論理回路の出力部までの範囲）である。なお、原子炉停止系における制御棒動作回路については、設計上、応答時間の制約からデジタル化せずにアナログとしている。
- ✓ 補機冷却系などの関連系の制御回路は概ねデジタル化されている。一方、非常用ディーゼル発電機の起動制御はアナログである。

② 多重性、独立性が求められる MS-1,2 等以外の制御回路のデジタル化の状況

- ✓ MS-1,2 以外の制御回路にもデジタル制御回路は採用されており、概ね多重化されている。ABWR の再循環流量制御は 3 重化されている。

③ デジタル安全保護系に係る共通要因故障に対しての多様性の考慮

- ✓ 多重化されたデジタル制御系に多様性は導入しておらず、安全保護系の一部の機能（原子炉停止機能、格納容器隔離機能、高圧注水機能及びそれに必要な監視系）に対してハードワイヤードによるバックアップ設備を導入。
  PWR：ハードワイヤードの制御回路及び中央制御室からの手動操作
  BWR：中央制御室からの手動操作（ただし、原子炉停止系は安全系として設置）
- ✓ ハードワイヤードのバックアップ設備は、常用系統（ノンクラス）扱いであり、耐震 C クラスであるが、基準地震動に対して機能維持する設計としている。なお、ハードワイヤード設備のうち新基準対応として ATWS 緩和設備とした設備は、重大事故等対処設備として設計。

④ JEAC４６２０−２００８及び JEAG４６０９−２００８に対する設計上の考慮

- ✓ 定周期処理、シングルタスク構成、割り込み処理なしのシンプルなソフトウェア構造とするとともに、可視化言語の適用により第三者による検証を容易にしている。

⑤ V&V の具体的なチェック方法

- ✓ メーカベースでは、設計者ではない第３者が、図面等の図書を塗りつぶしチェックすることにより、上位仕様と下位仕様の整合性を確認している。

5

- ✓ 事業者ベースでは、メーカの実施した確認内容が問題ないかメーカベースの報告書を確認する。

⑥ 中央制御盤の入力システムにおける常用系と安全系の分離措置

- ✓ PWR の一部のプラントにおいて、操作性向上の観点から、常用系から安全系の操作も可能な設計としているが、常用系での故障が安全系に波及しないよう機能的分離を図っている。
- ✓ その他のプラントにおいては、入力システムの常用系と安全系は共用していない。

２．過去のデジタル安全保護系に関する文献調査

過去に原子力安全・保安院において、JEAC 及び JEAG の規格をエンドースする際に、保安院が示したデジタル安全保護系の共通要因故障に対しての考え方を、当時の WG 資料から確認した。

〇多重化されたデジタル安全保護系の健全性が実証されていれば、共通要因故障対策としての異なる原理の手段を手当する必要はない。

〇共通要因故障の発生確率がゼロであることを実証することは現実的ではないため、発生要因が十分に分析され、それを排除するための対策が有効であることを示せば、健全性が実証されていると判断できる。

〇具体的には、プログラミングエラーを排除するための品質確保対策としてのソフトウェアの設計・制作の単純化、可視化言語の採用等による検証の容易化が図られること、Ｖ＆Ｖを実施することで共通要因故障の発生は極めて低いとしている。

〇よって、国内プラントに採用されているバックアップとしてのハードワイヤード設備は自主設備としての扱いとなる。

〇なお、健全性が実証できない場合の別手段を設ける範囲については、ソフトウェアの共通要因故障と事故、過渡事象との同時発生確率を評価する等により、各事象に対して必要な安全機能を選定し、決定する必要がある。

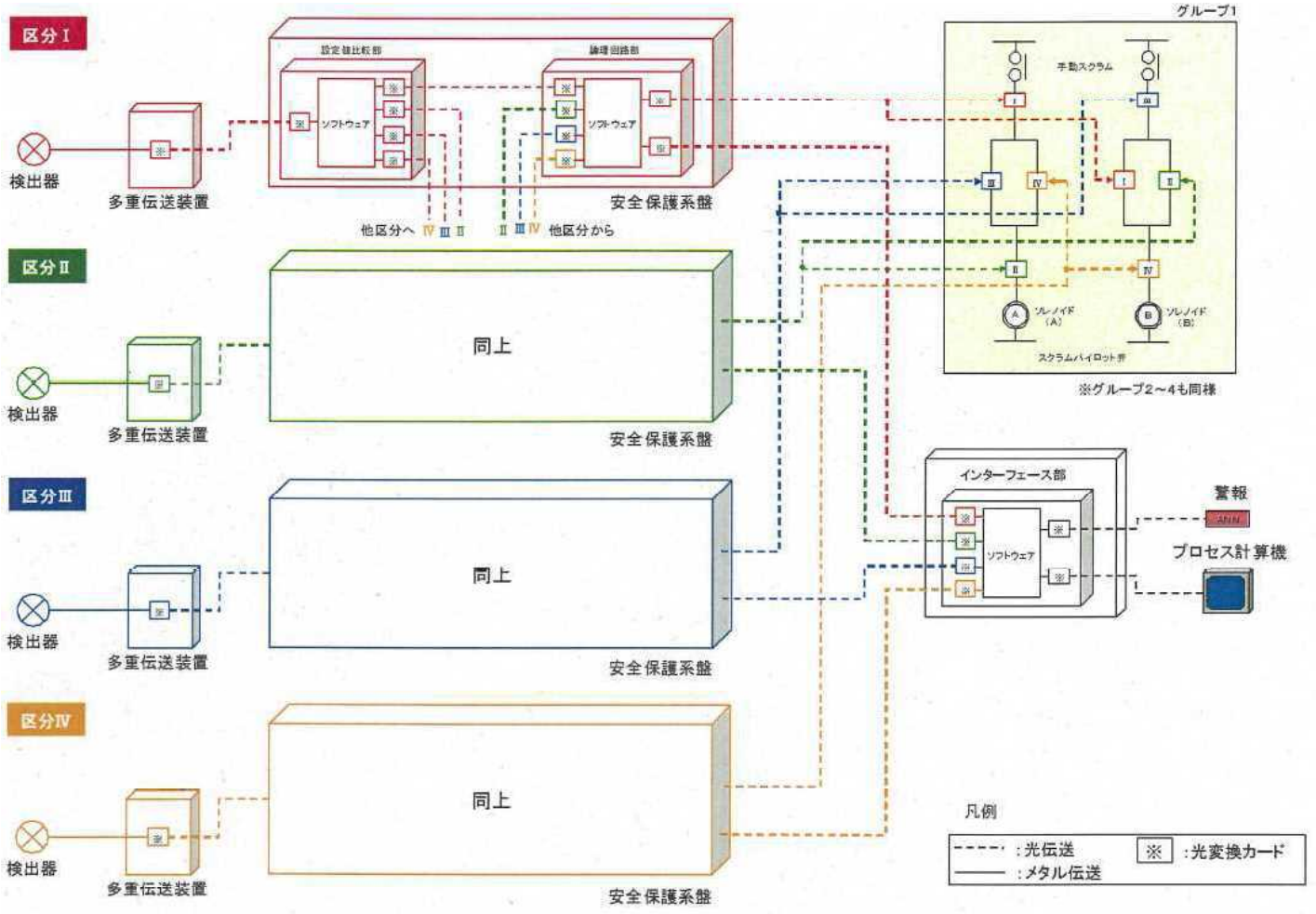
３．その他の文献調査（デジタル安全保護系に関する文献調査）

〇アナログ計測制御系については、モニタリング、制御機能等に関して良好な実績を有するが、経年劣化による機械的故障等が顕在化。

〇製造業界がデジタルに流れたため、アナログ機器の生産量の低下により、予備品の入手が困難な状況。

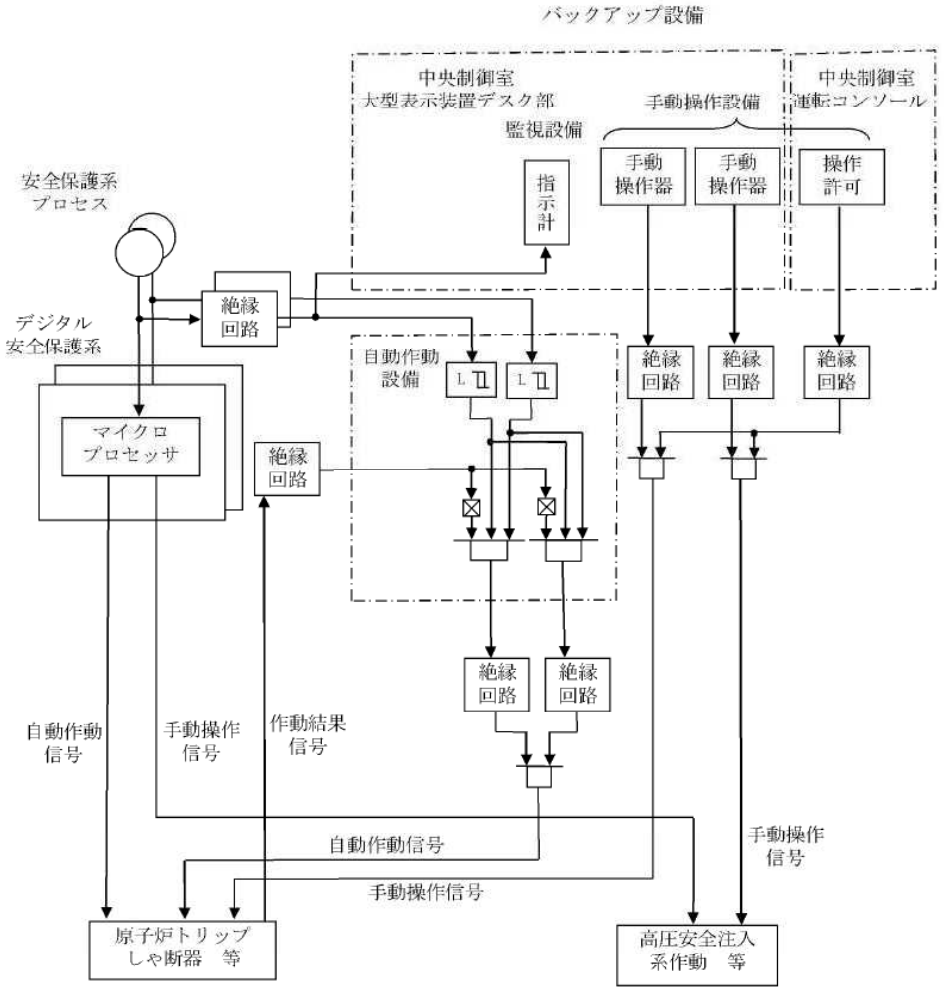
〇デジタル機器の保守の簡便さと、大量のデータを処理する能力としてのメリットがある。

〇一方、ソフトウェアの共通要因故障や使用実績の不足など、アナログにはない新たな信頼性に関する課題が浮上。



（柏崎刈羽原子力発電所６号及び７号炉審査資料から抜粋）

図１　安全保護系の構成概要図（例）



（高浜発電所審査資料から抜粋）

図２　バックアップ設備の構成概要図（例）

以上

8

別添１

平成30年3月14日
北海道電力（株）
東京電力HD（株）
中部電力（株）
関西電力（株）

No	ご質問	関西：高浜−1,2（PWR）	北海道：泊−3（PWR）	東京：KK−6/7（ABWR）	中部：H−4（BWR−5）
①	安全保護系のうち、デジタル化され得る範囲はどこまでか。	【T12工認資料47デジタル制御方式を使用する安全保護系等の適用に関する説明書P12,13,14参照】 ▪原子炉保護計器ラック ▪安全防護系シーケンス盤	【泊3号システム構成概要図参照】 安全保護系（検出器～制御装置～動作装置入力端子）のうち、制御装置の入力～出力までがデジタル化されている。	【（KK67添付資料）−①デジタル安全保護系システム構成図参照】 原子炉緊急停止系：多重伝送盤への入力～設定値比較部～論理回路部の出力部 工学的安全施設：多重伝送盤への入力～論理回路部～多重伝送盤の出力	安全保護系はデジタル化されていない。 H−5（ABWR）については、KK−6/7と同様。（以下同じ）
①−2	安全保護系の作動に際して必要となる間連系の制御回路はデジタル化されているか。	・安全保護系の作動に係る関連系（CCW,海水系等）の制御回路にもデジタル制御回路を採用している。 ▪D／G起動制御盤はｱﾅﾛｸﾞである。	安全保護系の作動に係る関連系（CCW,海水系等）の制御回路にもデジタル制御回路を採用している。 なお、D／G制御盤はｱﾅﾛｸﾞである。	【（KK67添付資料）−②計測制御設備の全体構成参照】 安全保護系の作動に係る関連系（原子炉補機冷却水系、原子炉補機冷却海水系等）の制御回路も基本的にデジタル化されている。 なお、D/G起動制御はアナログである。	安全保護系の作動に関する関連系はデジタル化されていない。 原子炉機器冷却水系，同海水系，D/Gはアナログである。なお、M/C，P/Cの保護継電器についてはデジタル制御回路に随時更新している。
①−3	多重性、独立性等が求められるMS−1,2等以外の制御回路について、同一の機能に対して複数のデジタル制御回路を採用している機器はどんなものがあるか（ABWRのRIP制御等）。	MS−1,2等以外の制御回路にもデジタル制御回路が採用されているものもあり、それらは概ね多重化されている。	【泊3号システム構成概要図参照】 MS−1,2等以外の制御回路にもデジタル制御回路が採用されているものもあり、それらは概ね多重化されている。	MS−1,2等以外の制御回路にもデジタル制御回路が採用されているものもあり、それらは概ね多重化されている。 例えば、再循環流量制御系は3重化構成としている。	再循環流量制御系、プロセス計算機、タービン系でデジタル制御回路が採用されている。 これらは概ね多重化されている。
②	（多重化され独立性が確保されている）デジタル安全保護系について、共通要因故障に対しての「多様性」を設計で考慮している場合、具体的にどのような多様性か。 ※NUREG/CR−7007レベルの情報。	【T12工認補足説明資料「デジタル安全保護系のバックアップ設備について」参照】 ハードワイヤード（マイクロプロセッサ以外）で制御回路を構成しているバックアップ設備を設定している。	ハードワイヤード（マイクロプロセッサ以外）で制御回路を構成しているバックアップ設備を設置している。	ハードワイヤードによるバックアップ設備を設けている。	−
③	デジタル安全保護系の共通要因故障を考慮してハードワイヤードのバックアップが設置されているか否か。				
③−1	設置されている場合ハードワイヤードがバックアップする安全機能の範囲はどこまでか。その範囲設定の考え方は何か。	【T12工認補足説明資料「ﾃﾞｼﾞﾀﾙ安全保護系のバックアップ設備について」参照】 1次系減圧事象「加圧器圧力低」、1次系加圧事象「加圧器圧力高」、2次冷却材喪失事象「SG水位異常低」の3つの信号をバックアップ設備に設けることにより、事象の発生を検知するとともに、自動での原子炉トリップ、タービントリップ、主給水隔離を行うものとする。 また、原子炉トリップ後、高温停止状態を維持するためには、ほとんどの事象で補助給水が必要となるため、「蒸気発生器水位異常低」により補助給水を自動起動する。	【泊3号設置許可申請書安全審査資料補足説明資料「共通要因故障対策盤（自動制御盤）（ATWS緩和設備）に関する健全性について」P.44−5(3)−11～13参照】 1次系減圧事象「加圧器圧力低」、1次系加圧事象「加圧器圧力高」、2次冷却材喪失事象「蒸気発生器水位低」の3つの信号をバックアップ設備に設けることにより、事象の発生を検知するとともに、自動での原子炉トリップ、タービントリップ、主給水隔離を行うものとする。 また、原子炉トリップ後、高温停止状態を維持するためには、ほとんどの事象で補助給水が必要となるため、「蒸気発生器水位低」により補助給水を自動起動する。	【（KK67添付資料）−③デジタル安全保護系のバックアップ設備】 ハードワイヤードによるバックアップ設備の範囲は「止める」「冷やす」「閉じ込める」機能のうち、以下の範囲としている。 操作系 ▪手動スクラム ▪主蒸気隔離弁閉止（手動） ▪主要な隔離弁　（原子炉冷却材浄化系，原子炉隔離時冷却系の内側隔離弁閉止（手動）） ▪高圧炉心注水系起動（手動） 監視系 ▪原子炉水位 ▪ドライウェル圧力 ▪主蒸気隔離弁の状態 ▪主要な隔離弁の状態　（原子炉冷却材浄化系，原子炉隔離時冷却系の内側隔離弁） ▪高圧炉心注水系起動状態 ▪高圧炉心注水系系統流量指示 また、重大事故等対処設備としてATWS緩和設備を設置している。 （ATWS緩和設備） ▪代替制御棒挿入機能 ▪代替冷却材再循環ポンプ▪トリップ機能	−
③−2	バックアップとしてハードワイヤードの安全重要度と耐震重要度はどう設定しているか（そもそも安全施設か）。 ※モデルは高浜1，2の工認の参考資料	【T12工認資料47デジタル制御方式を使用する安全保護系等の適用に関する説明書P12参照】 当該バックアップ設備は、ATWSへの対応機能を付加したことから、重大事故等対処設備として設計（改良）している。	当該バックアップ設備は、ATWSへの対応機能を付加したことから、重大事故等対処設備として設計（改良）している。	ハードワイヤードによるバックアップ設備については、以下の通り。 安全重要度：常用系の設計 耐震重要度：Cクラスの設計 但し、それぞれの系統と同じ重要度として扱っており、実力としては以下の通り。 操作系：Ss機能維持 監視系：ドライウェル圧力、原子炉水位低及びドライウェル圧力高警報以外はSs機能維持 ATWS緩和設備については、重大事故等対処設備として設計している。	−

9

No	ご質問	関西：高浜-1,2（PWR）	北海道：泊-3（PWR）	東京：KK-6/7（ABWR）	中部：H-4（BWR-5）
⑤	技術基準第35条解釈JEAC4620-2008、JEAG4609-2008、旧保安院技術評価書における要求事項に対して、具体的にどのように設計上考慮しているか。 （例）ソフトウェア処理構造の簡素化、等	【T12工認資料47デジタル制御方式を使用する安全保護系等の適用に関する説明書 別添参照】 ソフトウェアの品質を高めるため、定周期処理、シングルタスク構成、割り込み処理を認めない処理構造とするとともに、可視化言語を適用し、第三者による確認、検証を容易としている。	ソフトウェアの品質を高めるため、定周期処理、シングルタスク構成、割り込み処理を認めない処理構造とするとともに、可視化言語を適用し、第三者による確認、検証を容易としている。	デジタル安全保護系については、定周期処理、シングルタスク構成、割り込み処理なしのシンプルなソフトウェア構造にするとともに、可視化言語の適用により第三者による確認、検証を容易としている。	－
⑤－1	V＆Vについて、具体的なチェック方法等はどうなっているか（事業者ベース、メーカーベース）。	【T12工認資料47デジタル制御方式を使用する安全保護系等の適用に関する説明書 別添Ⅴ参照】 JEAGに基づいたV&Vを実施。	【泊3号設置許可申請書安全審査資料 安全保護回路の不正アクセス等防止について 補足説明資料P.5～8参照】 メーカ：設計者でない第3者が基準図書と確認図書の塗潰しチェックを実施し、上位仕様と下位仕様の整合が取れていることを確認する。確認結果を報告書にまとめる。 事業者：上記メーカ作業前に、メーカから提出される計画書、要領書を承認し、メーカ作業後、基準図書と確認図書の確認内容が問題無いか、メーカ報告書を確認する。	【（KK67添付資料）-④KK67設置許可24条まとめ資料_抜粋参照】 JEAG-4609，JEAC-4620に基づいたV&Vを実施している。 メーカ：設計者でない第3者が基準図書と確認図書の塗潰しチェックを実施し基準図書と確認図書の整合が取れていることを確認する。確認結果を報告書にまとめる。 事業者：報告書を確認し、基準図書と確認図書の確認内容が問題無いか目視確認を行い承認をする。	事業者が実施するV&Vは、デジタル安全保護系以外は社内規定化されていない。
⑥	中央制御盤をデジタル化する場合、入力システム（タッチパネル等）は常用系と安全系を共用しているか。共用している場合であって互いの分離措置がとられている場合、どのように担保されているか。	【T12工認補足説明資料「4-1_設計基準事故時の中央制御室の機能」参照】 ▪常用系は監視操作VDU、安全系は安全系VDUで構成している。 ▪運転性向上の観点より、常用系VDUから安全系補機の操作もできる設計としている。 ▪安全系の信号を優先し、常用系で故障が生じたとしても安全系に悪影響を与えないように、機能的に分離した設計としている。（弊社のみ関係）	中央制御盤はデジタル化しており、入力システム（タッチパネル）は、安全系と常用系で共用していない。	デジタル制御回路の操作画面であるFDについては、安全系と常用系で共用していない。	－

<技術情報検討会資料>
技術情報検討会は、新知見のふるい分けや作業担当課の特定を目的とした事務的な会議体であり、その資料及び議事録は原子力規制委員会の判断を示すものではありません。

参考２

デジタル安全保護系の共通要因故障(CCF)対策設備に関する調査結果について（案）

平成30年6月20日
技術基盤グループ

1. 現状

CCF 対策は、その発生防止のためのソフトウエア健全性確保策、多様化設計等と、発生した場合の影響緩和策（バックアップ設備の設置等）からなり、これらに関する国内外の現状は、概略以下にまとめられる。

	国内	海外（主に米国）
発生防止策（健全性確保策）	検証と妥当性確認(V&V)を義務付け ・専用実行環境(シングルタスク/割り込み無し)による決定論的動作を保証する検証性の高い S/W 構造 ・可視化言語による上流図書との一貫性保証とコーディング作業の排除 1980 年代には主要制御系、1990 年代には安全保護系へと段階的に適用し、実績に基づいて信頼性を確保	検証と妥当性確認(V&V)を義務付け ・市販の OS、開発環境で可能な範囲の S/W 構造の簡素化、可視化等の対策を実施 米国では最近の設備更新、建設中の新規プラントでデジタル安全保護系システムが適用されている。
影響緩和策	規制基準として、健全性が実証されない場合の追加対策を求めている。 事業者は上記発生防止策、設計ベース設備内の多様化設計により追加の多様化設備は必須ではなく、自主設置のものと位置付けている。	規制基準として、共通要因故障に対する脆弱性の評価と対策を求め、規制要件として DAS*1 が導入されている。 事業者は規制当局の評価ガイドに加え、より実用性の高いガイドの開発を規制当局と連携して進めている。

*1: DAS：Diverse Actuation System （補足資料－１参照）

2. 評価

国内外とも、発生防止策を施した上で、更に脆弱な部分について必要な対策をとるものとしており、基本的な考え方については共通している。

我が国においては発生防止策であるソフトウエアの信頼性確保を重視してきており、デジタルシステムの豊富かつ良好な適用実績からこの効果を確認でき、また事業者における多様化設計も海外に比べ特段の差異がある状況ではない。

但し、比較的影響緩和策を重視する海外とは、多様化設備を規制要件とするか否かの点で差異を生じている。

以上

補足資料-1：共通原因故障(CCF)と多様化設備の概要

(1)共通原因故障（CCF：Common Cause Failure）

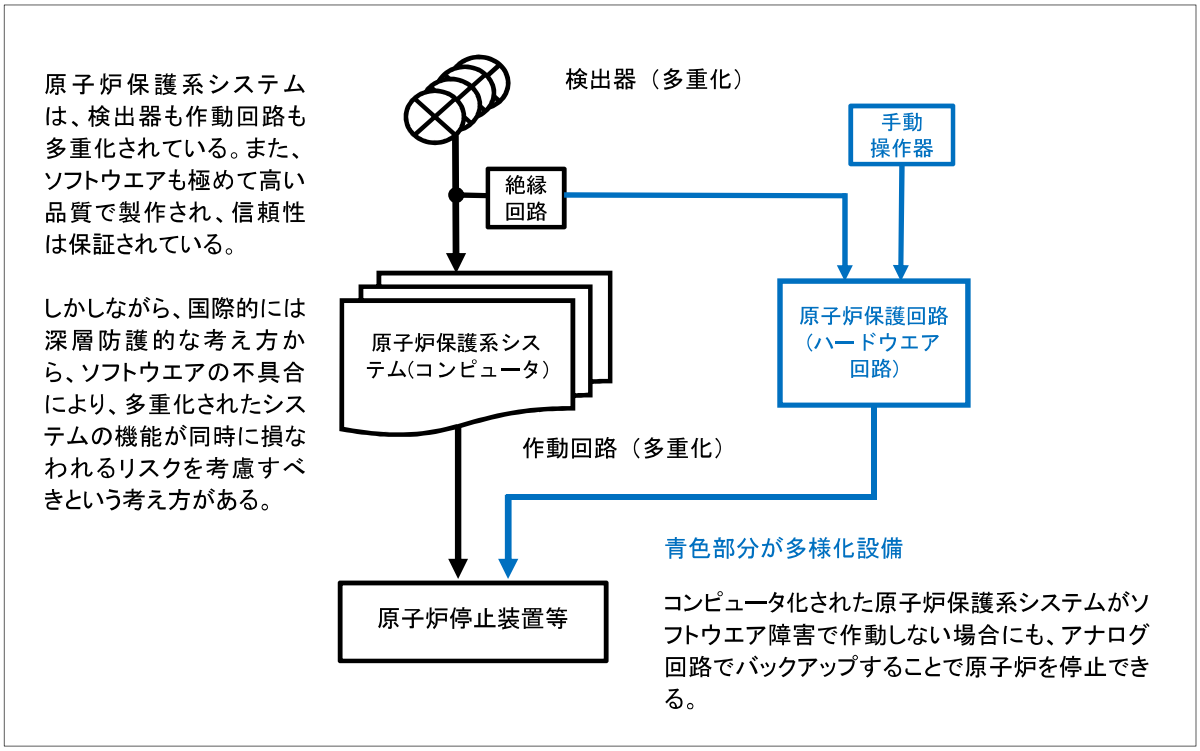
IAEA では CCF は、「単一の特定の事象または原因による二つ以上の構造、システムおよび機器の不具合」と定義されている。このうち、本調査が対象とするのは原子炉安全保護系システムにコンピュータが適用される場合に、ソフトウエアの不具合に起因して多重化された安全システムが、同時に機能しなくなる不具合である。

(2)多様化設備

上記(1)のソフトウエアの不具合に起因する CCF に対する対策として、異なる技術、例えばソフトウエアを含まないアナログのバックアップ回路等により対策するもの。 自動的に、あるいは手動操作で原子炉を停止する回路、事故時の運転操作のために手動操作を行うための回路等がある。

同様に多様化設備である ATWS（過渡変化時のスクラム失敗事象）緩和設備と統合して一つのシステムとしても良いと考えられている。

海外では、これと関連する概念として DAS（Diverse Actuation System）がある。本資料では、米国の規制要件に相当する設備と考えられるものを DAS と称している。



多様化設備の例

注）原理を説明するために簡略化した図であり、実際のシステム構成とは異なります。

参考３

V.　デジタル安全保護系ソフトウェアの品質保証について

1. 概要

本資料は、安全保護系へデジタル制御装置を適用するに当たり、安全保護上要求される機能を正しく確実に実現するためのソフトウェアに対する品質保証活動について説明する。

2. 基本方針

デジタル安全保護系は、「原子力発電所における安全のための品質保証規程」（JEAC4111-2009）並びに「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」（JEAG4121-2009 の付属書）に基づく品質保証活動により、十分な品質を確保している。

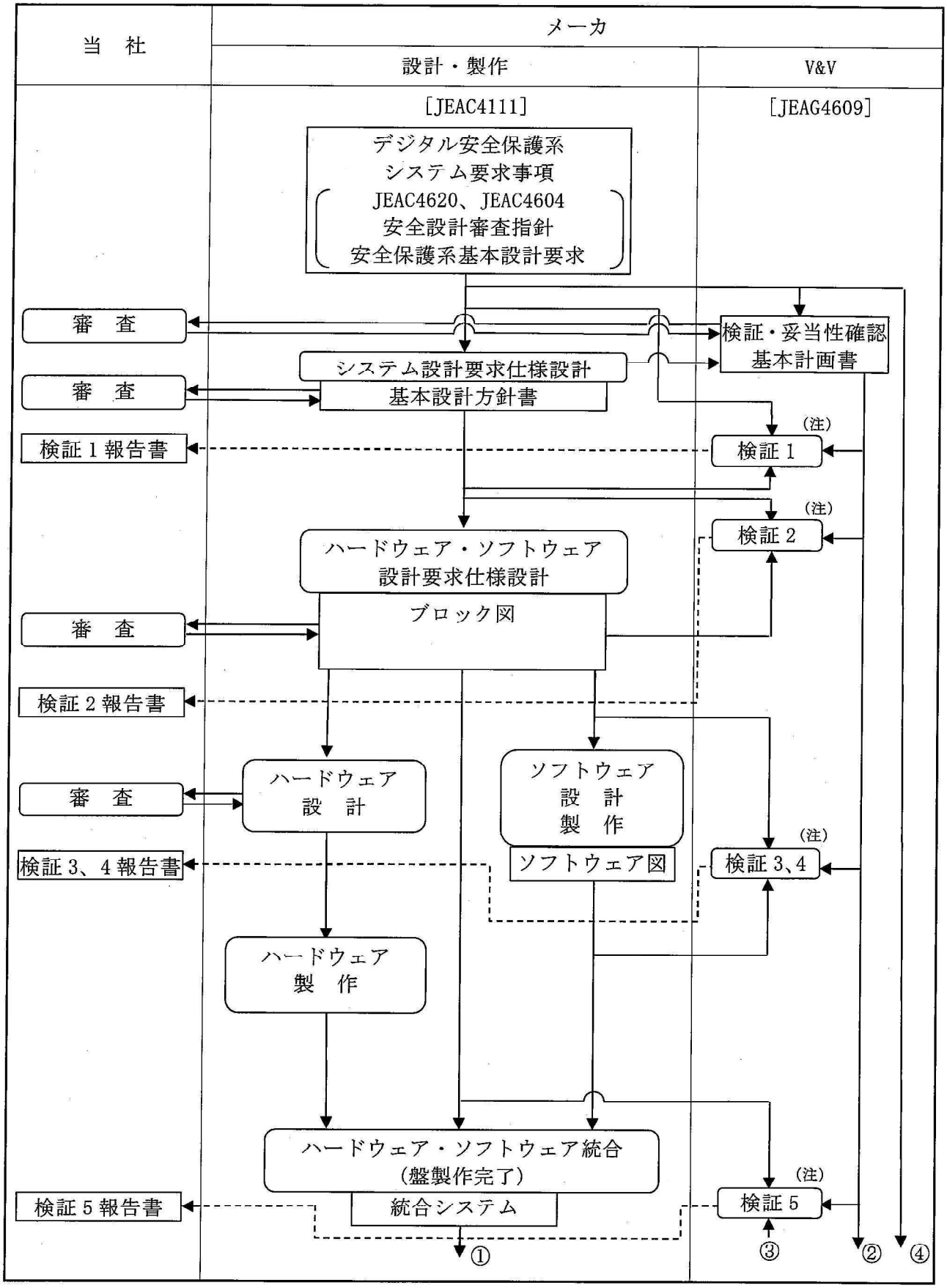
デジタル安全保護系は、ソフトウェアの品質を高めるために、定周期処理、シングルタスク構成、割り込み処理を設けない簡素なソフトウェア処理構造にするとともに、可視化言語の適用により第三者による確認、検証を容易としている。

また、デジタル安全保護系に採用予定の制御装置は、国内では原子力プラントの計測制御系等において 15 年以上、安全保護系にも 5 年以上の稼動実績を有しているが、これまでソフトウェアに起因する故障は発生しておらず、十分に高い信頼性が実証されている。

これらに加えて、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、「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）に基づき以下の品質保証活動を実施する。

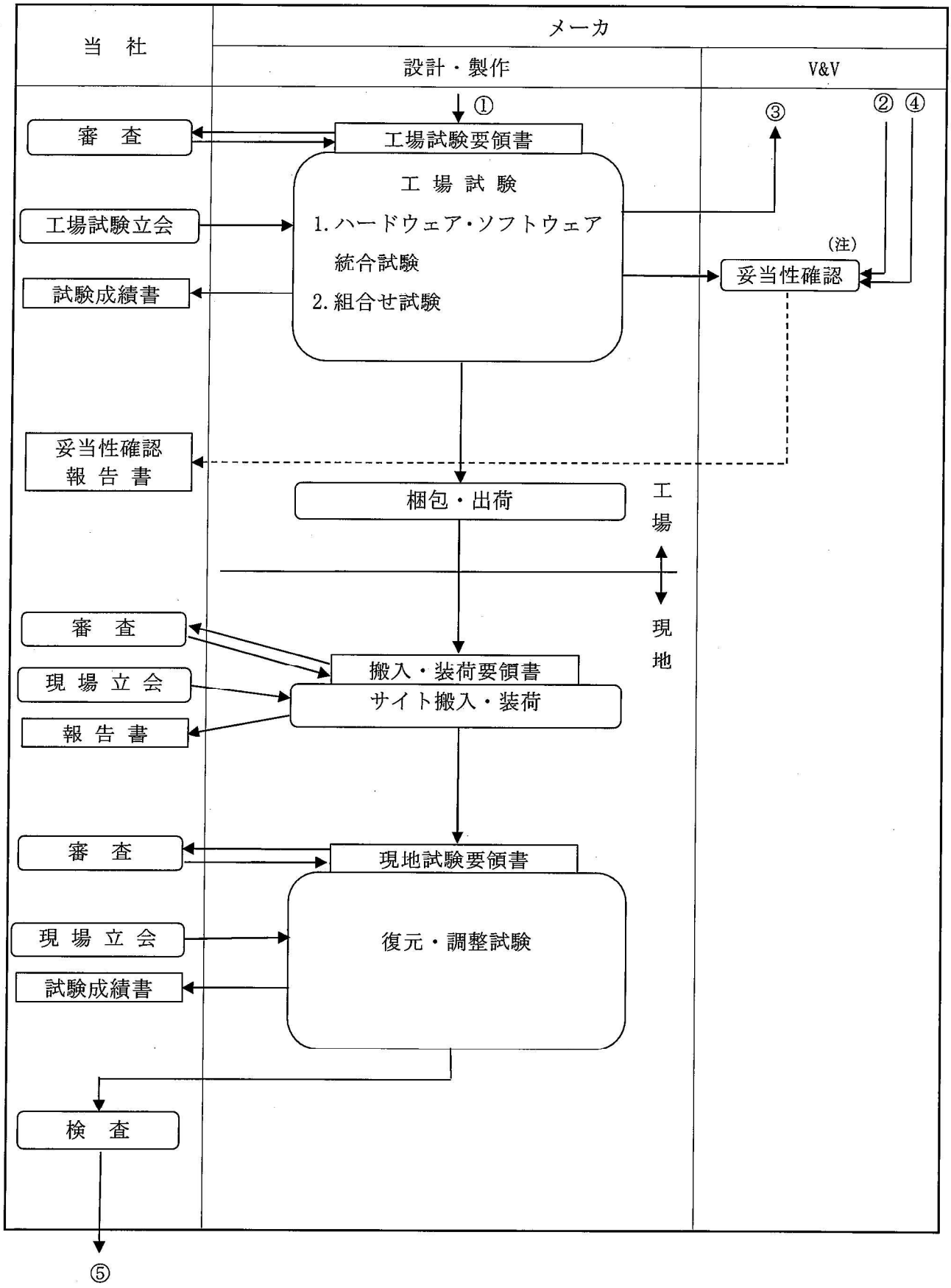
・ソフトウェアのライフサイクルのプロセス（設計、製作、試験、装荷、運転、変更、廃止）における品質管理方法を予め定め、実施するとともにその結果を文書化し管理する。
・各々のプロセスでのアウトプットについては、構成管理手法を予め定め、それに従ってソフトウェアの構成を管理する。
・設計、製作、試験、変更のプロセスの過程で、JEAG4609-2008「ディジタル安全保護系の検証及び妥当性確認に関する指針」に基づく検証及び妥当性確認（V&V）を実施する。

第１図　デジタル安全保護系の設計・製作及び検証と妥当性確認の流れ

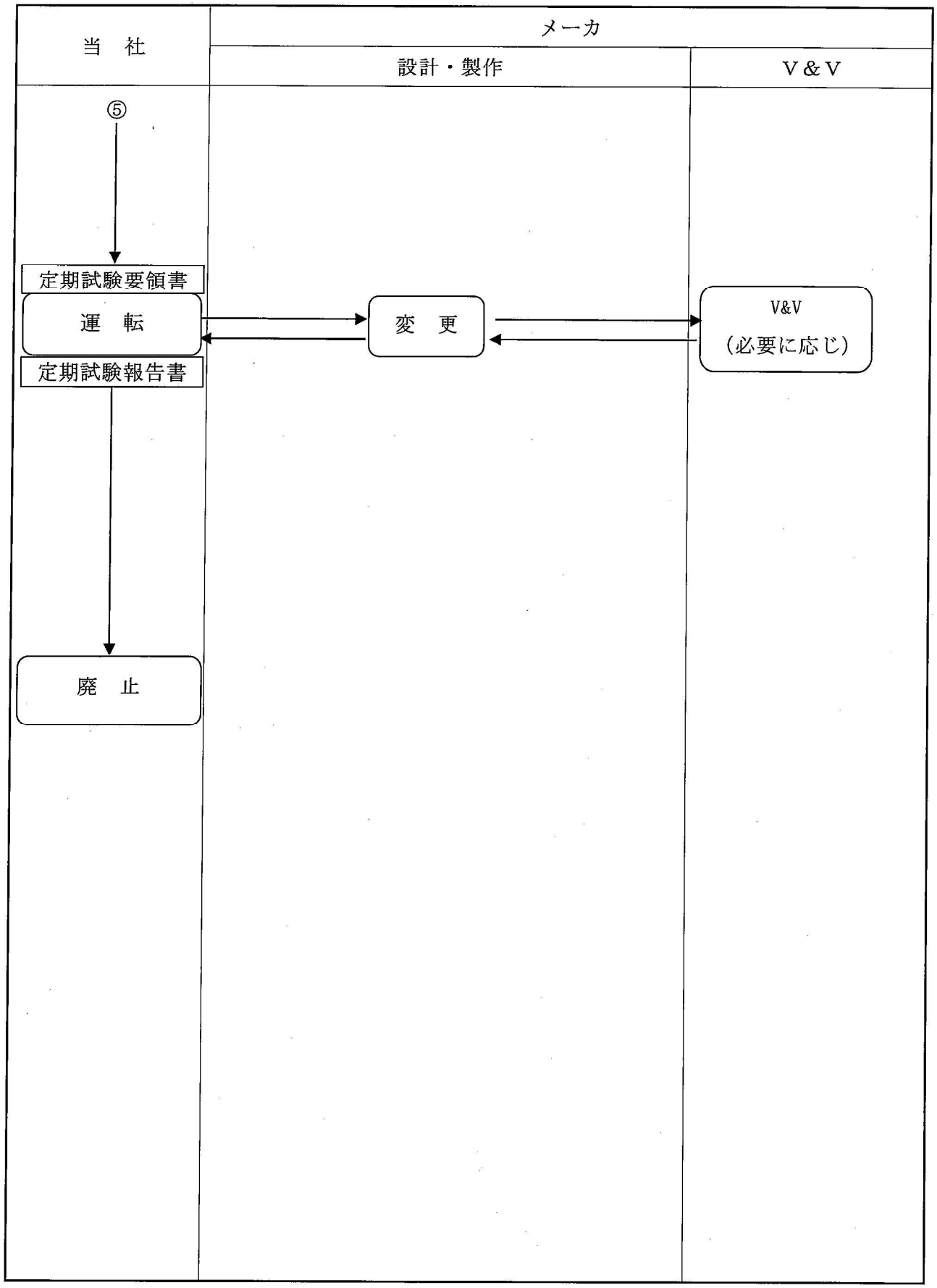


（注）作業内容、合格基準、不良結果等に対する措置を「検証要領書」として文書化する。

15



(注) 作業内容、合格基準、不良結果等に対する措置を「検証要領書」として文書化する。


当　社
メーカ
設計・製作
V＆V
⑤
定期試験要領書
運　転
定期試験報告書
変　更
V&V
（必要に応じ）
廃　止

参考４

玄海原子力発電所３号炉及び４号炉
原子炉安全保護計装盤等の更新について

２０１９年５月９日

九州電力株式会社

枠囲みの範囲は、防護上の観点又は機密に係る事項であるため、公開できません。

2．更新工事の概要（１／３）

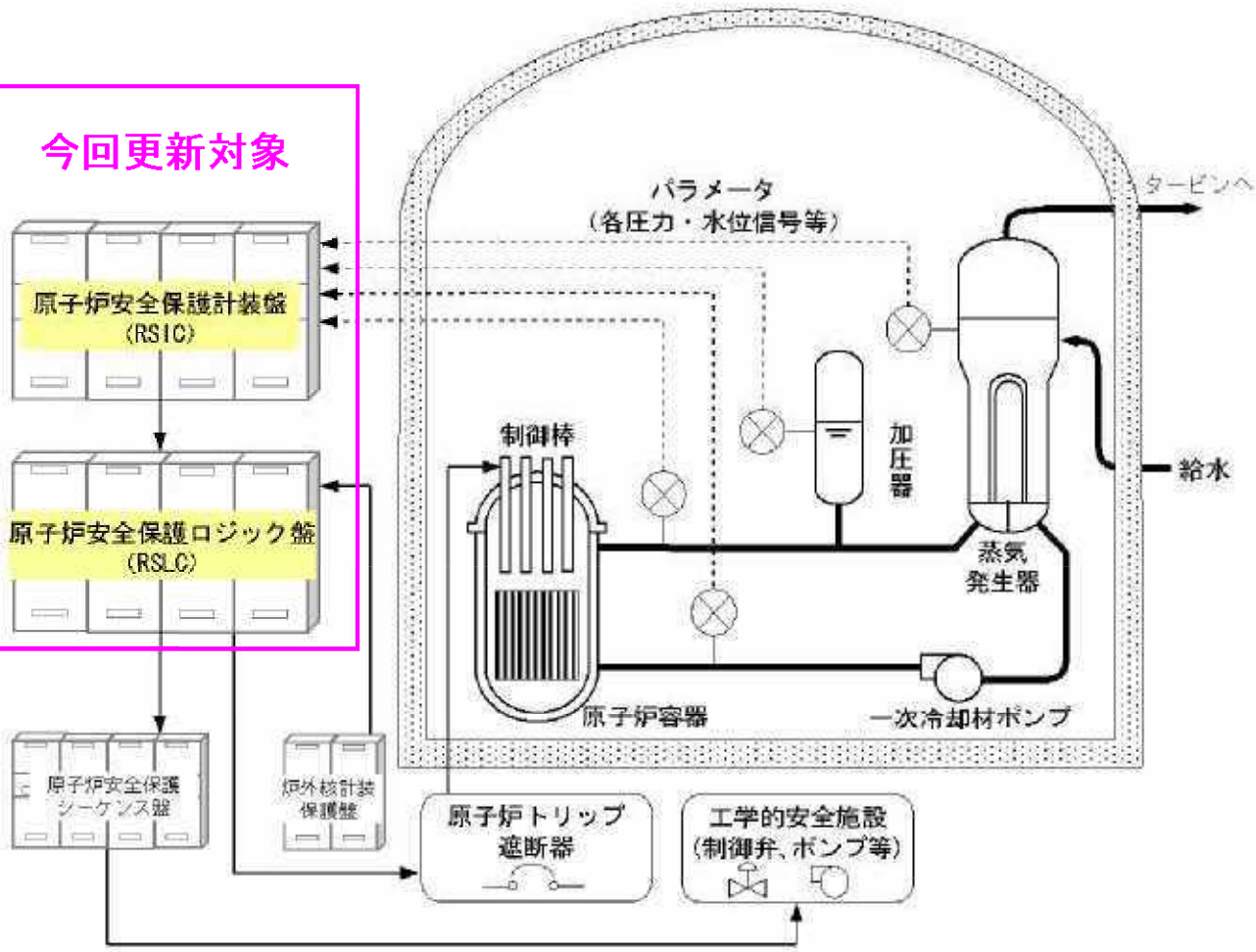
安全保護設備は、原子炉計装設備や１次冷却材系統の圧力・水位等の信号、又は中央制御室の手動スイッチからの信号を受けて、それぞれ定められたロジックと一致した場合に、原子炉トリップ系や工学的安全施設等を作動させる設備である。

【原子炉安全保護計装盤】
１次冷却材圧力等のパラメータ信号を受け作動設定値との比較演算を行い、作動設定値に達したチャンネルは、原子炉安全保護ロジック盤に異常信号を発信すると共に、中央制御室に警報を発信する。

【原子炉安全保護ロジック盤】
異常信号を受け、規定のロジック（規定チャンネル数以上）に従って原子炉トリップ及び工学的安全施設作動用の信号を発信すると共に、中央制御室に警報を発信する。

【原子炉安全保護シーケンス盤】
工学的安全施設作動用の信号を受け、シーケンスに従って工学的安全施設の弁、ポンプ等を作動させる。

【炉外核計装保護盤】
中性子束レベルの信号を受け作動設定値との比較演算を行い、作動設定値に達したチャンネルは、原子炉安全保護ロジック盤に異常信号を発信すると共に、中央制御室に警報を発信する。



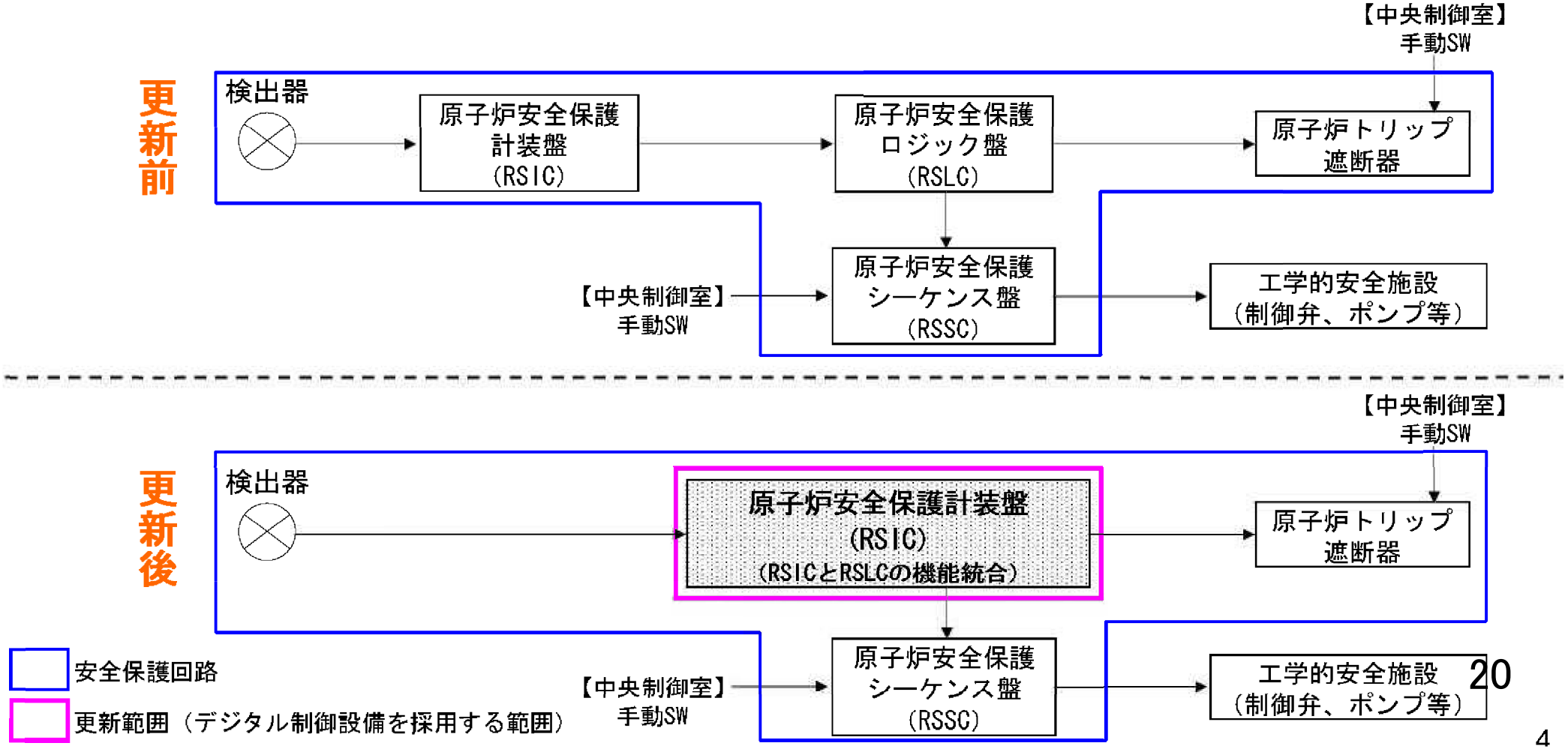
2．更新工事の概要（2／3）

○更新にあたっては以下を考慮する

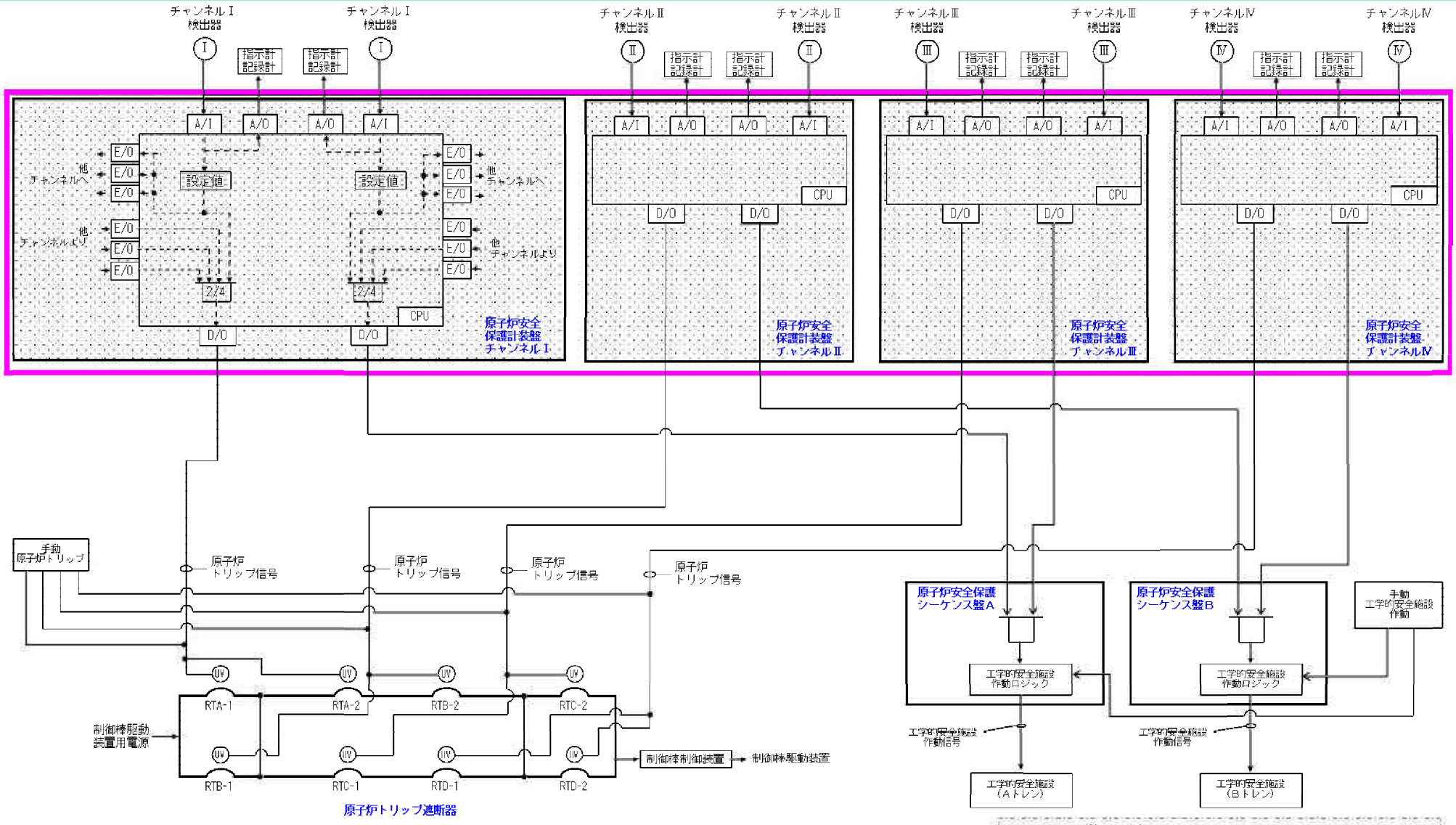
・安全保護設備へのデジタル制御設備採用においても、設置（変更）許可を受けた安全解析で使用している安全保護設備の応答時間を満足する設計とする。

・機能及び設置場所（設置建屋及び区画）の変更はしない。

（原子炉補助建屋　ＥＬ．１１．３ｍ　Ａリレー室（Ａトレン）及びＢリレー室（Ｂトレン））



2．更新工事の概要（3／3）



更新範囲（デジタル制御設備を採用する範囲）

参考５

島根原子力発電所２号炉

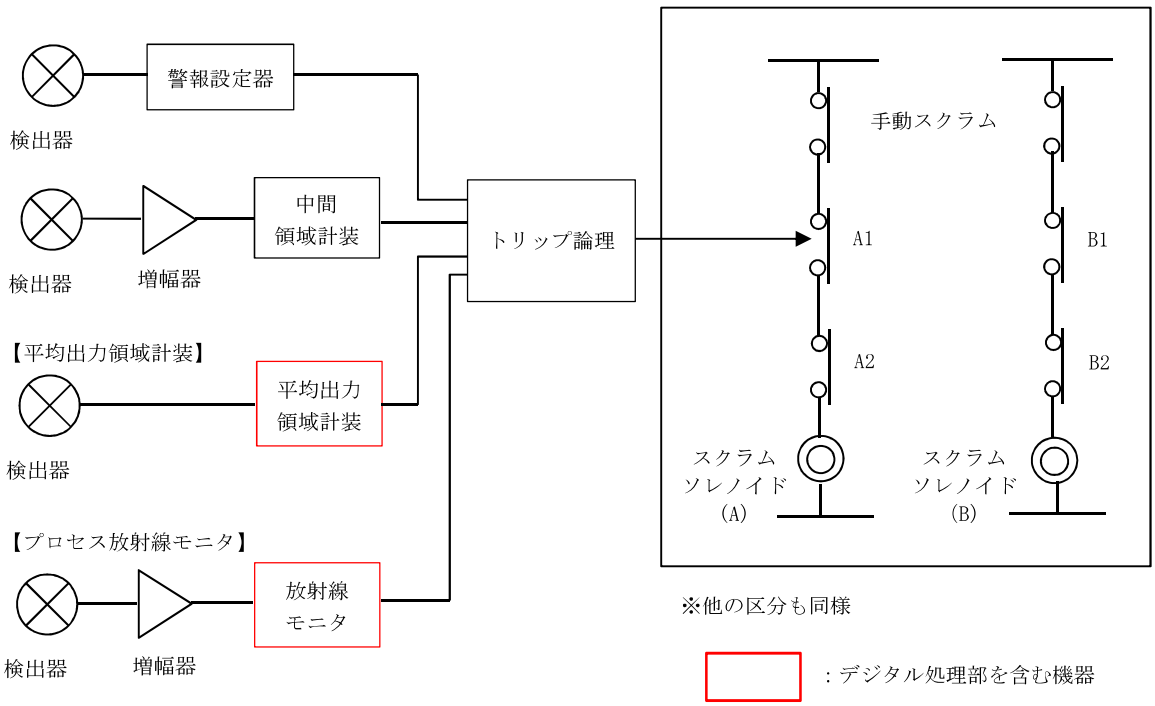
安全保護回路

平成31年2月

中国電力株式会社

本資料のうち，枠囲みの内容は機密に係る事項のため公開できません。

アナログ型安全保護回路（A1 チャンネル）の例



第１図　安全保護回路の構成例（原子炉保護系）

第１表　原子炉保護系の構成機器

原子炉スクラム信号の種類		検出器	設定器
原子炉圧力高		アナログ	アナログ
原子炉水位低（レベル３）		アナログ	アナログ
格納容器圧力高		アナログ	アナログ
中性子束高	平均出力領域計装	アナログ	デジタル
	中間領域計装	アナログ	アナログ
中性子計装不作動	平均出力領域計装	アナログ	デジタル
	中間領域計装	アナログ	アナログ
スクラム排出水容器水位高		アナログ（接点）	
		アナログ	アナログ
主蒸気隔離弁閉		アナログ（接点）	
主蒸気止め弁閉		アナログ（接点）	
蒸気加減弁急速閉		アナログ（接点）	
主蒸気管放射線高		アナログ	デジタル
地震大		アナログ（接点）	
手動		アナログ（接点）	
原子炉モードスイッチ「停止」位置		アナログ（接点）	

参考６

高浜発電所１号機

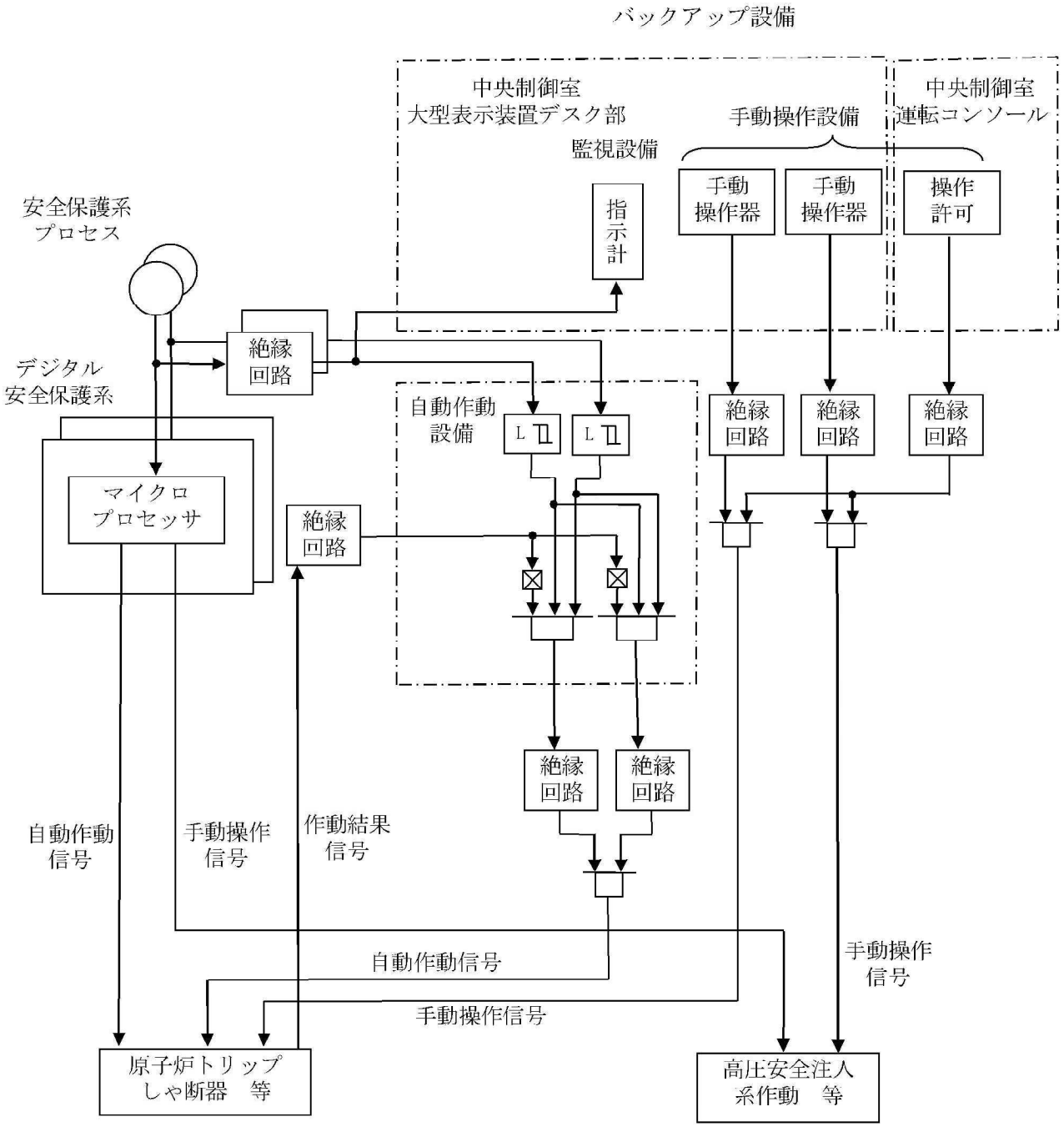
デジタル制御方式を使用する安全保護系等の適用に関する説明書に係る補足説明資料

デジタル安全保護系のバックアップ設備について

平成28年6月

関西電力株式会社

枠囲みの範囲は機密に係る事項ですので公開することはできません。



第１図　バックアップ設備の構成概略

3.2 機能選定の考え方

バックアップ設備に要求される機能を選定するに当たっては、

◇起因となる事象の起こり易さ（起因事象発生頻度）

◇各事象に対する「必要最小限の安全機能」

◇「必要最小限の安全機能」が必要となるタイミング

に着目し、適切な安全機能を確保できる機能を選定する。

3.2.1　起因事象発生頻度

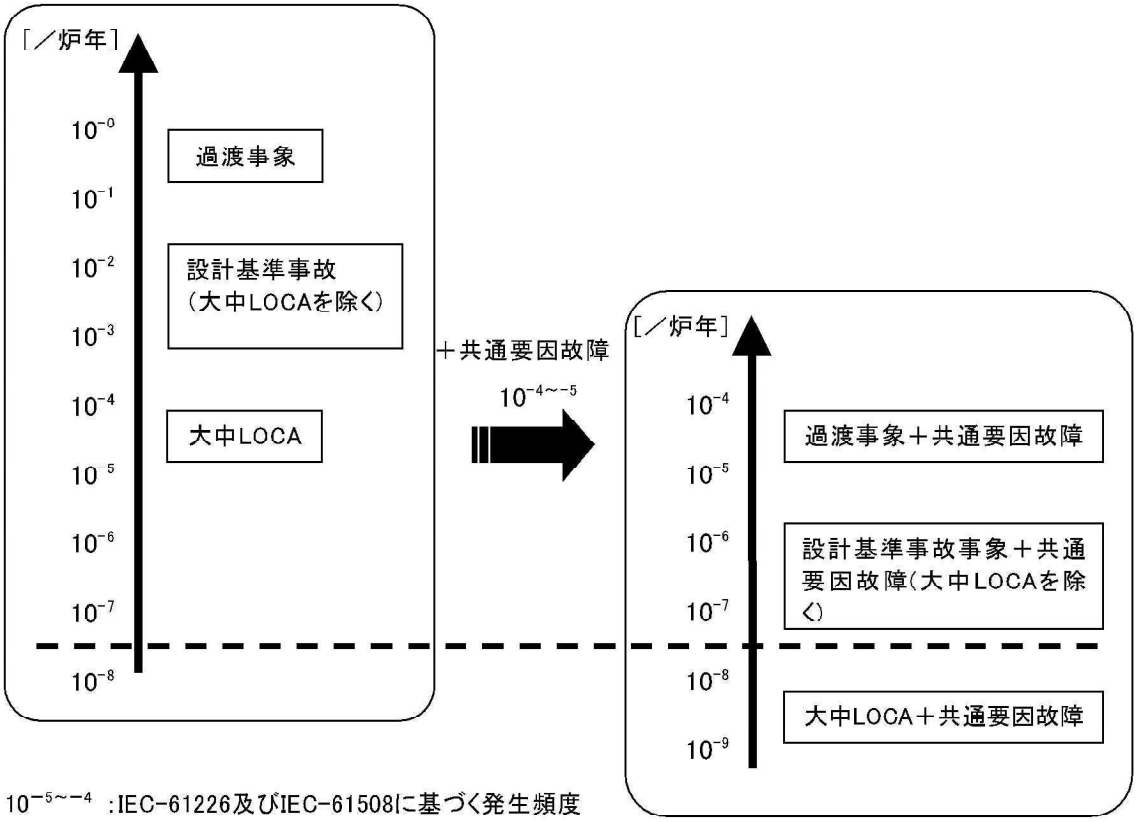
起因事象の発生頻度を第2図に示す。第2図から分かるように、大中破断の「原子炉冷却材喪失」（ＬＯＣＡ）については、他の設計基準事故事象と比較しても、その発生頻度は1桁小さい。

さらに、共通要因によりデジタル安全保護系のソフトウェアが機能喪失したことによる作動失敗確率をIEC 61508※1にて示される安全機能の安全度水準を参考に 10^{-5}～10^{-4} /demandとした場合の、大中破断ＬＯＣＡ＋共通要因故障の発生頻度は、第2図から分かるように極めて低い頻度となる。

以上より、発生頻度の極めて低い大中破断ＬＯＣＡについては、共通要因によりデジタル安全保護系のソフトウェアが機能喪失する場合との重ね合わせは対象外とすることで、合理的な設備を実現するものとする。

※1

IEC-61508（Functional safety of electrical/electronic/ programmable electronic safety-related systems （電気・電子・プログラマブル電子安全関連系の機能安全））の安全機能の安全度水準（safety integrity level）における作動失敗確率の目標値。安全機能の最も高い水準「4」のシステムの目標作動失敗確率は、10^{-5}以上10^{-4}未満とされている。



第２図　起因事象と起因事象＋共通要因故障の発生頻度の関係（概念図）

3.2.2　必要最小限の安全機能と必要となるタイミング

バックアップ設備として「運転時の異常な過渡変化」及び「設計基準事故」の各事象の収束を図るため、「止める」、「冷やす」、「閉じ込める」の観点から必要となる「必要最小限の安全機能」を第１表に示す。

バックアップ設備としてこれらの機能を実現するに当たっては、

◇「必要最小限の安全機能」が必要となるタイミング

に着目し、適切に設計目標を達成できるよう考慮する。

具体的には、「運転時の異常な過渡変化」及び「設計基準事故」の各事象において、「必要最小限の安全機能」が必要となるタイミングによって下記の３つに分類を行い、その分類毎に「必要最小限の安全機能」をどのように実現させるか（自動作動又は手動操作）を決定する。

各分類に対するバックアップ設備としての対応は、以下に示す考え方に従うものとする。

a)　早期の対応が必要なもの（第１表のＡ）

・自動で対応するものとし、自動設備を設ける。

b)　10 分程度での対応（第１表のＢ）

・中央制御室等の比較的操作が行いやすい場所からの操作とする。

c)　30 分程度以上での対応（第１表のＣ）

・時間余裕は大きく、基本的に現場での操作とする。

なお、事象発生時の影響が非常に大きい、及び／又は、運転操作性を考慮する必要がある場合には、ワンランク上の対応とする。

また、自動設備の動作確認及び手動操作に必要な監視機能を設けるものとする。

第１表　バックアップ設備として必要となる安全機能

	止める		冷やす					閉じ込める			
	原子炉トリップ	タービントリップ	補助給水	補助給水隔離	安全注入作動	主蒸気逃がし弁	加圧器逃がし弁	給水隔離	主蒸気隔離	内部スプレ	原子炉格納容器隔離
運転時の異常な過渡変化	A	A	A					A			
蒸気発生器伝熱管破損	A		C	C	C	B	B	A	C		
主蒸気管破断	A		C	C				A	C	C	
主給水管破断	A		A	B						C	
小破断ＬＯＣＡ	A		C		B					C	C

Ａ～Ｃは事象が発生してから各機能が要求されるタイミングを表す。

Ａ：早期　→　自動で対応するものとし、自動設備を設ける

Ｂ：１０分程度　→　中央制御室等の比較的操作が行いやすい場所からの操作とする

Ｃ：３０分程度以上　→　基本的に現場での操作とする

なお、事象発生時の影響が非常に大きい、及び／又は、運転操作性を考慮する必要がある場合には、ワンランク上の対応とする

参考７

デジタル安全保護系に関する海外調査結果について

令和元年９月１３日
システム安全研究部門

１．海外におけるデジタル安全保護系 CCF 対策の実態調査

平成３０年６月２０日に開催された第３２回技術情報検討会において報告した「デジタル安全保護系の共通要因故障（CCF）対策設備に関する調査結果について」以降、技術基盤グループにおいて、海外における安全保護系等に係る共通原因故障対策（以下、CCF 対策という。）について調査を継続し、現時点までにとりまとめたものを報告する。

２．調査内容

技術基盤グループでは、平成２９年度に着手して以降、安全保護装置等へ適用された各国プラントの CCF 対策、及びこれに関連する規制基準、国際標準等について調査を実施している。

ここでは、昨年度に調査を完了した内容のうち、海外（米国、フランス、カナダ等）の２０プラントの CCF 対策状況について概要調査を実施した部分についてまとめた。

３．調査結果

調査したプラントの CCF 対策について、調査した結果を添付資料に示す。

４．今後の予定

〇これまでの調査結果を踏まえ、バックアップを設ける範囲、PLD 等の新技術の適用に関する規制上の取り扱い、「デジタル安全保護回路」以外も含めた I&C 全体でデジタル技術がどのように適用され、どのように規制されているか等について、今後も調査研究を継続する。

〇これまでに調査した CCF の影響緩和策に加え、発生防止策としての検証と妥当性確認を含むソフトウエア等の品質確保策について最新動向を調査する。

〇米国では、CCF 対策を含む既設設備のデジタル化更新について、統合アクションプラン（IAP：Integrated Action Plan）における検討が実施されているため、この最新動向を調査する。

添付資料

安全保護系等共通原因故障（CCF）対策海外動向調査結果

1. 調査内容

安全保護装置等へ適用された各国プラントの CCF 対策、及びこれに関連する規制基準、国際標準等について調査を実施している。ここでは、H30年度に調査を完了した内容のうち、海外20プラントの CCF 対策状況について概要調査を実施した部分について結果をまとめた。

2. 調査対象

各国のプラントに適用されているデジタル安全保護装置、及び深層防護多様化設備(DAS)の概要について幅広く調査・分析するため、以下の観点から調査対象を選定した。

【対象国】

a. 米国、及び欧州の最新プラントから代表例を選定する。
b. デジタル技術が新興国の新規建設プラントに適用される例があることから、この代表例を含める（結果として、中国、韓国、台湾、ロシア等を選定）
c. 同一の炉型で建設する国が異なるものを含める。（結果として各国で計画がある EPR、A-BWR を含めて選定）

【対象炉型】

d. 国内のプラントに類似したプラントを選定する（A-PWR、A-BWR）
e. 一般的な軽水炉(PWR/BWR)を主たる調査対象とするが、炉型の異なるものを含める（結果として、静的安全炉（AP-1000）、CANDU 炉、小型モジュール炉（SMR）を選定）

【建設時期】

f. 時期的な変遷を把握できるように、建設年代の異なるものを選定する。（結果として、米国で CCF 対策が規制化される１９９３年前後の比較ができるように選定）

【設計変更・設備更新】

g. 建設時にデジタル設備への設計変更を実施した事例、及び既設プラントの設備更新の代表例を含める。

これらにより調査対象として選定したプラントを以下の①～⑳に示す。（括弧内は主たる選定理由を示す。）

調査対象プラント

① カナダで運転中の Darlington-1/2/3/4(建設時からデジタル安全保護装置採用)(a, e, f)
② 英国で運転中の Sizewell-B(建設時からデジタル安全保護装置採用)(a, f)
③ 米国で運転中の Watts Bar-1/2(建設時からデジタル安全保護装置採用)(a, g)
④ フランスで運転中の P4/P'4/N4 プラント(建設時からデジタル安全保護装置採用)(a, f)
⑤ チェコで運転中の Temelin-1/2(建設中にデジタル安全保護装置に変更)(a, f, g)
⑥ 韓国で運転中の Hanul(Ulchin)-5/6(建設時からデジタル安全保護装置採用)(b. f)
⑦ 台湾で建設中の Lungmen-1/2(建設時からデジタル安全保護装置採用)(b. c. d)
⑧ 米国で運転中の Oconee-1/2/3(デジタル安全保護装置に更新済)(a, g)
⑨ ロシアで運転中の NVNPP-6/7(建設時からデジタル安全保護装置採用)(b)
⑩ 米国で建設中の AP-1000 プラント(建設時からデジタル安全保護装置採用)(a, e)
⑪ 米国で DC 更新審査中の ABWR プラント(デジタル安全保護装置採用で申請)(a, c, d)
⑫ フィンランドで建設中の Olkiluoto-3(建設時からデジタル安全保護装置採用)(a, c)
⑬ フランスで建設中の Flamanville-3(建設時からデジタル安全保護装置採用)(a, c)
⑭ 中国で建設中の ACPR-1000 プラント(建設時からデジタル安全保護装置採用)(b)
⑮ 米国で運転中の Diablo Cannyon-1/2(デジタル安全保護装置への更新認可を取得)(a, g)
⑯ 米国で DC 審査中の U.S.EPR プラント(デジタル安全保護装置採用で申請)(a, c)
⑰ 米国で DC 審査中の US-APWR プラント(デジタル安全保護装置採用で申請)(d)
⑱ 米国で DC 認可取得済の APR-1400 プラント(デジタル安全保護装置採用で申請)(b)
⑲ 英国で審査中の UK-ABWR プラント(デジタル安全保護装置採用で申請)(a, c, d)
⑳ 米国で DC 審査中の SMR プラント(デジタル安全保護装置採用で申請)(a, e)

3. 調査項目

多様化設計に関する概要調査は、主に以下a～cの観点から実施した。

a. I&C システム設計方針及びこれに基づくシステムの概要

CCF 対策は、安全保護系設備自体の設計、及びプラントレベルの多様化設計・深層防護の考え方等にも影響を受ける可能性があることを考慮し、以下をまとめることとした。

- プラントの概要(国及び炉型)
- 適用時期(プラントの建設時期、デジタル更新を実施した時期等)
- 深層防護の考え方
- 安全保護装置の概要(多重化構成等)

b. 深層防護のための多様化設計の概要

デジタル安全保護系の CCF 対策として、以下の両面を調査項目とした。

- 発生防止対策（主として V&V を基本とする品質管理による対策）
- 影響緩和対策（主として多様化設計による対策）

c. その他

最新動向として国際的な課題となっている、組込デジタルデバイス、及びコンピュータセキュリティとの関連等について以下を調査項目とした。

- 入力部の多様性（検出系等の信号入力部の組込デジタルデバイスの取り扱い）
- 出力部の多様性（作動機器等の信号出力部の組込デジタルデバイスの取り扱い）
- コンピュータセキュリティ（CS）との関連（多様化設備がセキュリティ対策としても期待されているか否かについて、安全設計側の公開資料から調査した。）

4. 調査結果

調査した結果を別表-1に示す。また、調査結果の概要を以下にまとめる。

（1）CCF の防止対策と緩和対策

海外においても国内と同様に、デジタル安全保護回路を設ける場合には、ソフトウェア等のプログラマブルなロジックに起因する CCF を考慮した設備（以下、多様化設備という）が別に設けられている。すなわち、多重化されたデジタル安全保護回路に対しては、そのソフトウェアの健全性を確保するための V&V 等を実施することに加え、多様化設計によりその影響を緩和する設計がなされている。

（2）多様化対策の想定事象

多様化設備が代替する機能については、安全保護系が有する機能に比べ限定的であるのが一般的で、低頻度の DBA を除外している事例がある。

（3）多様化設備

①多様性の評価

多様性に関する解析評価を実施してその妥当性を確認している例がある。

補足）多様性に関する評価は、設計の多様性、設備の多様性、機能の多様性、人的な多様性、信号の多様性、論理の多様性等の観点から実施される。

補足）多様性に関する解析評価のため、D3（Diversity and Defence in Depth: 深層防護多様性）評価のガイダンス文書が発行されておりこれを適用している例がある。

②安全保護系内の多様化設計

CCF の対策としては、安全保護系内においても一定の多様化設計を実施し、更に CCF に対する脆弱性を評価して必要な多様化設備を追加として設ける事例がある。安全保護系内の多様化設計は機能的な（信号の）多様性等による事例がある。

補足）機能的な（信号の）多様化設計は、例えば、原子炉の出力異常を炉心の中性子束で検知して処理するものと、温度により検知して処理するもの等がある。

③安全保護系に追加する多様化設備

多くの事例で、デジタル安全保護回路とは別に、その安全保護機能を代替する多様化設備が設けられている。

a. 多様化設備の実現手段

海外における多様化設備も国内と同様にハードワイヤードの機構で構成されるものがあるが、近年、特に新設炉において、PLD（Programmable Logic Device：ハードウェア記述言語で設計され、実行段階では、従来型のソフトウェアで論理演算を行うのではなく、ハードウェア上に構成された論理回路で信号処理が行われるデジタル半導体素子）といった新たなデジタル技術を多様化設備に適用しようとする動きも見られる。

b. 多様化設備の設備グレード

多様化設備の設計グレードについては、安全保護回路より低位の設計グレードとなっている。

補足）米国においては、多様化設備は非安全系であるが強化品質を求められており、欧州では IEC のクラス2に相当する、各国の設計グレードによるものがある。

（4）組み込みデジタルデバイス（EDD）の適用

調査した範囲では、いわゆる EDD を積極的に活用しているプラントは見当たらなかった。計画中のプラントにおいて、EDD を適用する場合は検証を実施する、あるいは改めて申請するとしているプラントがある。

（5）コンピュータセキュリティとの関連

調査した範囲では、セキュリティ上の要件を、多様化設備の設計条件としているプラントは見当たらなかった。

（6）その他

過去には、安全保護系内で設備的な多様性を確保する設計（例えば異なる2種類の計算機を安全保護系内に適用する設計）もあった。また、SMR 等の特殊な炉型では、安全系内に異なる2種類の PLD を適用することを計画している例もある。

各プラントを調査した結果の詳細を、以下の表にまとめている。

別表１：概要調査結果　①～⑳

別表-1

安全保護系等共通原因故障(CCF)対策海外動向調査結果 各国プラントの CCF 対策一覧

各国プラントの CCF 対策について、概要を一覧表にまとめた。

CCF 対策の調査の結果、国による相違に加え、適用時期における差異も見られたことから、ここでは、以下に分類して示した。

1： 最新の多様化設計(DAS の概念確立以降：概ね 2000 年代以降に建設・設備更新がされた、又はされる予定のもの)

2： 過去における多様化設計(DAS の概念確立以前：概ね 2000 年までに認可を得て 2000 年代までに建設されたもの)

3： 特殊な事例(SMR 等の特殊な炉型のもの、及び廃炉になったため設備更新が実施されなかったもの等)

表中の記載項目及び記載内容は以下とした。

項目		記載内容
1	国	プラントが建設、又は計画されている国を記載
2	プラント	個別プラント名、又はプラントの型式を記載
3	安全保護系等デジタル化範囲	デジタル化範囲を分類して以下の通り記載。あわせて、デジタル化の主たる手段(μP、PLD)を示した ・安全保護系の一部をデジタル化 → ～の一部 ・安全保護系を全面デジタル化 → 全安全保護系デジタル*2 ・中央制御室の安全系手動操作を含めた全面デジタル化 → 全面デジタル*3
4	安全系内多様化*1	安全保護系内で実施されている多様化設計の内容を記載
5	追加多様化設備*1	安全保護系に追加して設置される多様化設備の内容を記載。あわせて多様化設備の主たる実現手段（ハードワイヤード、μP、PLD）を示した
6	多様化検討の想定事象	多様化設計を実施する際に考慮されたプラント事象を以下の通り記載。但し、追加多様化設備の有する機能は現実的な仮定のもとで対処できるための最小限の機能に限定されている。 ・過渡変化事象について考慮 → AOO ・発生頻度の比較的高い事故事象について考慮 → 高頻度 DBA ・全ての設計想定事故事象について考慮 → 全 DBA
7	追加多様化設備(DAS)の設計グレード	追加多様化設備(注)の設計グレードを、各国で適用されている安全設備の区分を考慮して以下の通り記載 ・クラス2又はこれに相当する設計グレード → 低位の安全区分 ・米国の定義による安全上重要な設備(非安全系)に相当するグレード → 強化品質の非安全系 注)一部のプラントでは安全保護系内のクラス2相当設備が多様化設備を兼ねる場合がある
8	詳細	詳細調査結果の対応する番号を記載

*1： 補足に多様化設計のイメージを示す　*2：自動作動系の部分をデジタル化する場合等(補足参照)　*3：自動作動系に加え手動操作系をデジタル化する場合等(補足参照)

1. 最新の多様化システム(DAS の概念確立以降:概ね 2000 年代以降に建設・設備更新がされる(された)もの

(1)稼働中

国	プラント	安全保護系等デジタル化範囲	安全系内多様化	追加多様化設備	多様化策検討の想定事象	追加多様化設備グレード	詳細
米国	Watts Bar (新設)*1	信号処理等の一部(μP)	機能多様化等*4	HW	全 AOO	低位の安全区分又は強化品質の非安全系	③
米国	Oconee (既設)*2	全安全保護系デジタル(μP)	ー	HW(一部μP)*5	全 AOO+全 DBA		⑧
ロシア	NVNPP-6/7 (新設)*3	全面デジタル(μP)	機能多様化等*4	HW	全 AOO+DBA(範囲不明)		⑨

*1:建設中断後 2016 年営業運転、 *2:2014 に設備更新完了し営業運転、 *3:2017 年営業運転、 *4:自動作動系の機能的な多様化、手動操作の一部を設備的に多様化する等
*5:工安系の DAS は HW、既設の ATWS 緩和設備は μP により実現

(2)建設中

国	プラント	安全保護系等デジタル化範囲	安全系内多様化	追加多様化設備	多様化策検討の想定事象	追加多様化設備グレード	詳細
米国	AP1000(Vogtle3/4)(新設)	全面デジタル(μP)	機能多様化等*1	デジタル(PLD)	全 AOO+全 DBA	低位の安全区分又は強化品質の非安全系	⑩
仏国	EPR(FL-3)(新設)	全面デジタル(μP)	機能多様化等*1	デジタル(μP)*2	全 AOO+高頻度 DBA		⑬
フィンランド	EPR(OL-3)(新設)	全面デジタル(μP)	機能多様化等*1	HW	全 AOO+高頻度 DBA		⑫
中国	ACPR-1000 (新設)	全面デジタル(μP)	機能多様化等*1	デジタル(PLD)	全 AOO+DBA(範囲不明)		⑭

*1: (1)*4 に同じ、 *2:低位の安全区分の安全系デジタル設備と共用、ATWS 緩和機能は別途(非安全系)、クラス2設備の品質が課題になった時に HBS(HW)を追加したが、その後不要とされている

(3)計画中

国	プラント	安全保護系等デジタル化範囲	安全系内多様化	追加多様化設備	多様化策検討の想定事象	追加多様化設備グレード	詳細
米国	US-ABWR (新設)	全面デジタル(μP)	機能多様化等*2	HW	全 AOO+全 DBA	低位の安全区分又は強化品質の非安全系	⑪
	US-EPR (新設)	全面デジタル(μP)	機能多様化等*2	未定	全 AOO+全 DBA		⑯
	US-APWR (新設)	全面デジタル(μP)	機能多様化等*2	HW (PLD も検討)	全 AOO+全 DBA		⑰
	APR-1400 (新設)	全面デジタル(μP)	機能多様化等*2	デジタル(PLD)	全 AOO+全 DBA		⑱
英国	UK-ABWR (新設)	全面デジタル(PLD)*1	機能多様化等*2	HW	全 AOO+高頻度 DBA		⑲

*1: GDA として基本承認を得ているが、FPGA(PLD の一種)適用に関連する検証等の事項は詳細設計段階の審査で取り扱うとされている。 *2: (1)*4 に同じ

2. 過去における多様化システム（DAS の概念確立以前：概ね 2000 年までに認可を得て 2000 年代までに建設されたもの）

（1）稼働中

国	プラント	安全保護系等デジタル化範囲	安全系内多様化	追加多様化設備	多様化策検討の想定事象	追加多様化設備グレード	詳細
カナダ	Darlington（新設）*1	全安全保護系デジタル（μP）	異なる計算機*6	―	全 AOO＋全 DBA	―	①
英国	Sizewell-B（新設）*2	全安全保護系デジタル（μP）	HW(一部機能）*6	―	全 AOO＋高頻度 DBA	―	②
仏国	P4/N4（新設）*3	全面デジタル（μP）	機能多様化等*7	デジタル（μP）	全 AOO	強化品質の非安全系	④
チェコ	Temelin-1/2（既設）*4	全安全保護系デジタル（μP）	機能多様化等*7	デジタル（μP）	全 AOO＋高頻度 DBA	―	⑤
韓国	Ulchin-5/6（新設）*5	全安全保護系デジタル（μP）	機能多様化等*7	デジタル（μP）	全 AOO	強化品質の非安全系	⑥

*1: 1990～1993 営業運転、 *2: 1995 営業運転、 *3:80～90 年代営業運転(N4 初号機が 1996)、 *4:建設中断後 2004 営業運転、 *5:2004～5 営業運転、
*6:設備的な多様性とあわせて機能的な多様性も実現、 *7:1.(1)*4 に同じ

（2）建設中断中

国	プラント	安全保護系等デジタル化範囲	安全系内多様化	追加多様化設備	多様化策検討の想定事象	追加多様化設備グレード	詳細
台湾	Lungmen-1/2（新設）	全面デジタル（μP）	機能多様化等*1	デジタル（μP）	全 AOO	―	⑦

*1: 1.(1)*4 に同じ

3. 特殊な事例

（1）新型炉

国	プラント	安全保護系等デジタル化範囲	安全系内多様化	追加多様化設備	多様化範囲(対応事象）	追加多様化設備グレード	詳細
米国	SMR(NuScale）（新設）	全面デジタル（PLD）	異なる PLD 適用	―	全 AOO＋全 DBA	―	⑳

（2）デジタル化更新計画中に廃炉の動向となったプラント

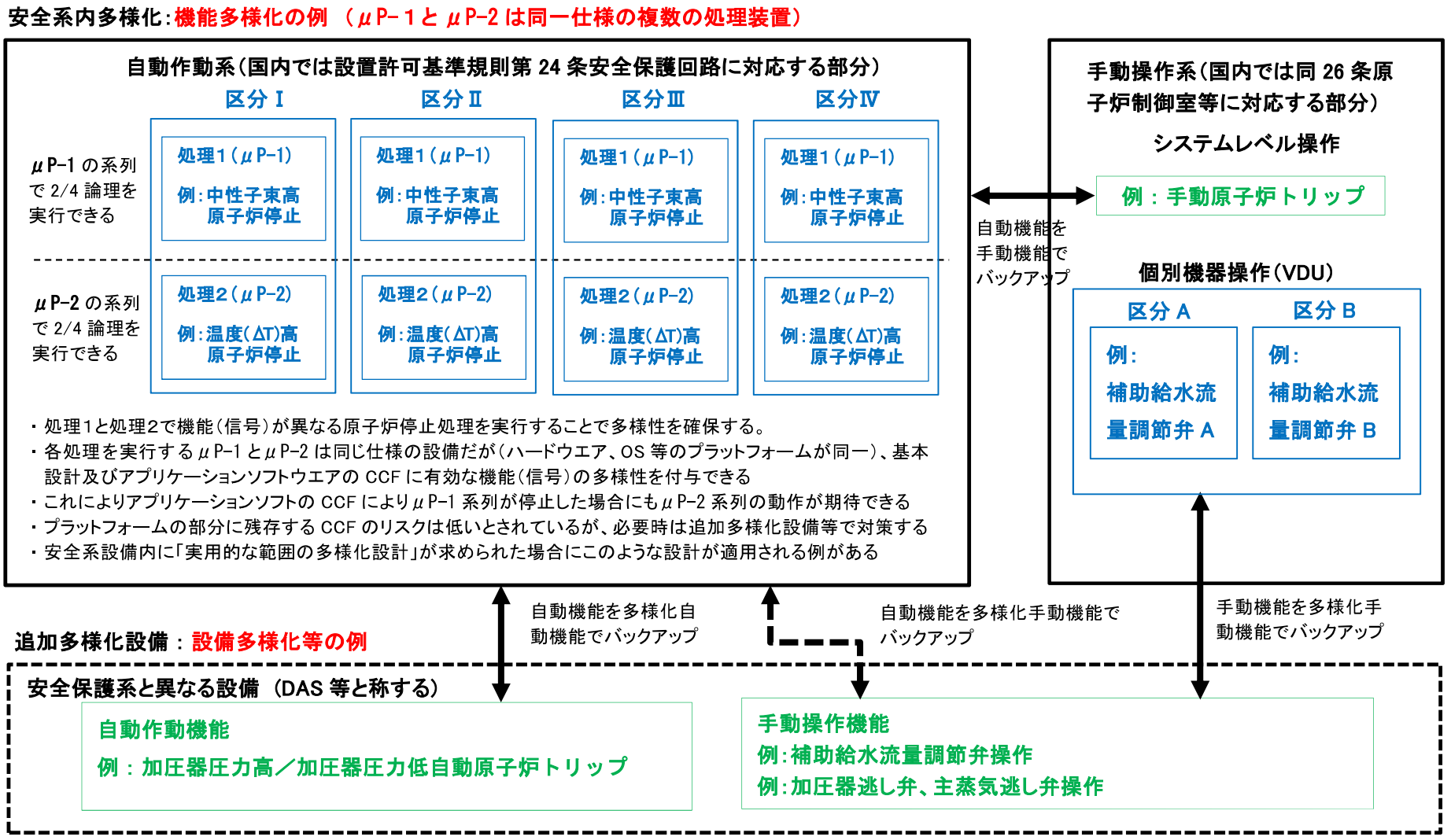
国	プラント	安全保護系等デジタル化範囲	安全系内多様化	追加多様化設備	多様化策検討の想定事象	追加多様化設備グレード	詳細
米国	Diablo Canyon （既設）	信号処理等の一部（μP）	PLD 適用	―*1	全 AOO＋全 DBA	―*1	⑮

*1:既設の ATWS 緩和設備は HW で強化品質の非安全系

【用語】

μP:マイクロプロセッサ方式のデジタル設備、 PLD:プログラマブルロジックデバイスによるデジタル設備、 HW:ハードワイヤードによる設備
DAS:多様化作動設備（Diverse Actuation System）

補足： 多様化設計のイメージ （PWR の原子炉停止機能の例）



青：プログラマブルな処理の部分（例えばマイクロプロセッサによる） 緑：青の部分に対して設備的な多様性を有する設備・機能（例えばハードウエア回路による）

注）本図は別表-1 に示す「安全系内多様化」と「追加多様化設備」のイメージを示すための例示であり、特定のプラント、あるいはシステムを示すものではない

参考８

IAEA Safety Standards

for protecting people and the environment

Design of Instrumentation and Control Systems for Nuclear Power Plants

Specific Safety Guide

No. SSG-39

IAEA
International Atomic Energy Agency

4.33. Analysis of the concepts of defence in depth and diversity is one method of performing the analysis described in para. 4.32. See para. 2.81.

4.34. If the analysis described in para. 4.32 determines that a postulated initiating event in combination with a common cause failure of a protection system results in unacceptable consequences, the design should be modified.

4.35. Complete elimination of all vulnerabilities of I&C systems and architecture to common cause failure is not achievable, but justification should be provided for the acceptance of any vulnerabilities identified.

Diversity

4.36. The IAEA Safety Glossary [6] defines 'diversity' as "The presence of two or more redundant systems or components to perform an identified function, where the different systems or components have different attributes so as to reduce the possibility of common cause failure, including common mode failure."

4.37. Diversity is a way of reducing vulnerability to common cause failures resulting from errors in requirements, design, manufacturing or maintenance, and of including conservatism to compensate for the difficulty of demonstrating the specified level of reliability.

4.38. Where diversity is credited as mitigating the effects of common cause failure in the protection system, justification should be provided that the diverse features actually achieve the mitigation of the effects of the common cause failure that is claimed.

4.39. When diverse I&C systems are provided, the diverse systems should not be subject to the same errors in specification, design, fabrication or maintenance.

4.40. Probabilistic studies[21] should not treat I&C items important to safety as fully independent[22] unless they are diverse and meet the recommendations for functional independence, electrical isolation, communications independence, environmental qualification, seismic qualification, electromagnetic qualification,

[21] Probabilistic studies include, for example, reliability analysis and probabilistic safety assessment.

[22] In probabilistic studies, systems are treated as fully independent by simply taking the product of their individual failure probabilities.

Annex III

AREAS WHERE PRACTICES OF MEMBER STATES DIFFER

INTRODUCTION

III–1. There are a number of areas where the academic bases or engineering practice supporting the design criteria for instrumentation and control (I&C) safety are not widely accepted by all Member States. This annex discusses areas where such differences were identified during the development of this Safety Guide. It may be expected that the practices of Member States will evolve over time.

RELIABILITY DETERMINATION FOR DIGITAL SYSTEMS

III–2. Software errors may lead to common cause failure in redundant digital systems if the same software is used in multiple redundancies. Thus, to estimate digital system reliability, it is necessary to estimate the probability of system failure due to hardware failure and, for some Member States, software error. For other Member States, design errors (including software errors) and their consequences are adequately treated only by qualitative analyses of the architecture and of the design.

III–3. Some Member States, when developing the I&C design basis, ensure consistency between the reliability requirements of the I&C systems and the probabilistic safety analysis by maintaining an explicit numerical reliability target for each I&C system important to safety. Consequently, these Member States consider numerical estimates of digital system reliability to be a necessary element for demonstration of reliability.

III–4. For Member States that apply numerical reliability to software, claims of high software reliability are not demonstrable at the present time. Hence, designs requiring a single computer based system to achieve a probability of failure on demand (pfd) lower than 10^{-4} for software need to be treated with caution.

III–5. Some regulatory bodies that make use of numerical reliability estimates for digital systems have established limits on the reliability levels that they consider to be justifiable for I&C systems. For example, reliability claims for any

— The consequences of a design basis accident do not exceed acceptable dose limits if a safety system fails.

Analytical approaches

III–10. In making determinations on consequences as part of the analysis described in para. 4.32, some regulatory bodies expect the use of conservative methods; others allow the use of best estimate methods. IAEA Safety Standards Series No. SSG-2, Deterministic Safety Analysis for Nuclear Power Plants [III–1] discusses conservative methods and best estimate analysis methods.

DIVERSE ACTUATION SYSTEMS

III–11. When digital systems are used to implement protection system functions, it is not uncommon for the analysis described in para. 4.32 to find that common cause failures within the digital protection system might result in unacceptable consequences for certain combinations of common cause failures and postulated initiating events. When this situation is encountered, a diverse actuation system is often provided to backup the protection system.

III–12. There is general agreement that a diverse actuation system may effectively mitigate the consequences of specific postulated initiating events in conjunction with a postulated common cause failure of a protection system. There are, however, different approaches to the safety classification, the use of digital diverse actuation systems to backup a digital protection system, and the use of manual actuation to mitigate the consequences of a common cause failure of the protection system.

Safety classification

III–13. Some regulatory bodies expect that diverse actuation systems will be classified as safety systems. Some regulatory bodies allow them to be systems in a lower safety class. Some regulatory bodies base the expected safety class upon the reliability claims made for the diverse actuation system.

Technology of the diverse actuation system

III–14. Some regulatory bodies expect that diverse actuation systems will be hardwired systems. Some regulatory bodies discourage, but do not prohibit,

the use of digital systems. Some regulatory bodies allow the use of digital systems if adequate diversity is demonstrated.

Use of manual actions for diverse actuation

III–15. Generally, manual actuation may be accepted as a diverse backup for the protection system but the conditions under which manual actuation may be credited vary. The range of accepted practices include the following:

— Manual action may be credited if the action is not needed in less than 30 min and human factors analysis has confirmed that a proper decision can be taken and implemented within that time;
— Manual action may be credited if the action is not needed in less than 20 min;
— Manual action may be credited for actuation of engineered safety features, but not for reactor trip;
— Manual action may be credited without restriction.

III–16. While the above illustrates the range of practices among regulatory bodies, a regulatory body may take a different approach based upon the specific situation proposed.

REFERENCE TO ANNEX III

[III–1] INTERNATIONAL ATOMIC ENERGY AGENCY, Deterministic Safety Analysis for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-2, IAEA, Vienna (2009).

参考９

○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の解釈（抜粋）

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	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の解釈
（安全保護回路） 第二十四条　発電用原子炉施設には、次に掲げるところにより、安全保護回路（安全施設に属するものに限る。以下この条において同じ。）を設けなければならない。	第２４条（安全保護回路）
一　運転時の異常な過渡変化が発生する場合において、その異常な状態を検知し、及び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とすること。	１　第１号について、安全保護回路の運転時の異常な過渡変化時の機能の具体例としては、原子炉の過出力状態や出力の急激な上昇を防止するために、異常な状態を検知し、原子炉停止系統を含む適切な系統を作動させ、緊急停止の動作を開始させること等をいう。
二　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。	
三　安全保護回路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、多重性を確保するものとすること。	２　第３号に規定する「チャンネル」とは、安全保護動作に必要な単一の信号を発生させるために必要な構成要素（抵抗器、コンデンサ、トランジスタ、スイッチ及び導線等）及びモジュール（内部連絡された構成要素の集合体）の配列であって、検出器から論理回路入口までをいう。
四　安全保護回路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ものとすること。	３　第４号に規定する「それぞれ互いに分離し」とは、独立性を有するようなチャンネル間の物理的分離及び電気的分離等をいう。
五　駆動源の喪失、系統の遮断その他の不利な状況が発生した場合においても、発電用原子炉施設をより安全な状態に移行する	４　第５号に規定する「駆動源の喪失、系統の遮断その他の不利な状況」とは、電力若しくは計装用空気の喪失又は何らかの原因

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ものとすること。	により安全保護回路の論理回路が遮断される等の状況をいう。なお、不利な状況には、環境条件も含むが、どのような状況を考慮するかは、個々の設計に応じて判断する。 5　第５号に規定する「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もの」とは、安全保護回路が単一故障した場合においても、発電用原子炉施設をより安全な状態に移行することにより、最終的に発電用原子炉施設が安全側の状態を維持するか、又は安全保護回路が単一故障してそのままの状態にとどまっても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をいう。
六　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ことができるものとすること。	6　第６号に規定する「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こと」とは、ハードウェアの物理的分離、機能的分離に加え、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等、承認されていない動作や変更を防ぐ設計のことをいう。
七　計測制御系統施設の一部を安全保護回路と共用する場合には、その安全保護機能を失わないよう、計測制御系統施設から機能的に分離されたものとすること。	7　第７号に規定する「安全保護機能を失わない」とは、接続された計測制御系統施設の機器又はチャンネルに単一故障、誤操作若しくは使用状態からの単一の取り外しが生じた場合においても、これにより悪影響を受けない部分の安全保護回路が第１号から第６号を満たすことをいう。

○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（抜粋）

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	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
（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。	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。
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	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

被害を防止するために必要な措置が講じられているものであること。 六　計測制御系の一部を安全保護装置と共用する場合には、その安全保護機能を失わないよう、計測制御系から機能的に分離されたものであること。 七　発電用原子炉の運転中に、その能力を確認するための必要な試験ができるものであること。 八　運転条件に応じて作動設定値を変更できるものであること。	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 4609-2008）本文及び解説－９に以下の要件を付したものによること。ただし、「ディジタル」は「デジタル」と読み替えること。 （１）JEAC4620の４．１の適用に当たっては、運転時の異常な過渡変化が生じる場合又は地震の発生等により原子炉の運転に支障が生じる場合において、原子炉停止系統及び工学的安全施設と併

	せて機能することにより、燃料許容損傷限界を超えないよう安全保護系の設定値を決定すること。 （２）JEAC4620の４．１８．３において検証及び妥当性確認の実施に際して作成された文書は、４．１８．２の構成管理計画の中に文書の保存を定め、適切に管理すること。 （３）JEAC4620の４．８における「想定される電源擾乱、電磁波等の外部からの外乱・ノイズの環境条件を考慮した設計とすること」を「想定される電源擾乱、サージ電圧、電磁波等の外部からの外乱・ノイズの環境条件を考慮して設計し、その設計による対策の妥当性が十分であることを確証すること」と読み替えること。 （４）JEAC4620の４．５及び解説－６の適用に当たっては、デジタル安全保護系は、試験時を除き、計測制御系からの情報を受けないこと。試験時に、計測制御系からの情報を受ける場合には、計測制御系の故障により、デジタル安全保護系が影響を受けないよう措置を講ずること。 　デジタル安全保護系及び計測制御系の伝送ラインを共用する場合、通信をつかさどる制御装置は発信側システムの装置とすること。 （５）JEAC4620の４．１６の「外部からの影響を防止し得る設計」を「外部影響の防止された設備」と読み替えること。 （６）JEAC4620の４．における安全保護機能に相応した高い信頼性を有するとは、デジタル安全保護系のトリップ失敗確率及び誤トリップする頻度を評価し、従来型のものと比較して同等以下

	とすること。また、デジタル安全保護系の信頼性評価において、ハードウェア構成要素に異常の検出、検出信号の伝送、入出力信号の処理、演算処理、トリップ信号の伝送、トリップの作動等、評価に必要な構成要素を含むこと。 （７）安全保護系に用いられるデジタル計算機の健全性を実証できない場合、安全保護機能の遂行を担保するための原理の異なる手段を別途用意すること。 （「日本電気協会「安全保護系へのディジタル計算機の適用に関する規程（JEAC 4620-2008）」及び「ディジタル安全保護系の検証及び妥当性確認に関する指針（JEAG 4609-2008）」に関する技術評価書」（平成２３年１月原子力安全・保安院、原子力安全基盤機構取りまとめ））

○発電用原子炉施設の工事計画に係る手続ガイド（抜粋）

２．工事の計画の認可及び届出手続きの範囲

（２）工事計画に記載すべき設備及び機器等の範囲

１）機器等の仕様に関する記載要求範囲

Ⅰ．制御方式及び制御方法

安全保護系にデジタル安全保護系を適用する場合には、デジタル安全保護系を適用することを記載することとする。なお、ここでいうデジタル安全保護系とは、安全保護系の論理演算機能（作動（起動）回路）がデジタル化されている設備をいう。

また「原子炉の制御方法」に、制御棒価値ミニマイザによる制御方法について記載すること。

Ｎ．中央制御室機能、中央制御室外原子炉停止機能、緊急時制御室操作機能及び緊急時対策所機能

技術基準規則に対応して具備することとしている機能を記載する必要がある。