# 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（案）

## 2019年11月21日
## 原子力エネルギー協議会

# 第1回会合時のご質問内容

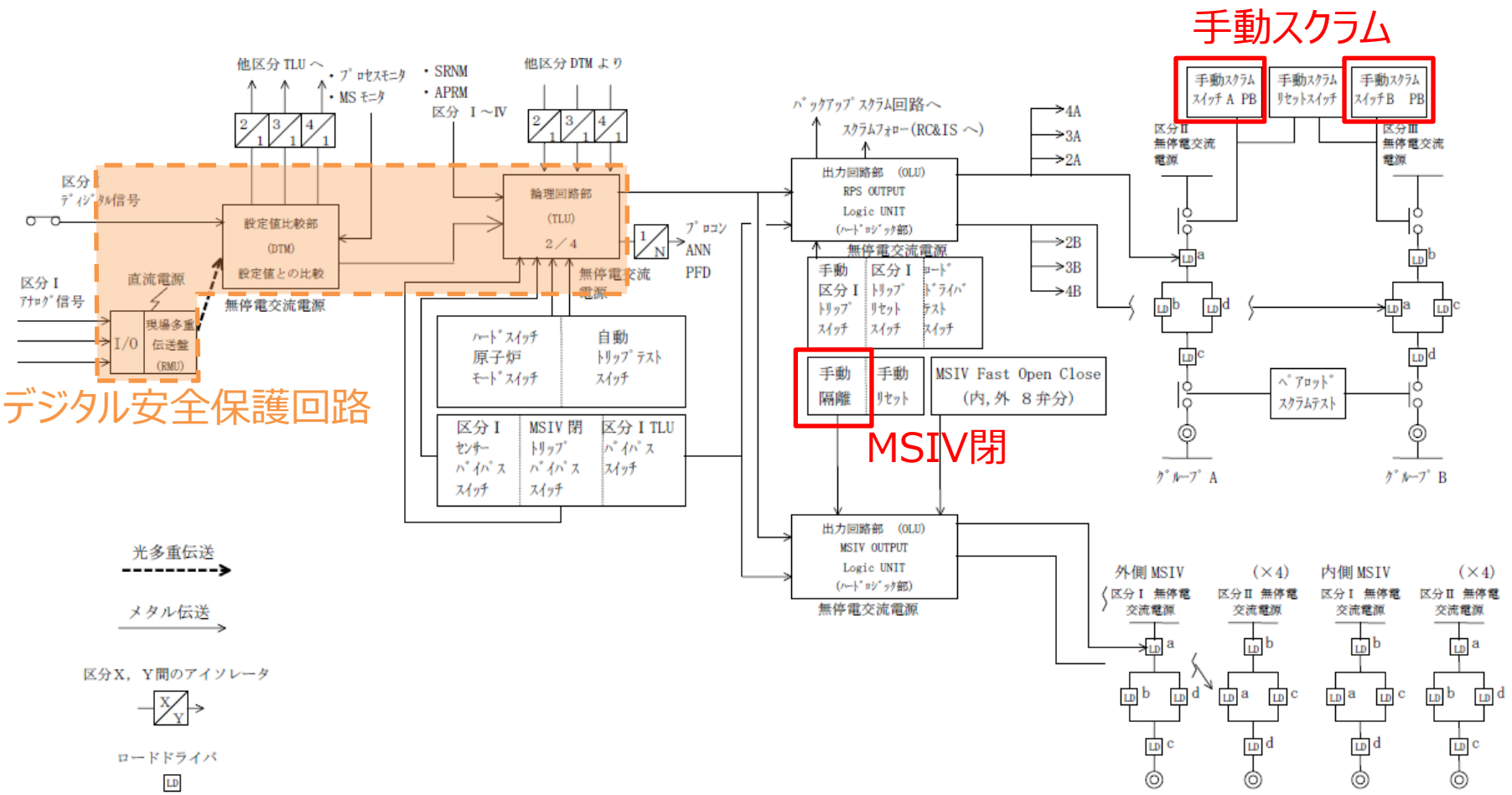


①自主的なバックアップ設備の構成・配置等について
⇒ **今回説明**

②デジタル安全保護回路の故障の検知に関する設計等について
⇒ **今回説明**

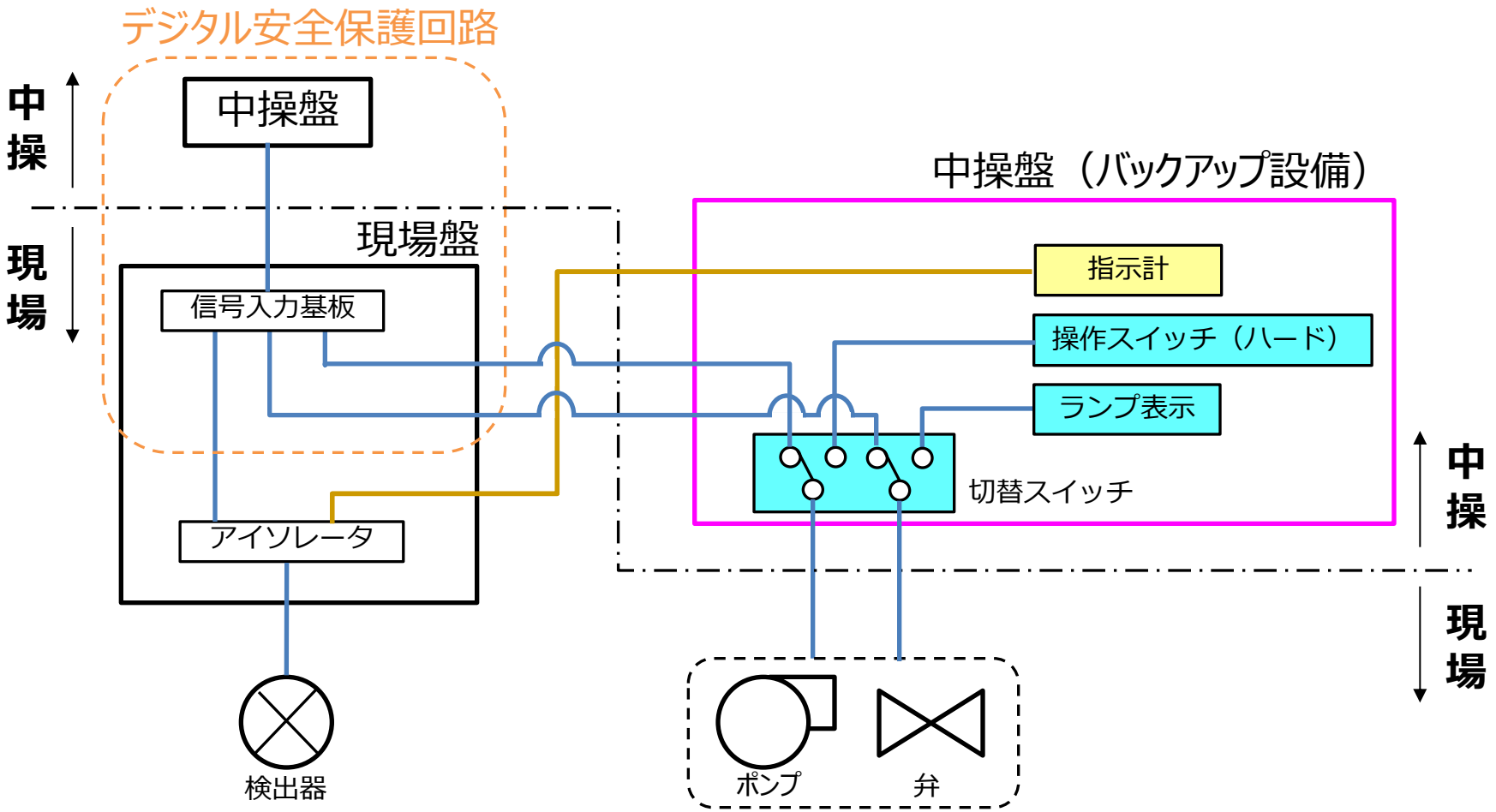
# バックアップ設備の構成（ABWRの例）（１／３）

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。



# バックアップ設備の構成（ABWRの例）（２／３）

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

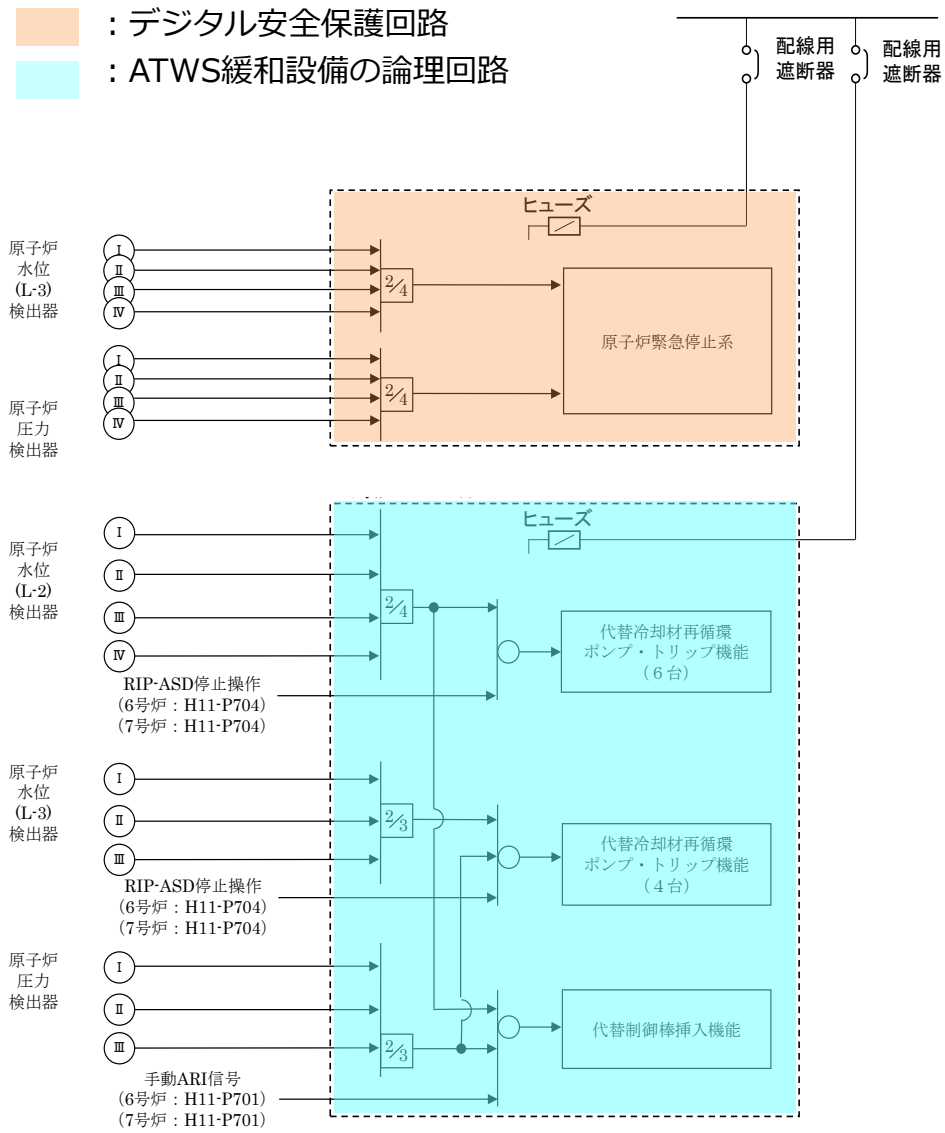


# バックアップ設備の構成（ABWRの例）（３／３）

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。



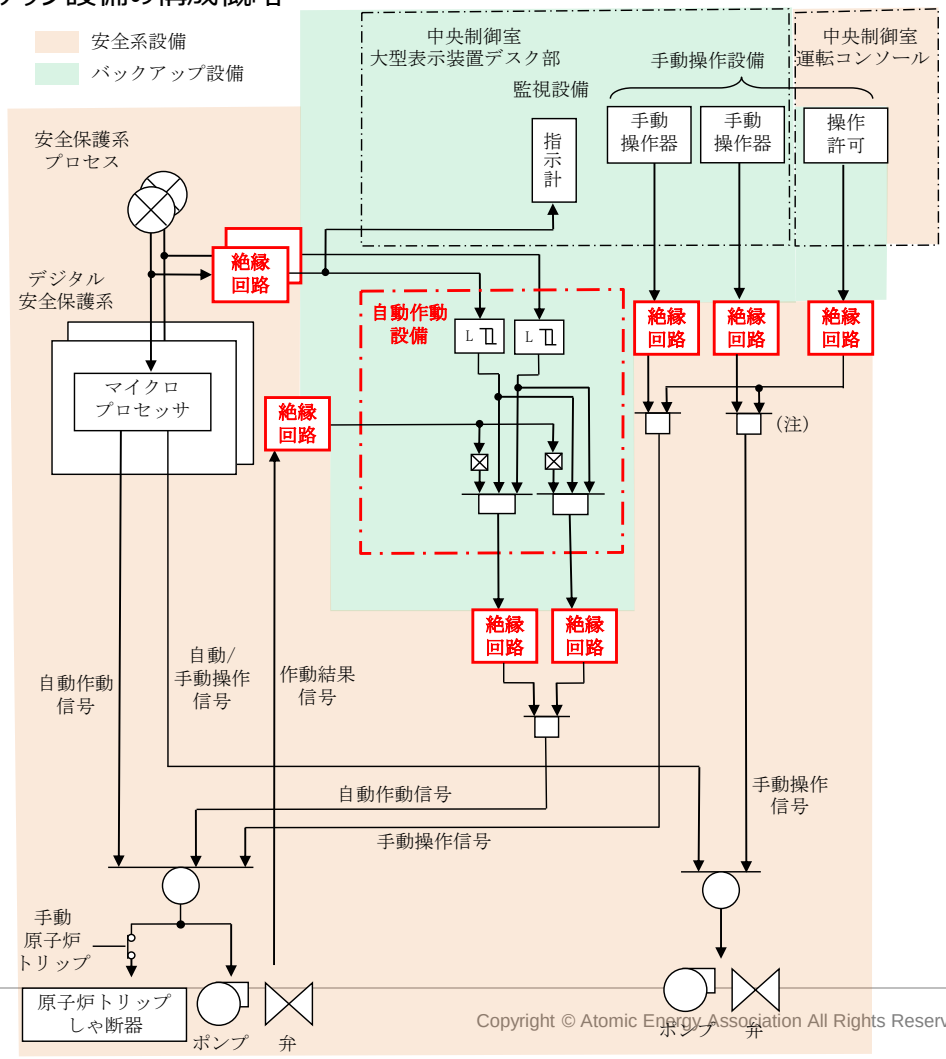
# バックアップ設備の構成（PWRの例）

バックアップ設備は、デジタル安全保護回路に対して多様性を持つ設備とし、十分な品質、信頼性及び実績を考慮して、従来のアナログ安全保護回路と同様のハードウェアを用い、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ている。

○電気的分離
バックアップ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。右図にバックアップ設備の構成概略を示す。

○物理的分離
バックアップ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、バックアップ設備は安全系とは独立して設置している。

バックアップ設備の構成概略




(注) 通常時は制御電源断。操作許可で制御電源入。

# 自己診断まとめ（例）



| 部位 | 機能 | NO | 項目 | 自己診断 | 外部からの認知 | V&V/工場試験<br>定期試験/保守 | 異常がSW起因共通要因故障として<br>未検出で残存する可能性<br>（×は無しを表す） | 備考 |
|---|---|---|---|---|---|---|---|---|
| a | プロセス値入力 | 1 | プロセス入力装置異常<br>（基板構成、AI・DI回路） | ○ | ○警報 | ○ | ×<br>HW起因、自己診断可 | |
| | | 2 | 入力上下限オーバ | ○ | ○警報 | ○ | ×<br>HW又はプロセス起因、<br>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） | ○ | ○警報 | ○ | ×<br>HW起因、自己診断可 | |
| b | 工学単位変換 | 4 | 変換式・定数<br>プログラムエラー | ー | ◇表示異常 | ○ | ×<br>試験で検出可 | |
| | | 5 | 制御命令チェック<br>（異常制御命令チェック） | ○ | ○警報 | ○ | ×<br>自己診断、試験で検出可 | |
| | | 6 | ＣＰＵ０割発生 | ○ | ○警報 | ○ | ×<br>自己診断、試験で検出可） | |
| | | 7 | 結果保存・読出異常<br>（メモリチェック） | ○ | ○警報 | ○ | ×<br>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 | 自区分論理判定部への送付 | 8 | データ化け | ○ | ○警報 | ○ | ×<br>自己診断、試験で検出可 | |
| | | 9 | 伝送停止 | ○ | ○警報 | ○ | ×<br>自己診断、試験で検出可 | |
| | | 10 | データ更新異常 | ○ | ○警報 | ○ | ×<br>自己診断、試験で検出可 | |
| f | 他区分論理判定部への伝送 | | 8,9,10による | | | | | |
| g | ＳＷ位置等入力、<br>論理判定部への送付 | | 入力部：１による | ○ | ○警報 | ○ | ×<br>HW起因、自己診断可 | |
| | | | 伝送部：9,10,11による | ○ | ○警報 | ○ | ×<br>自己診断、試験で検出可 | |
| h | 論理判定 | | 他区分からの伝送：8,9,10による | | | | | |
| | | | 論理演算エラー：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 | | 伝送部：8,9,10による | | | | | 注1） |
| | | 11 | プロセス入力装置異常<br>（基板構成、AO・DO回路） | ○ | ○警報 | ○ | ×<br>（HW起因、自己診断可） | |
| | プログラム動作 | | | | | | | |
| | 周期動作 | 12 | ウォッチドッグタイマ | ○ | ○警報 | ○ | ×<br>自己診断可 | |
| | ＣＰＵ異常 | 14 | ＣＰＵ命令チェック | ○ | ○警報 | ○ | ×<br>HW起因、自己診断可 | 注2） |
| | 想定外動作<br>（OS異常、コンパイラ異常等<br>含む） | 13 | アドレス範囲チェック<br>ウォッチドッグタイマ | ○ | ○警報 | ○ | ×<br>自己診断可 | |
| | | | 上記で検出できない場合 | ー | ◇表示異常 | ◇ | △<br>試験で未検出の場合<br>可能性有り | |

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。