資料２

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

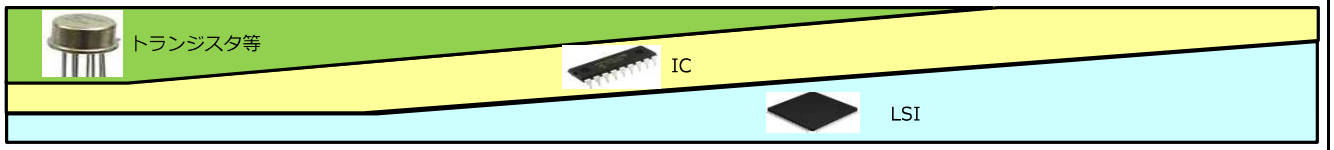
2019年10月30日
原子力エネルギー協議会

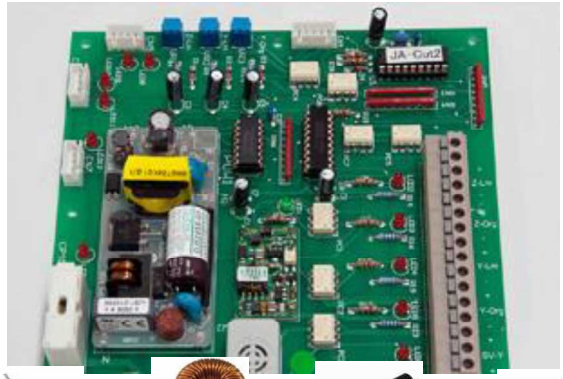
目 次

1．デジタル化する意味･目的

アナログ制御装置は、技術の進歩・変遷による部品の生産中止や製造者の減少による保守性の低下や拡張性の限界が課題になりつつあったことから、1980年代半ば以降、原子力分野への保守性向上を目的としてデジタル制御装置の適用を進めてきた。

【計測制御装置のデジタル化への変遷】

年　代	1970年代	1980 年代	1990 年代	2000 年代～
対象設備	アナログ制御装置 ⇨	デジタル制御装置 ⇨	デジタル安全保護回路	
主要構成部品	 部品形状の変遷			



抵抗　コイル　コンデンサ　トランジスタ…

デジタル化

マイクロプロセッサ

2．原子力施設に導入しているデジタル化技術

【原子力施設に導入してきたデジタル化技術】

・アナログ回路からの置換
・自己異常診断技術、保守ツールの導入

・多重化されたコントローラ

・監視・操作系へのVDU※の採用
・タッチオペレーションの採用
・光多重伝送の採用

・原子力利用を前提に開発・設計
　－シングルタスク処理（シンプルな構造）
　－定周期処理（シンプルな機能）
　－ソフトウェアのV&Vの実施
　－可視化言語の適用

【デジタル化の効果】

⇒ 保守性の向上

⇒ 運転信頼性の向上

⇒ 監視操作盤、ケーブル室等の省スペース化、プラント運転の支援拡大

⇒ ソフトウェア信頼性向上

安全保護回路への適用

※：VDU(Visual Display Unit)の略。フラットディスプレイ及び監視用画面を指す。

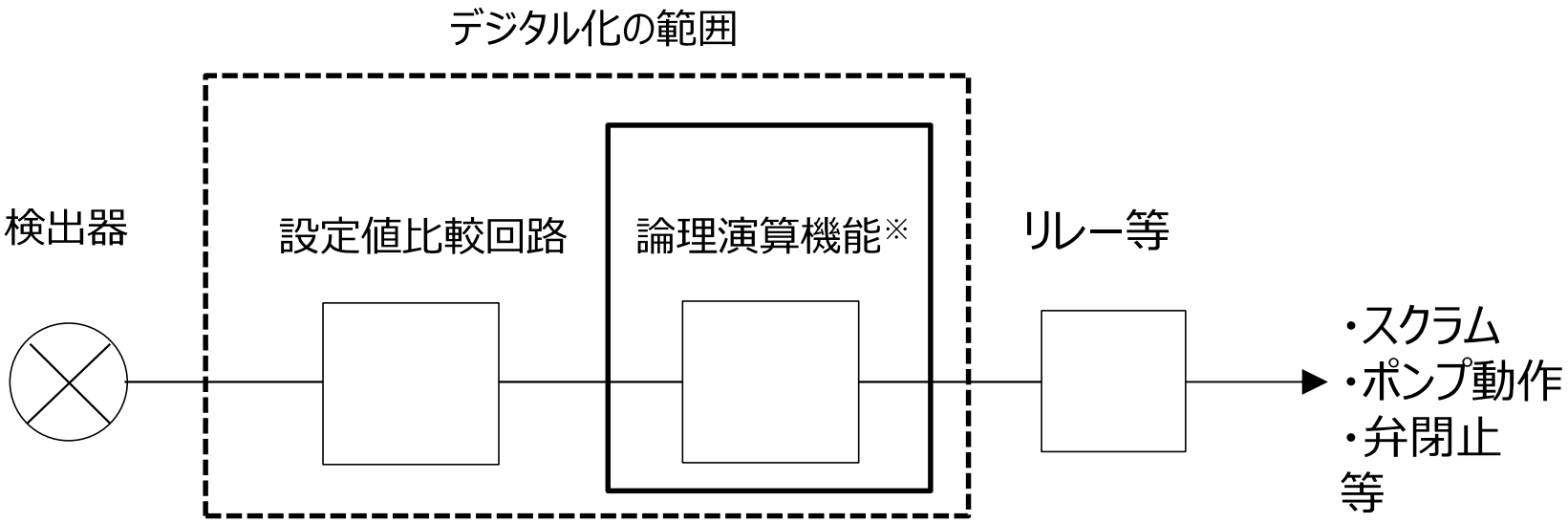
3．デジタル安全保護回路のデジタル化（1/2）

	PWR	BWR
当初からデジタル化されている原子力施設	泊３	柏崎刈羽6,7 浜岡５ 志賀２ 島根3 大間
既設設備（アナログ）をデジタル更新（計画含む）した原子力施設	高浜1, 2 ,3,4 大飯3,4 美浜３ 伊方3 川内1,2 玄海3,4 敦賀2	－

3．デジタル安全保護回路のデジタル化（2/2）

国内原子力施設における安全保護系のうち、デジタル化の範囲は、
設定値比較回路や論理演算機能の部分である。

自動作動系におけるデジタル化の範囲（例）



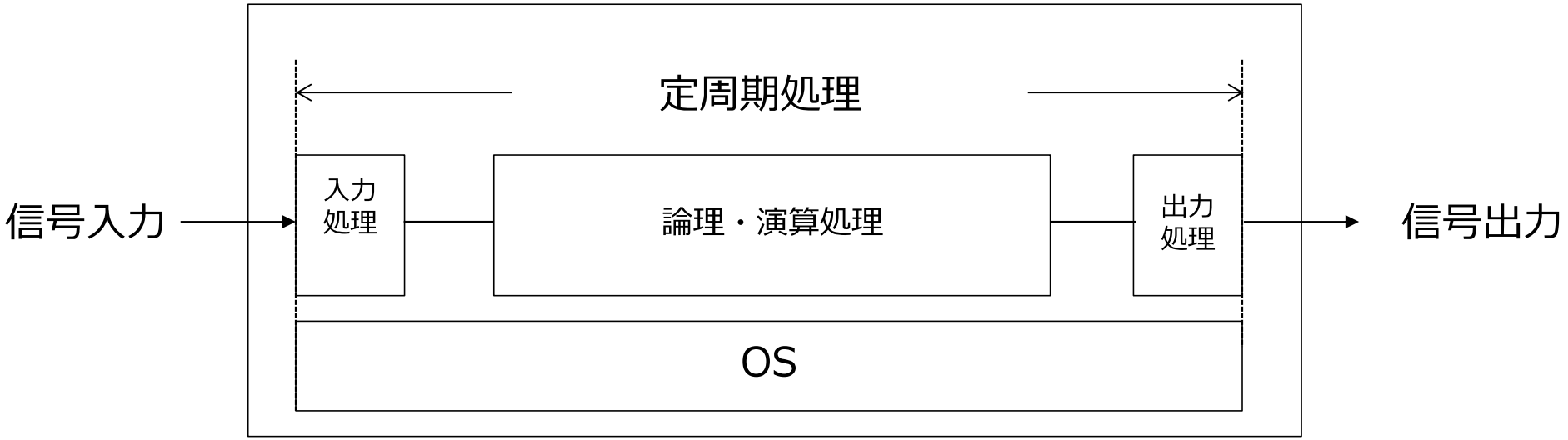
※：工認ガイドにおける安全保護回路の範囲

4．ソフトウェア信頼性向上に対する取組（1/2）

■ソフトウェアの信頼性確保としてのこれまでの取組み
・デジタル安全保護回路は，原子力施設で用いることを前提に開発・設計されており、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。

・OSは入力処理、論理・演算処理、出力処理までの動作を定周期で制御するシンプルな機能を有する。

ソフトウェア構造（例）



4．ソフトウェア信頼性向上に対する取組（2/2）

■ソフトウェアの信頼性確保としてのこれまでの取組み

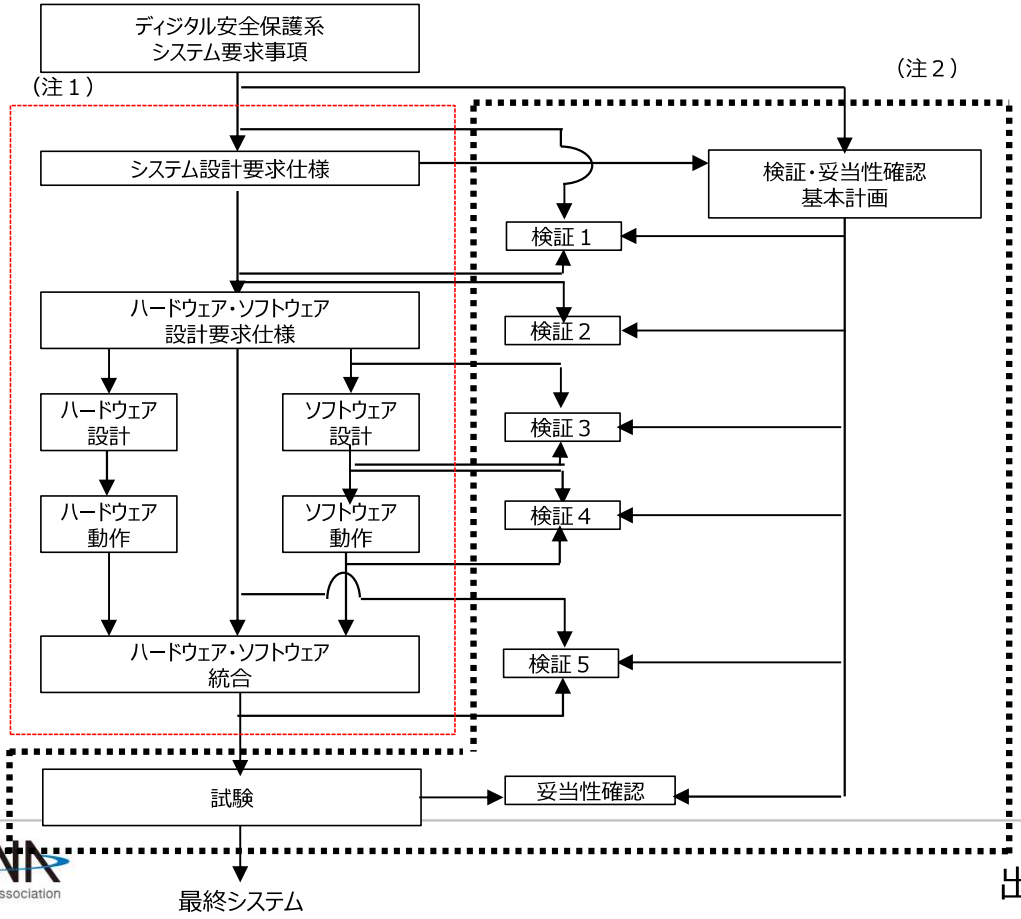
・デジタル安全保護回路は，JEAC4620／JEAG4609に基づき、ソフトウェアライフサイクル及び構成管理手法を含めた品質保証活動・検証及び妥当性確認（V&V）を実施している。

■これまで原子力施設に導入したソフトウェア起因の共通要因故障※実績

PWR/BWRともに、ソフトウェアに起因する共通要因故障（以下、「CCF」という）はこれまで発生していない

※：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動作による、多重化された制御装置の同時機能喪失

【デジタル安全保護回路のソフトウェアに対する検証及び妥当性確認の流れ】



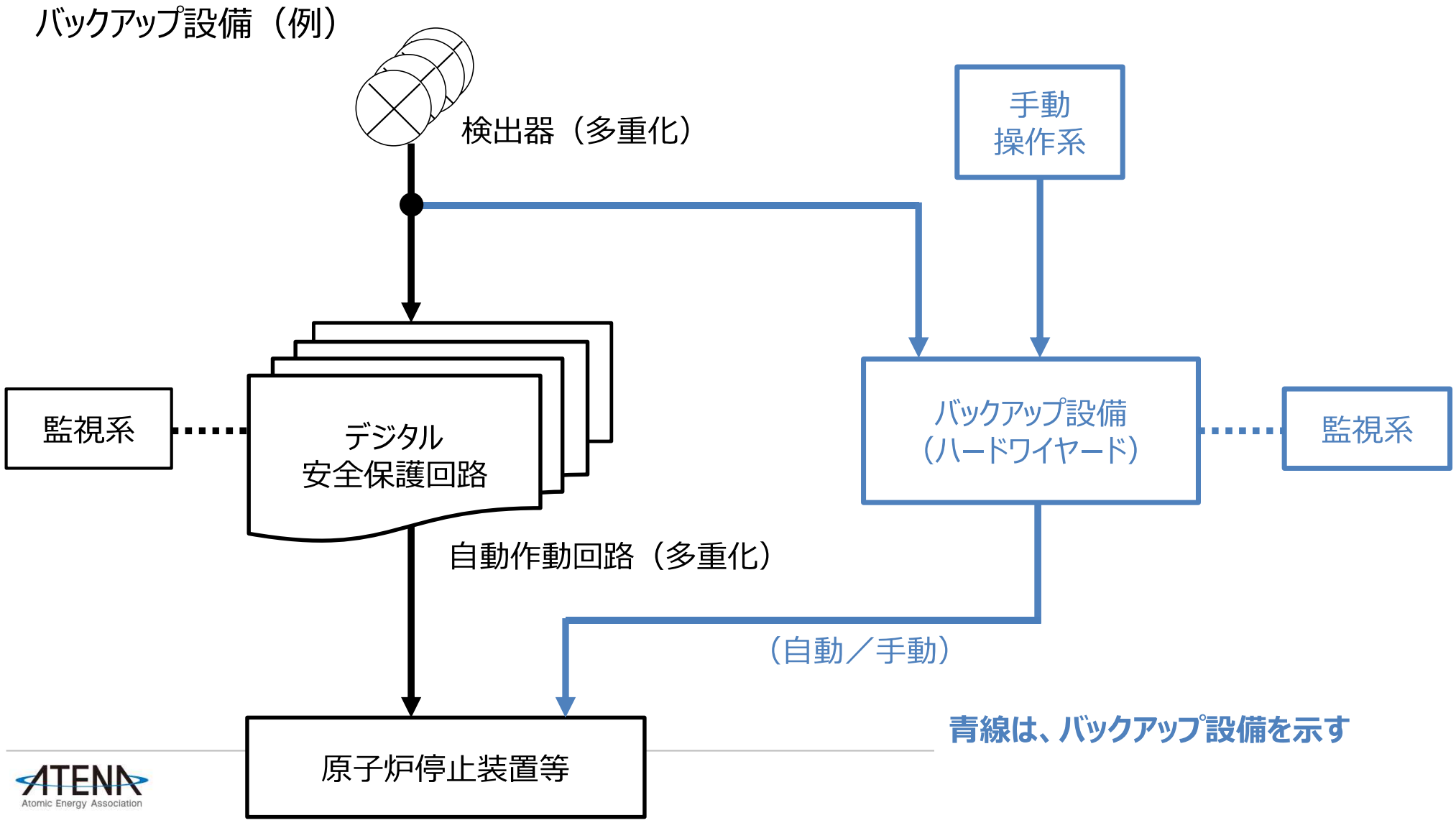
検証１・・システム設計基本仕様検証
検証２・・ハードウェア・ソフトウェア設計要求仕様検証
検証３・・ソフトウェア設計検証
検証４・・ソフトウェア製作検証
検証５・・ハードウェア・ソフトウェア統合検証

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

出典：JEAG4609

5．デジタル安全保護回路ソフトウェアCCFへの取り組み（1/2）

デジタル安全保護回路に搭載するソフトウェアは、設計・製造段階より信頼性を確保しているが、**<u>より一層の信頼性向上を目的として、自主的にバックアップ設備を設けてきた。</u>**



5．デジタル安全保護回路ソフトウェアCCFへの取り組み（2/2）

■バックアップ設備（例）

	自動作動系	操作系（手動）	監視系
ABWR	・原子炉スクラム※ ・原子炉再循環ポンプトリップ※	・原子炉スクラム ・主蒸気隔離弁閉止 ・主要な隔離弁閉止 ・高圧炉心注水系起動	・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

	自動作動系	操作系（手動）	監視系
PWR	・原子炉トリップ ・タービントリップ※ ・主給水隔離 ・補助給水起動※	・原子炉トリップ ・タービントリップ ・主給水隔離 ・補助給水隔離／流量調節 ・高圧注入系起動 ・格納容器隔離	・中間領域中性子束 ・加圧器圧力 ・１次冷却材圧力 ・１次冷却材低温側温度（広域） ・加圧器水位 ・主蒸気ライン圧力 ・蒸気発生器水位（狭域） ・格納容器圧力 ・蒸気発生器２次側放射線 ・対象補機の状態

※は、新規制基準施行後は、重大事故等対処設備として扱っている。

6． 現状バックアップ設備の設計の考え方、スペック

■バックアップ設備の設計（新規制基準適用後の現状仕様）

		ABWR	PWR
バックアップ設備（操作系（手動）、監視系）	安全重要度	常用系並みの設計	常用系並みの設計
	耐震性	Cクラス 但し、実力としては以下の通り 操作系：Ss機能維持 監視系：Ss機能維持（ドライウェル圧力、原子炉水位 以外）	Cクラス 但し、操作系はSs地震動による誤動作防止
	多重性	なし	なし
	耐環境性	事故時条件下で機能維持	事故時条件下で機能維持
	操作監視場所	中央制御室	中央制御室他
バックアップ設備（自動作動系）	安全重要度	重大事故等対処設備	重大事故等対処設備
	耐震性	Ｓｓ機能維持	Ｓｓ機能維持
	多重性	作動回路への信号（原子炉圧力、原子炉水位）を多重化	回路二重化（単一の回路の故障による誤動作防止）
	耐環境性	事故時条件下で機能維持	事故時条件下で機能維持
	設置場所	中央制御室	中央制御室他

7．デジタル安全保護回路でCCFが発生した場合の現状の対処

- デジタル安全保護回路で異常が発生し、装置の故障を示す警報が中央制御室に発報された場合には、警報の内容及び装置の状態を確認し、社内規定類に基づき必要な措置を実施するとともに、保安規定の運転上の制限に定める所要系統数を満足していないと判断した場合は、保安規定に定める措置を実施する。

- CCF対策も含めて、デジタル安全保護回路が全て作動不能となった場合には、バックアップ設備による原子炉トリップ、隔離弁閉止、高圧注入等を行う対応が可能である。

８．安全保護回路デジタル化の今後の見通し

【ABWR】
・安全保護回路はデジタル化されている。

【BWR5】
・安全保護回路はデジタル化されていない。
・現段階で安全保護回路のデジタル化の計画はない。

【PWR】
・安全保護回路のデジタル化を進めている。

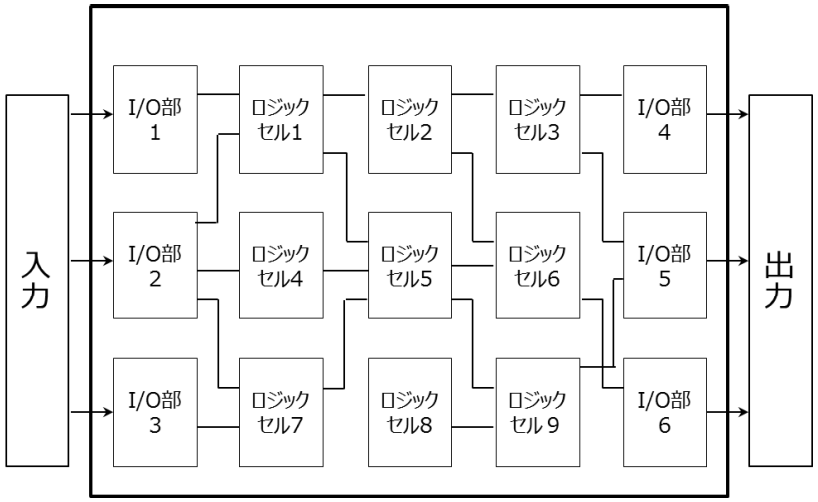
9．PLD等新たなデジタル機器・技術の実機適用の計画について

・FPGA ※1 等のPLD ※2は、マイクロプロセッサや通信コントローラ等のインターフェース回路において、信号変換装置の一部デバイスとして既に適用されている。（部品として扱っている）

・事業者として現状、デジタル安全保護回路をPLD等の新たな技術で実現する計画は無い。

・PLDはマイクロプロセッサとは異なる構造であるため、バックアップ設備に適用してマイクロプロセッサとの多様性を確保することができると考える。

PLD構成（例）



※１：FPGA：Field-Programmable Gate Array
　PLDの一種

※2：PLD： Programmable Logic Device
　マイクロプロセッサとは異なり、OS等のソフトウエアで動作するのではなく、I/O部、ロジックセル（論理・演算回路）の組み合わせや配線のデータを予め書き込むことにより、目的に応じた機能を実現することができる特徴がある。

・I/O部：外部との信号のやりとりを行う素子
・ロジックセル（論理・演算回路）：ANDやORのロジック回路

１０．基本方針（バックアップ設備義務化）に対する見解、検討にあたっての要望

１．これまで事業者が自主的に備えてきたCCF対策の規制化にあたっては、効果的に安全性を高める観点から、以下のような点について考慮が必要と考えている。

・CCF対策に関する規準は、デジタル技術の進展を踏まえ将来的にバックアップ設備をデジタル化する可能性や、アナログをはじめとした従来技術の衰退の可能性も踏まえ、実施方法の詳細（仕様規定）でなく、要求性能水準の規定（性能規定）を前提に検討が進められること

・性能については、これまでデジタル安全保護回路のソフトウェアが備えてきた高い信頼性や、設計想定事故を超える事象への対応としてATWS対策を重大事故等対処設備として備えてきた状況を踏まえ、安全上の重要度（例えば、CCFを含め、バックアップ機能を期待する想定起因事象の発生頻度等）を考慮した検討が進められること

・設備追加等の対策が必要な場合は、適切な経過措置期間が設けられること

２．原子力産業界としても、効果的に安全性を高めるために必要な、ソフトウェアCCF対策の性能及び当該性能を満たすための仕様について検討を進めるので、今後の会合を通じて意見交換を進めたい。