資料２－３

令和元年10月30日
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等に関する検討チーム
第１回会合時のご質問回答

2019年12月4日
原子力エネルギー協議会

第１回会合時のご質問内容

１．多様化設備がどのように接続されているのか具体的に示してほしい
（多様化設備の接続状況、安全保護回路の多重化等）

２．デジタル安全保護回路の異常検知について詳細を示してほしい
（自己診断機能と異常検知と警報の関係等）

１．多様化設備がどのように接続されているのか具体的に示してほしい
（多様化設備の接続状況、安全保護回路の多重化等）

のご回答

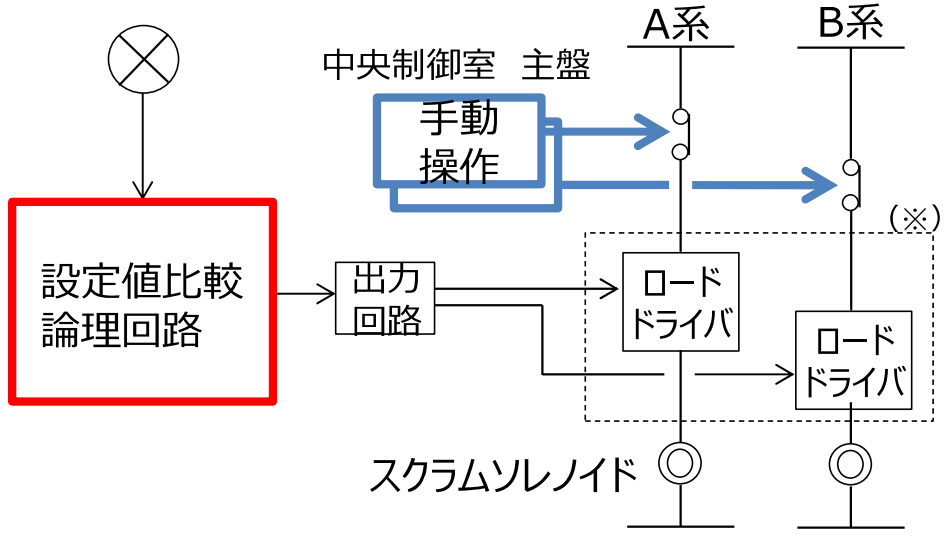
多様化設備の構成（1/4）

◎原子炉スクラム／トリップ

○ アイソレータ　デジタル安全保護回路　多様化設備

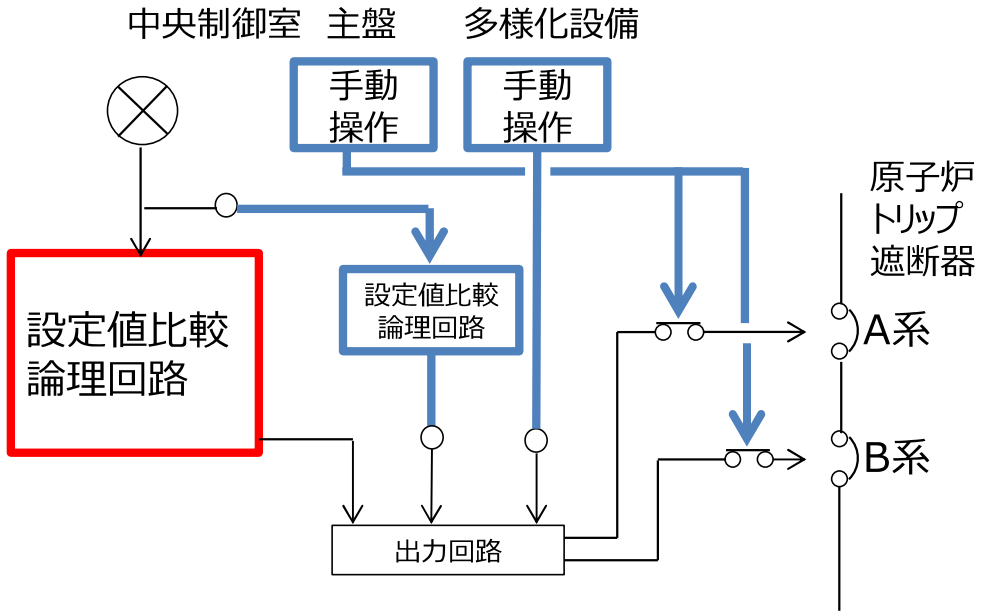
デジタル安全保護回路のソフトウェアを介さずに、中央制御室の主盤から手動でスクラム／トリップを作動させることが可能な設計としている（PWRの場合，多様化設備からの操作も可能）。
また、PWRについては、デジタル安全保護回路とは別に、多様化設備に自動トリップ回路を備え、自動で原子炉トリップを作動させることが可能な設計としている。

BWR



※：スクラムソレノイドA，B毎にロードドライバが４つずつ設けられており，
ハードワイヤード回路で２ out of 4論理を構成している。

PWR



多様化設備の構成（2/4）

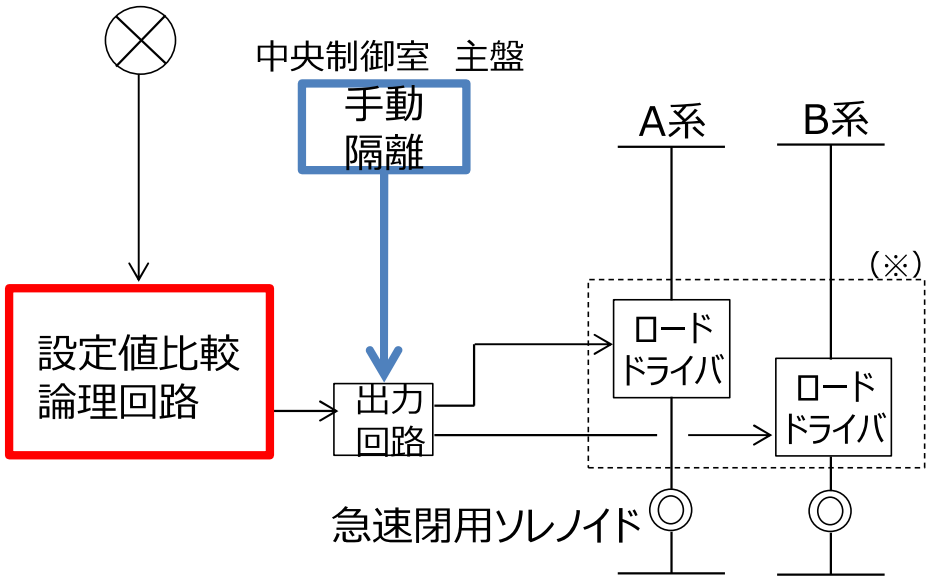
◎MSIV閉回路

○ アイソレータ　デジタル安全保護回路　多様化設備

デジタル安全保護回路のソフトウェアを介さずに、中央制御室の主盤で手動操作及び監視が可能な設計としている

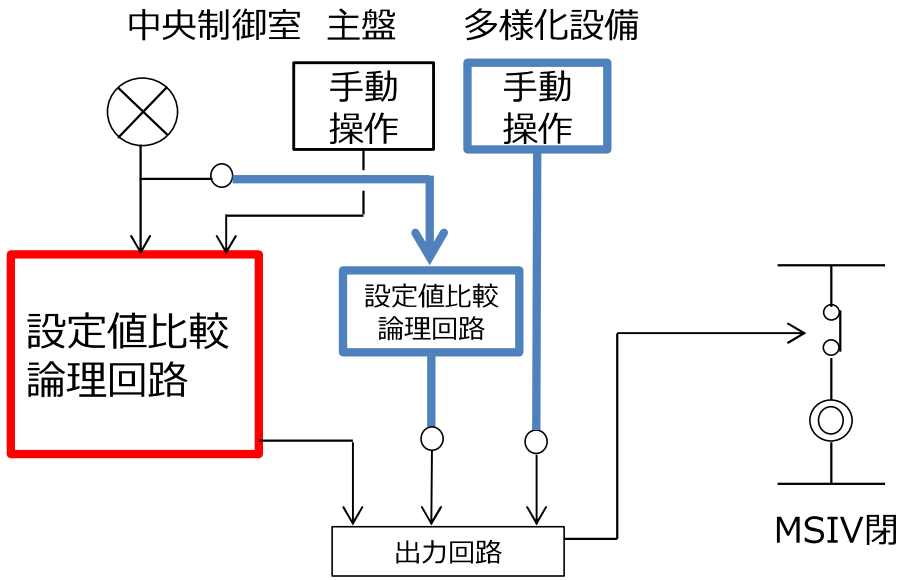
BWR

MSIVは外側隔離弁４弁，内側隔離弁４弁の計８弁あるが，以下には，代表して１弁分の回路を記載する。



※：ソレノイドA，B毎にロードドライバが４つずつ設けられており，ハードワイヤード回路で２ out of 4論理を構成している。

PWR



多様化設備の構成（3/4）

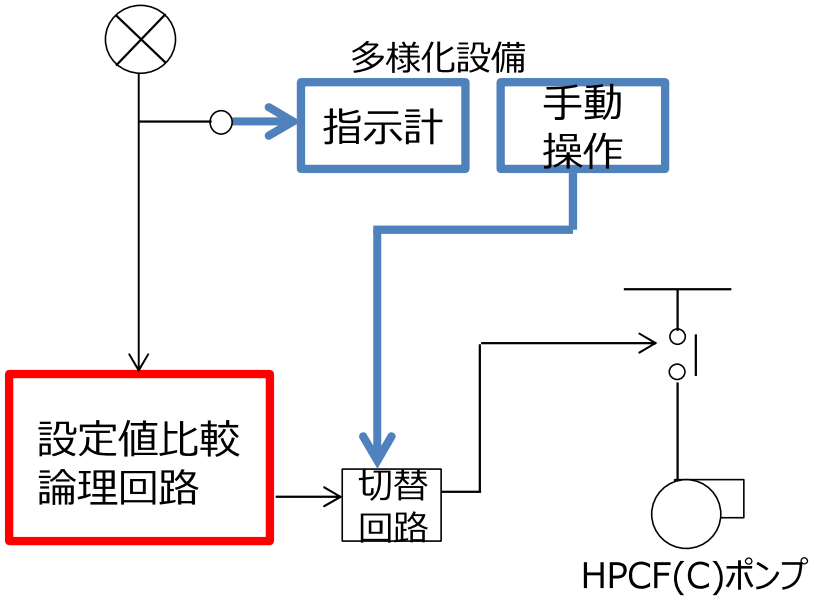
◎工学的安全施設作動

○ アイソレータ　デジタル安全保護回路　多様化設備

デジタル安全保護回路のソフトウェアを介さずに、中央制御室の主盤又は多様化設備から手動で安全系の設備を動作させる設計としている。

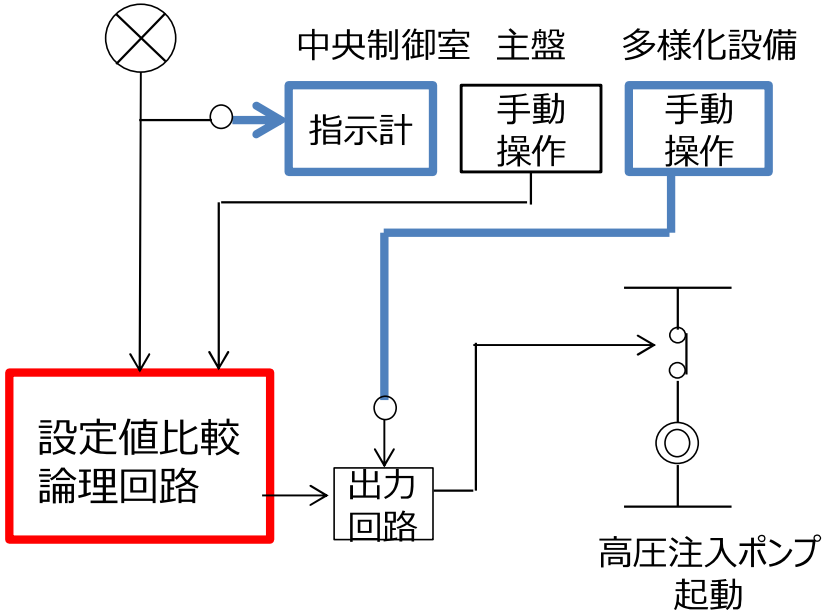
BWR

（例）HPCF(C) ポンプ起動回路



PWR

（例）高圧注入ポンプ

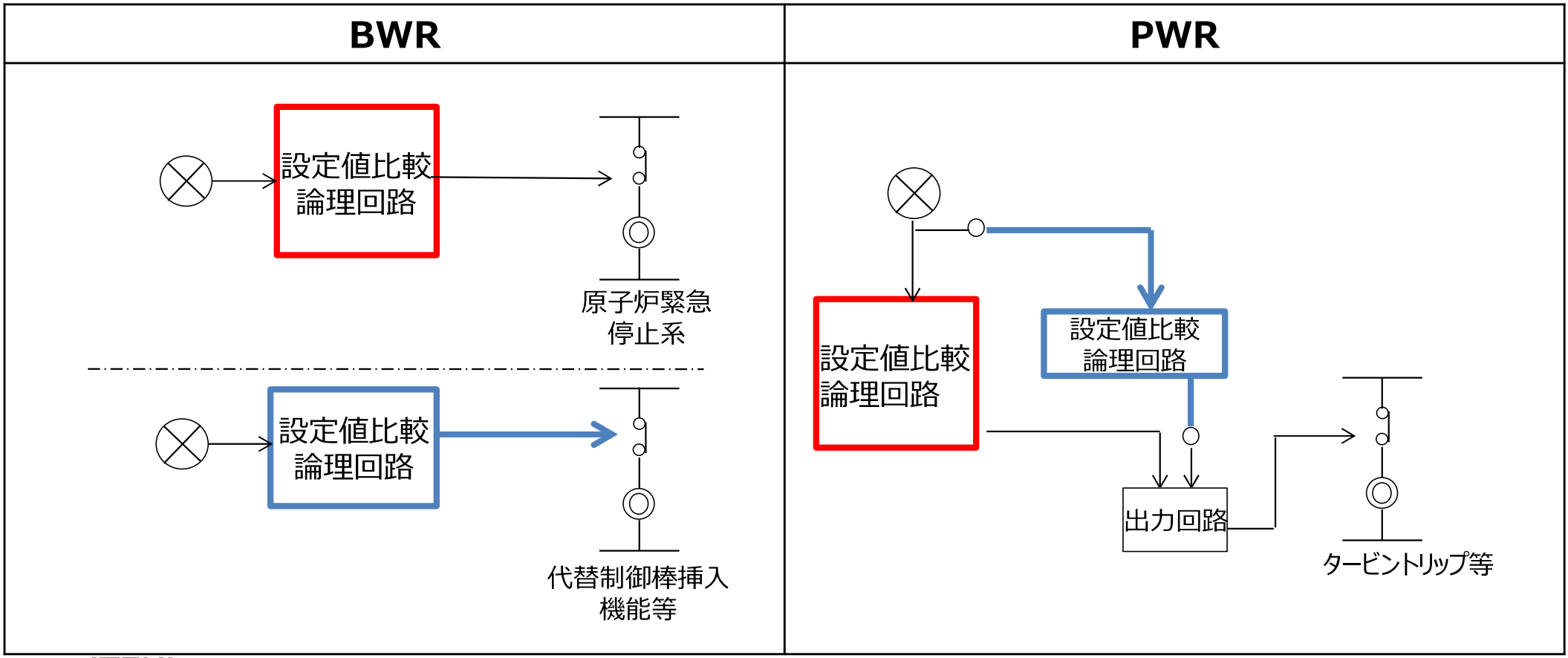


多様化設備の構成（4/4）

◎ATWS緩和設備

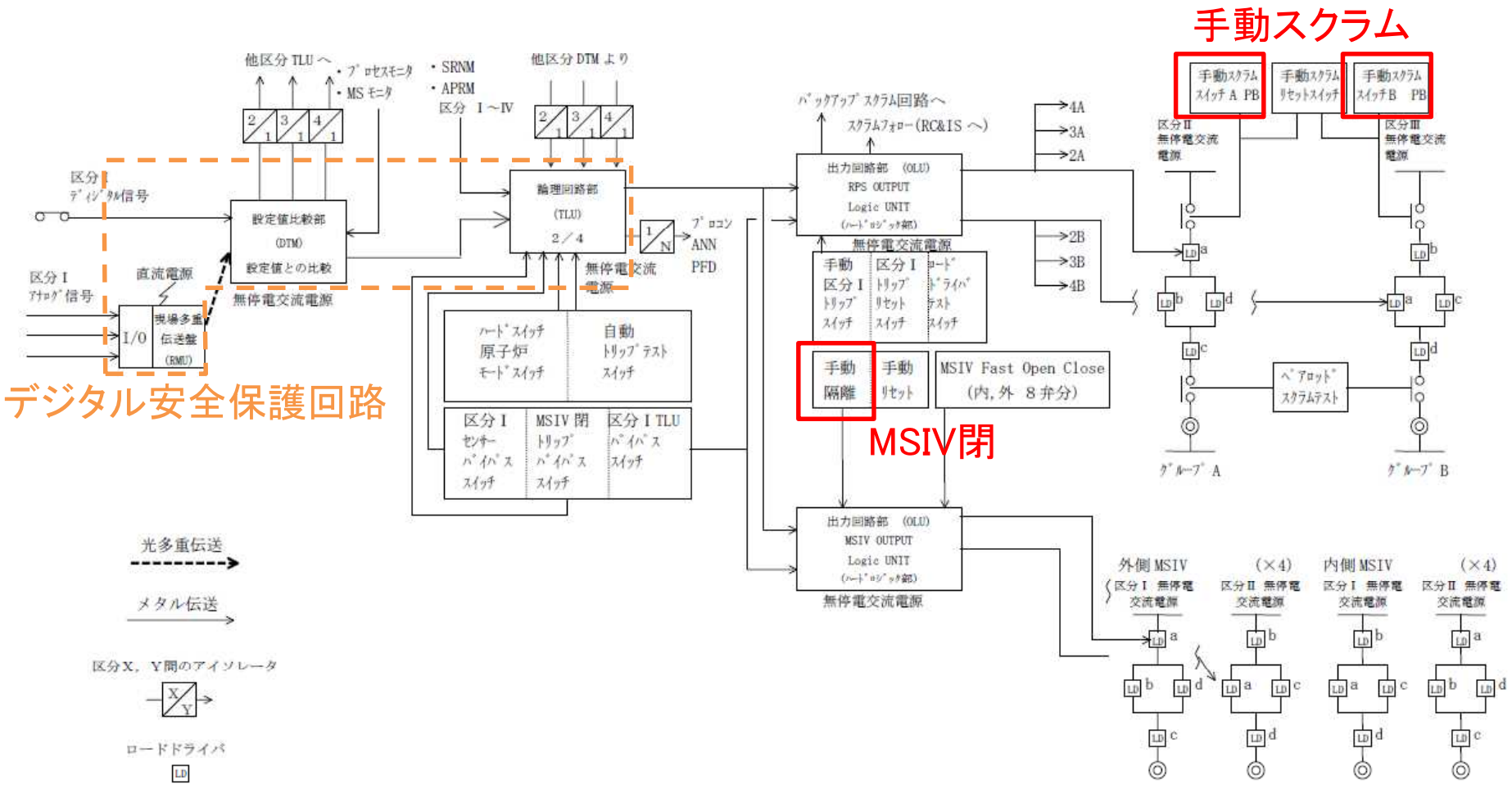
○ アイソレータ　デジタル安全保護回路　多様化設備

BWRの場合、AWTS緩和設備はデジタル安全保護回路から独立したアナログ回路で構成しており、自動で原子炉スクラム等を作動させる設計としている。
PWRの場合、デジタル安全保護回路のソフトウェアを介さずに、多様化設備にタービントリップ等の自動作動系を備え、安全系の設備を動作させる設計としている。



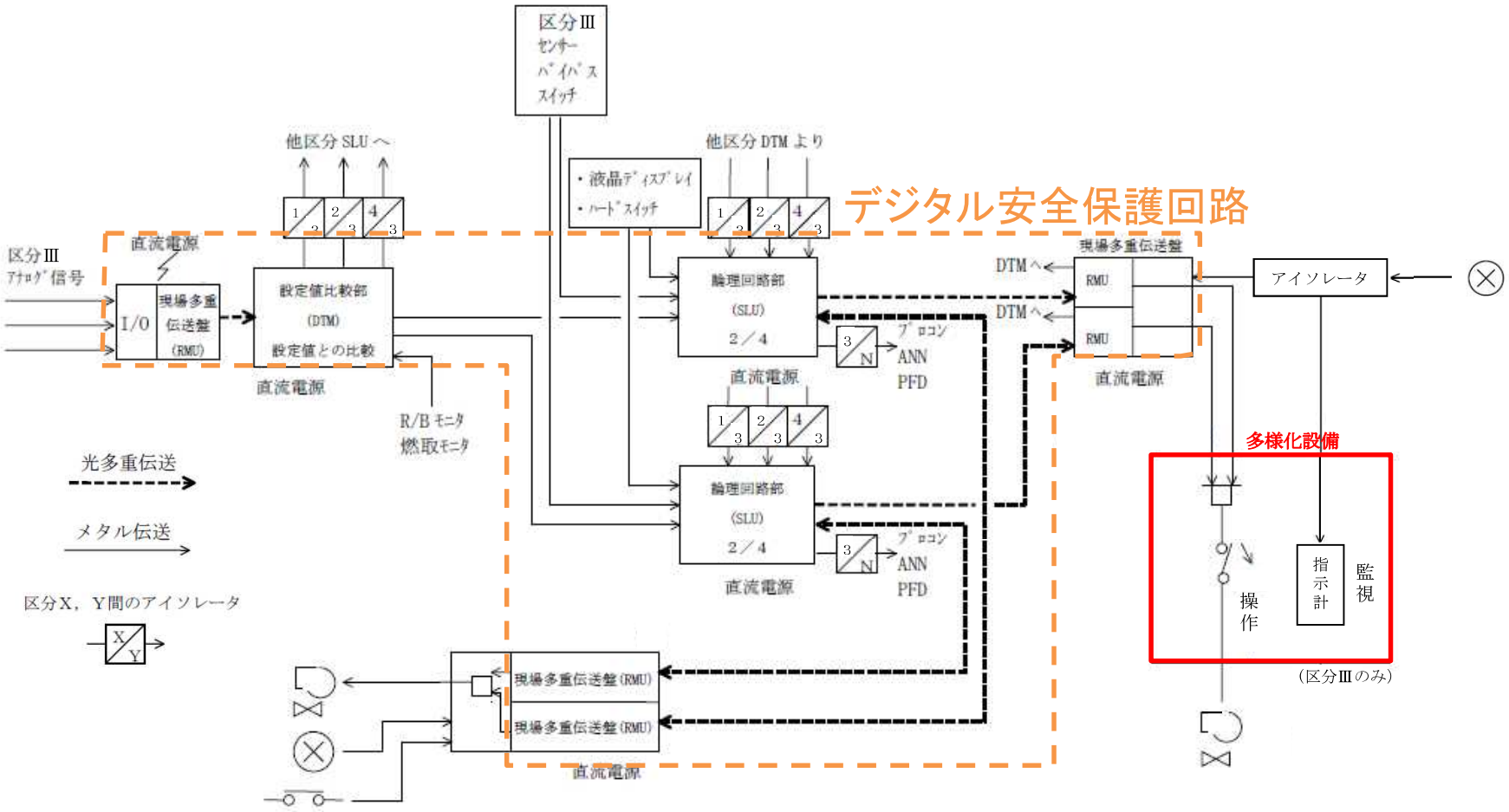
（参考）多様化設備の構成（ABWRの例）（1/6）

手動スクラム，MSIV閉回路：
デジタル安全保護回路のソフトウェアを介さない構成とし，中央制御室の主盤から安全系の回路を動作させることが可能な設計としている。



（参考）多様化設備の構成（ABWRの例）（2/6）

HPCF(C)手動起動回路他：
デジタル安全保護回路以外にも，中央制御室内の多様化設備で操作及び監視が可能な設計としている。

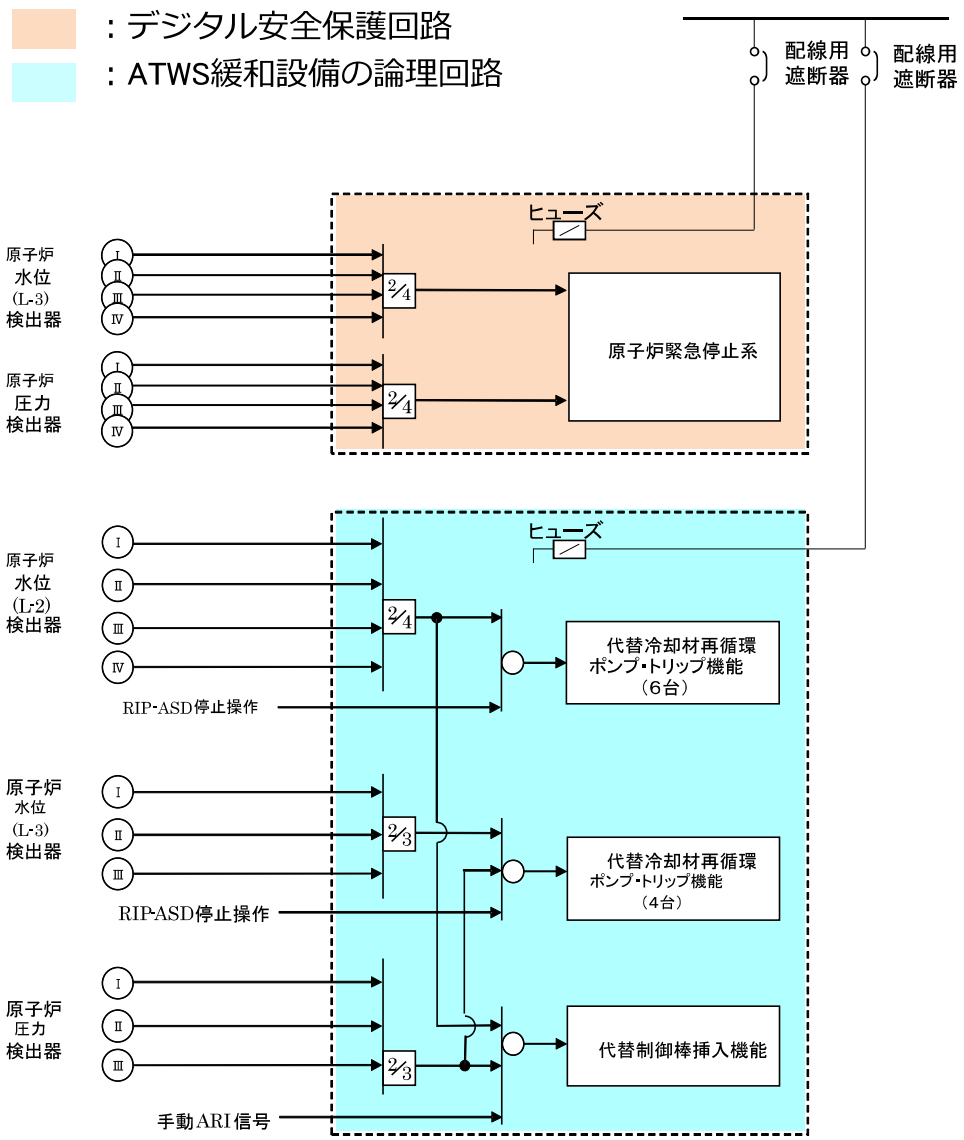


（参考）多様化設備の構成（ABWRの例）（3/6）

ATWS緩和設備：
ATWS緩和設備の論理回路はアナログ回路で構成されており，デジタル安全保護回路とは多様性を有する設計としている。

○電気的分離
ATWS緩和設備の電源は，遮断器又はヒューズによる電気的な分離をすることで，デジタル安全保護回路と同時に機能が損なわれない設計としている。

○物理的分離
ATWS緩和設備は，デジタル安全保護回路から独立した構成となっており，ATWS緩和設備が起因による火災によりデジタル安全保護回路に悪影響を及ぼさない設計としている。

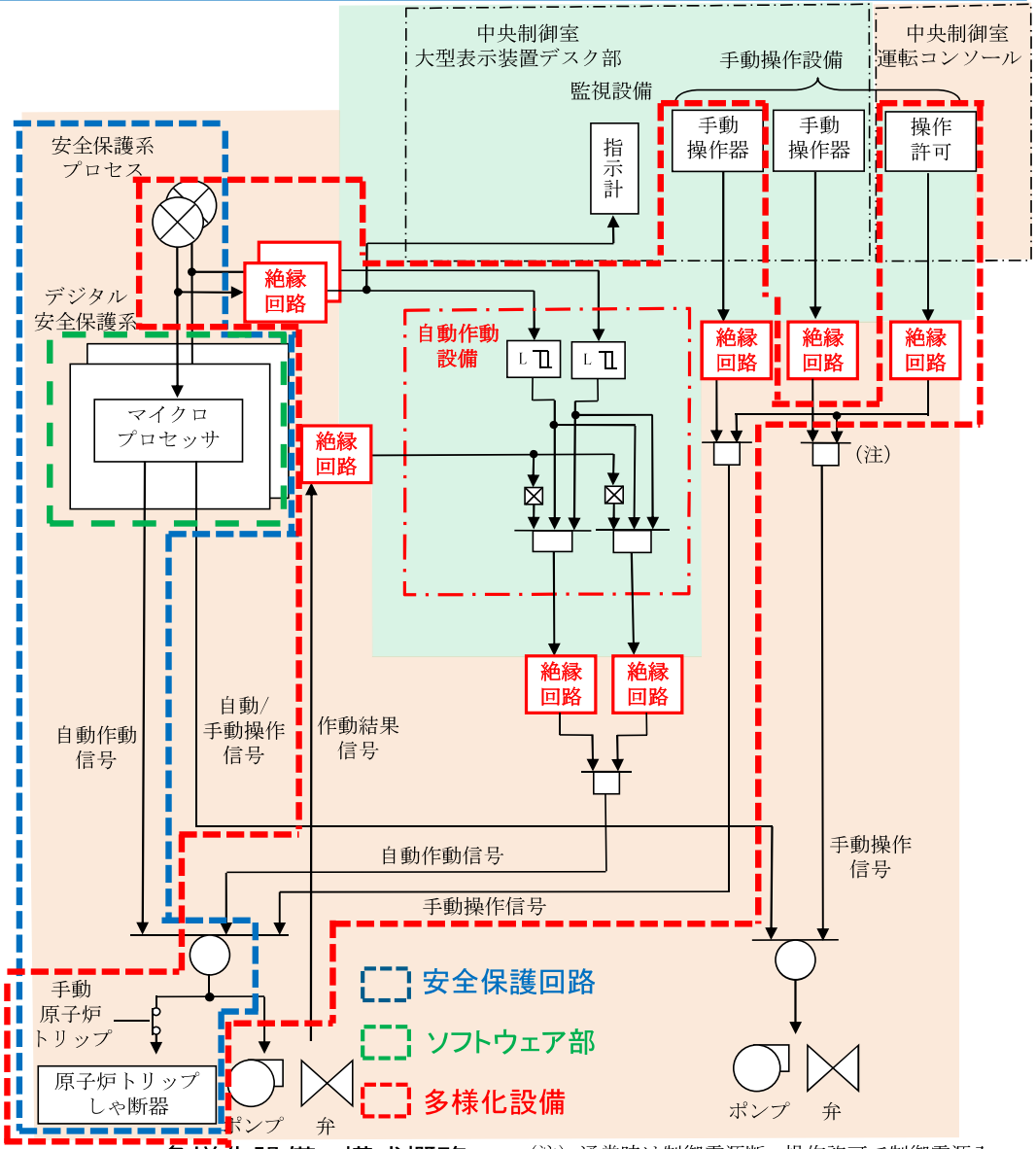


（参考）多様化設備の構成（PWRの例）（4/6）

原子炉トリップ：
デジタル安全保護回路のソフトウェアを介さない構成とし、多様化設備の自動作動設備から自動／中央制御室の主盤もしくは多様化設備から手動で原子炉トリップ遮断器を動作させることが可能な設計としている。

○電気的分離
多様化設備とデジタル安全保護回路の電気的分離を図る観点から、信号の取り合い部分には絶縁回路を設置している。右図に多様化設備の構成概略を示す。

○物理的分離
多様化設備とデジタル安全保護回路の物理的分離を図る観点から、多様化設備は安全系とは独立して設置している。

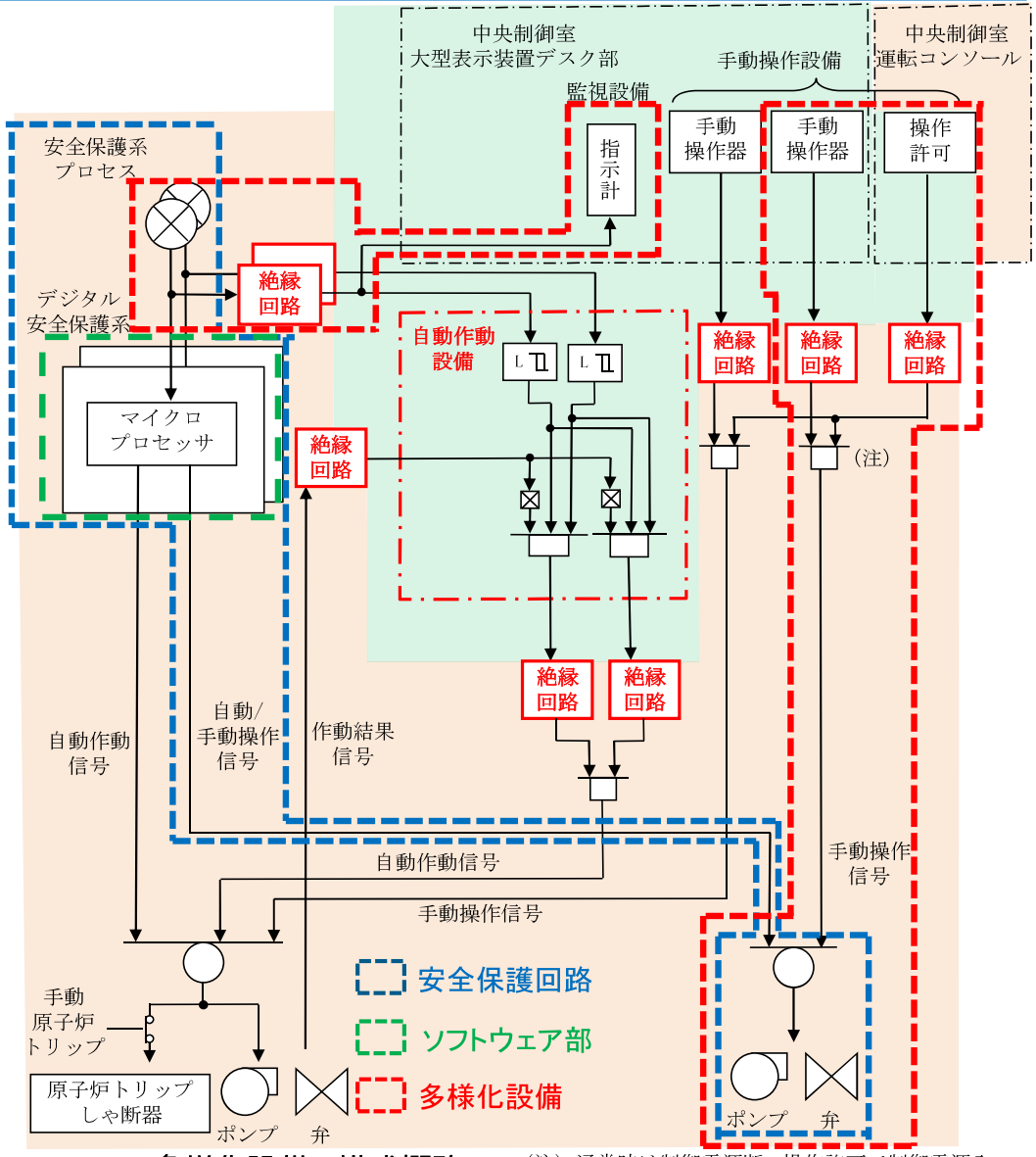


多様化設備の構成概略

（注）通常時は制御電源断。操作許可で制御電源入。

（参考）多様化設備の構成（PWRの例）（5/6）

工学的安全施設等の手動起動回路他：
デジタル安全保護回路のソフトウェアを介さない構成とし、中央制御室の多様化設備から手動で安全系の設備を動作させるとともに必要な監視が可能な設計としている。

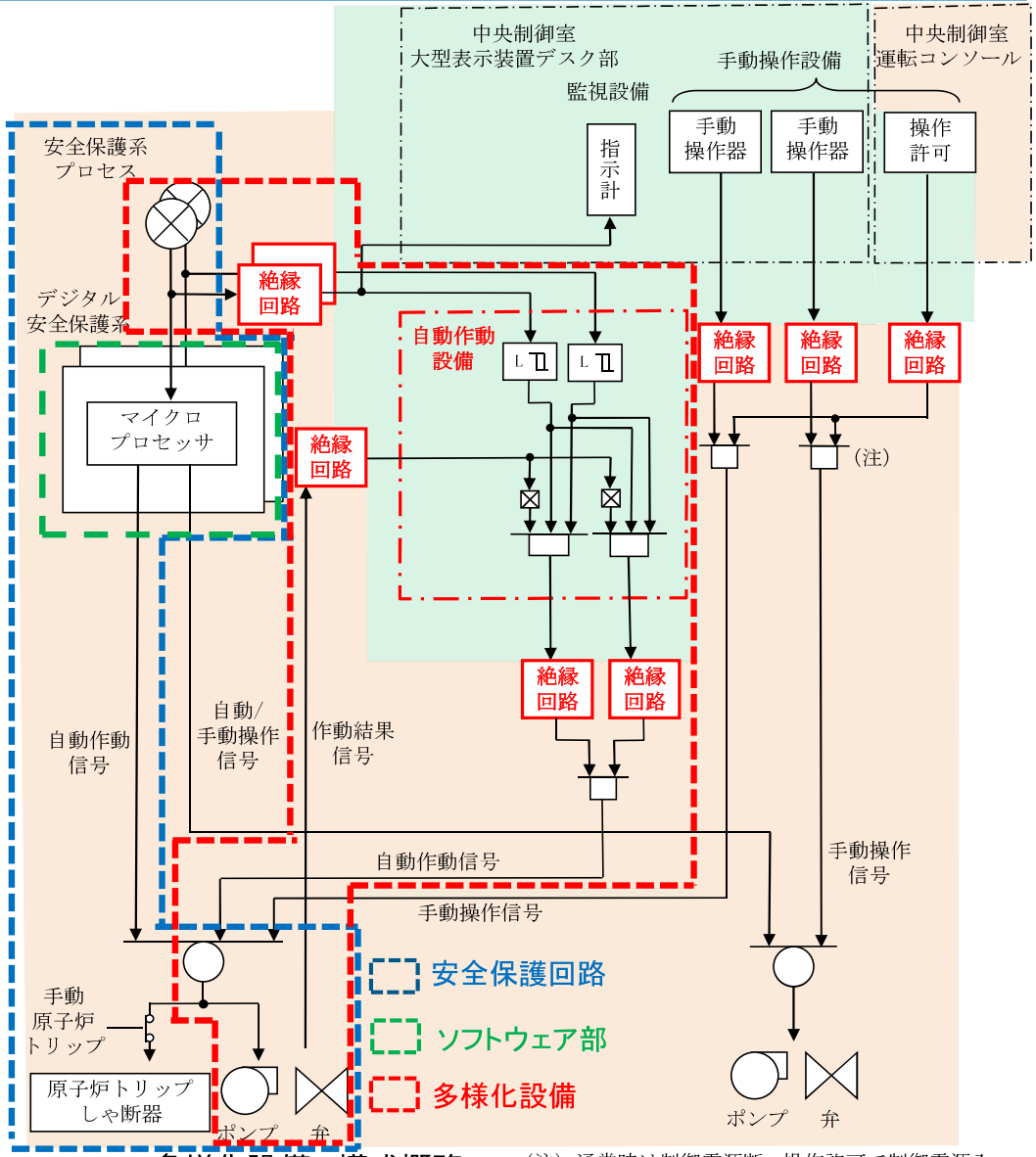


多様化設備の構成概略

（注）通常時は制御電源断。操作許可で制御電源入。

（参考）多様化設備の構成（PWRの例）（6/6）

ATWS緩和機能：
デジタル安全保護回路のソフトウェアを介さない構成とし、多様化設備の自動作動設備から安全系の設備を動作させる設計としている。



多様化設備の構成概略

（注）通常時は制御電源断。操作許可で制御電源入。

２．デジタル安全保護回路の異常検知について詳細を示してほしい（自己診断機能と異常検知と警報の関係等）

のご回答

自己診断機能と異常検知・警報との関係に関する説明（1/4）

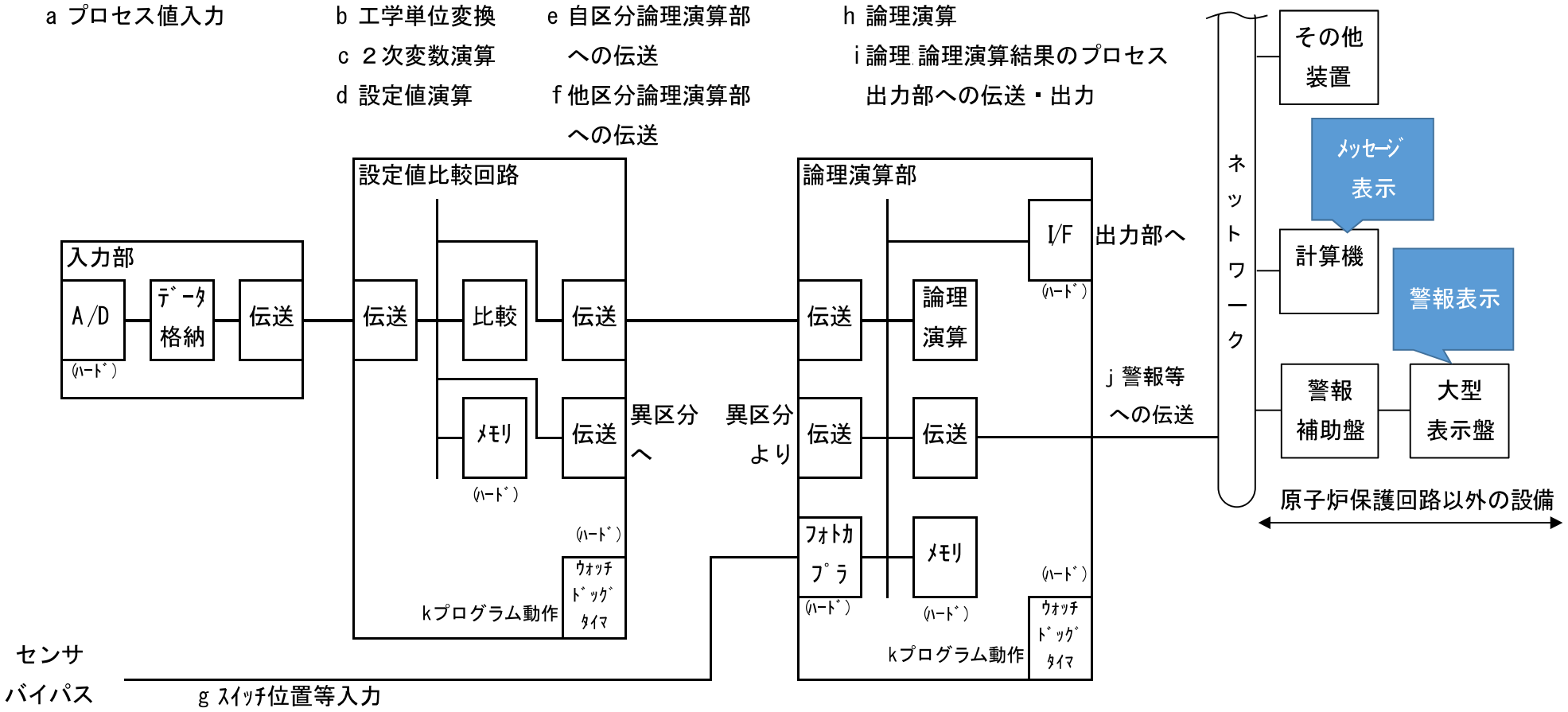
●「プロセス値入力～設定値比較～論理演算～出力」までの各機能に対して、故障モード分析に基づいた自己診断機能により、異常が発生した場合には警報を発報する機能を有している。

次頁以降に構成例と診断項目、診断対象、検出部、及び警報発生の有無について示す。

●自己診断は、異常発生個所と異なる正常な検出部で監視することから、中央制御室に警報として告知できる。警報設備に対する伝送異常が発生した場合でも、受信側設備で異常を検知し、警報等の発報により運転員は認知できる。

●自己診断機能及びV&V、工場試験、定期試験により、異常が未検出で残存する可能性は低いと考えられるが、想定外事象として「OS異常、コンパイラ異常等」時に自己診断が検出できない場合には、ソフトウェアCCFの可能性を否定できないものの、原子力以外の他分野を含む運用実績によりOS、コンパイラの信頼性は極めて高いと言えるので、ソフトウェアCCFとして残存するリスクは小さいと考える。

自己診断機能と異常検知・警報との関係に関する説明（2/4）



原子炉緊急停止系における構成（例）

自己診断機能と異常検知・警報との関係に関する説明（3/4）

【自己診断項目　例　（1/2）】

部位	機能	NO	項目	自己診断		運転員への告知	V&V/工場試験定期試験/保守	ソフトウェアCCFとしての異常が未検出で残存する可能性（×は無しを表す）	備考
				診断対象	検出部				
a	プロセス値入力	1	プロセス入力装置異常 (基板構成、ＡＩ/ＤＩ回路)	構成機器	ﾊｰﾄﾞｳｪｱ	○警報	○実施	× HW起因、自己診断可	
		2	入力上下限オーバ	入力信号	ｱﾌﾟﾘｹｰｼｮﾝ	○警報	○実施	× HW又はプロセス起因、 自己診断可	
		3	ＡＤコンバータの変換エラー （固着、特定ビットエラー）	ADｺﾝﾊﾞｰﾀ	ﾊｰﾄﾞｳｪｱ	○警報	○実施	× HW起因、自己診断可	
b	工学単位変換	4	変換式・定数 プログラムエラー	－	－	△ 指示値,プロセス警報により異常認知	○実施	× 試験で検出可	
		5	制御命令チェック （異常制御命令チェック）	ＣＰＵ	ＯＳ	○警報	○実施	× 自己診断、試験で検出可	
		6	ＣＰＵゼロ割発生	ｱﾌﾟﾘｹｰｼｮﾝ	ＯＳ	○警報	○実施	× 自己診断、試験で検出可	
		7	結果保存・読出異常 （メモリチェック）	メモリ	ﾊｰﾄﾞｳｪｱ	○警報	○実施	× HW起因、自己診断可	
c	2次変数演算		4,5,6,7による						
d	設定値演算		4,5,6,7による						
e	自区分論理演算部への伝送	8	データ化け	伝送信号	ＯＳ	○警報	○実施	× 自己診断、試験で検出可	
		9	伝送停止	伝送信号	ＯＳ	○警報	○実施	× 自己診断、試験で検出可	
		10	データ更新異常	伝送信号	ＯＳ	○警報	○実施	× 自己診断、試験で検出可	

自己診断機能と異常検知・警報との関係に関する説明（4/4）

【自己診断項目　例　（2/2）】

部位	機能	NO	項目	自己診断		運転員への告知	V&V/工場試験定期試験/保守	ソフトウェアCCFとしての異常が未検出で残存する可能性（×は無しを表す）	備考
				診断対象	検出部				
f	他区分論理演算部への伝送		8,9,10による						
g	スイッチ位置等入力		1による						
h	論理判定		4,5,6,7による						
i	論理判定結果のプロセス出力部への伝送・出力		伝送：8,9,10による						
		11	プロセス出力装置異常(基板構成、ＡＯ/ＤＯ回路)	構成機器	ﾊｰﾄﾞｳｪｱ	○警報	○実施	× HW起因、自己診断可	注1）
j	警報等への伝送		伝送：8,9,10による						
k	プログラム動作								
	周期動作	12	ウォッチドッグタイマ	ＯＳ ｱﾌﾟﾘｹｰｼｮﾝ	ﾊｰﾄﾞｳｪｱ ＯＳ	○警報	○実施	× 自己診断可	注2）
	ＣＰＵ異常	13	ＣＰＵ命令チェック	ＣＰＵ	ＯＳ	○警報	○実施	× HW起因、自己診断可	
	想定外動作（ＯＳ異常、コンパイラ異常等含む）	14	アドレス範囲チェック ウォッチドッグタイマ	ｱﾌﾟﾘｹｰｼｮﾝ	ＯＳ	○警報	○実施	× 自己診断可	
			上記で検出できない場合	－	－	△ 指示値,プロセス警報により異常認知	－	△ 試験で未検出の場合 残存の可能性あるが他分野を含めた採用実績等により残存するリスクは小さいと考える	

注1）Fail Safe動作が必要なものは伝送や出力装置異常の場合ソフトウェアによらず安全側に動作する。
注2）これらの異常の場合、Fail Safe動作が必要な機能については、ソフトウェアによらず安全側に動作する。