資料２－２

多様化設備に対する主な意見

2019年12月4日
原子力エネルギー協議会

項　目

１．多様化設備の信頼性確保の考え方（火災、溢水）

２．デジタル安全保護回路に対する代替機能

1．多様化設備の信頼性確保の考え方（火災、溢水）

【規制骨子案　抜粋（10/30公開会合）】

・**共通要因によって安全保護機能と同時にその代替作動機能が損なわれるおそれがない**よう適切な手段を講じること

【補足】「適切な措置を講じたもの」とは、安全保護回路の作動が要求される場合において**安全保護機能と代替作動機能が同時に損なわれない**よう、**物理的方法その他の方法によりそれぞれ互いに分離**することをいう。設計基準事故等の起因となる事象に対して、**その起因事象の影響を考慮しても安全保護機能に期待することなく多様化設備により適切に対処**できるよう設計すること。例えば、ある想定される火災区域での**火災により設計基準事故等が発生する場合には、その火災に対して安全保護回路と多様化設備が同時に機能喪失しないよう設計**すること

・許可基準規則（略）**第8条【内部火災】、第9条【溢水】・・によって安全保護機能と同時にその代替作動機能が損なわれるおそれがないよう適切な手段を講じる**こと

【補足】**第12条【安全施設】のうち、第2項（多重性又は多様性及び独立性）については（略）適用しない**

【上記を踏まえた信頼性確保の考え方（意見）】

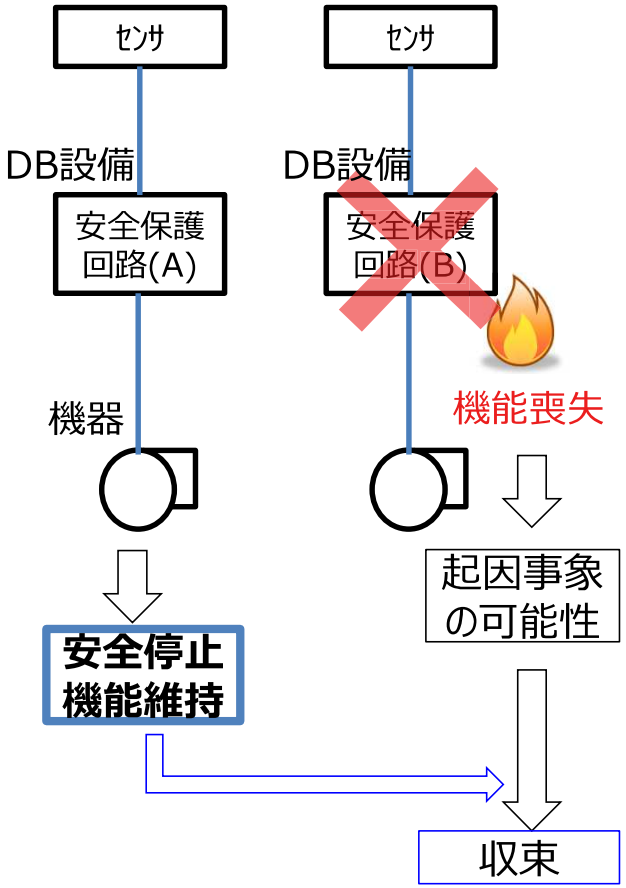
ソフトウェアCCFは設計上の残存リスクであり、火災等に伴う起因事象の発生と重畳するリスクは十分小さいため、火災等の発生に対しては、CCFは考慮せず、設計基準事故対処設備（DB設備）で安全機能を確保できるように対策を講じるものとする。

◎火災・溢水が発生しても、**DB設備で安全停止機能を確保**する

◎多様化設備が、火災・溢水の影響を受けたとしても、**DB設備の安全機能への影響防止を図る**

火災防護の考え方

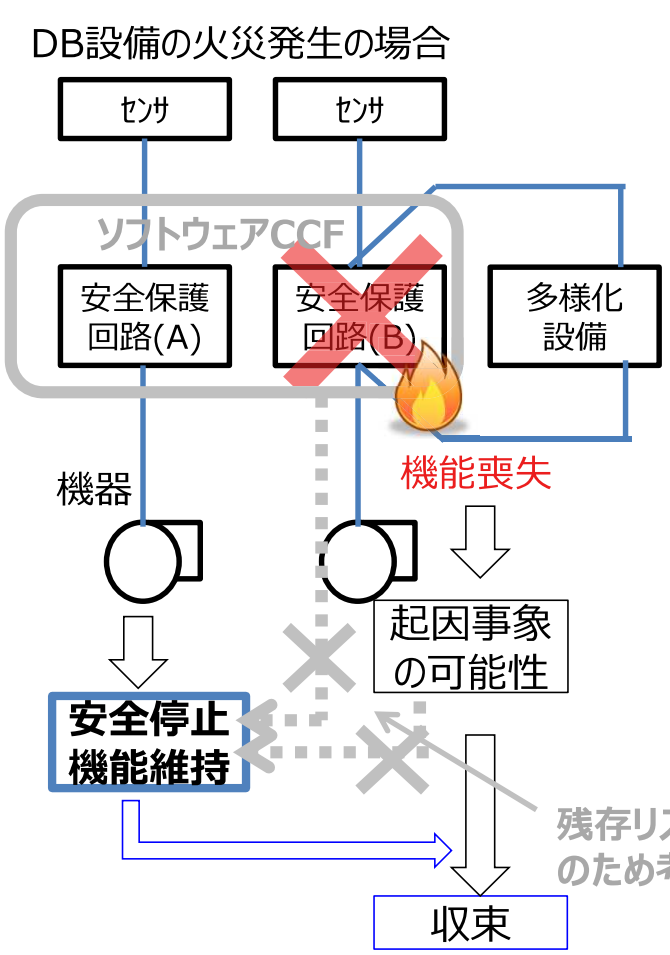
設計基準事故対処設備の場合



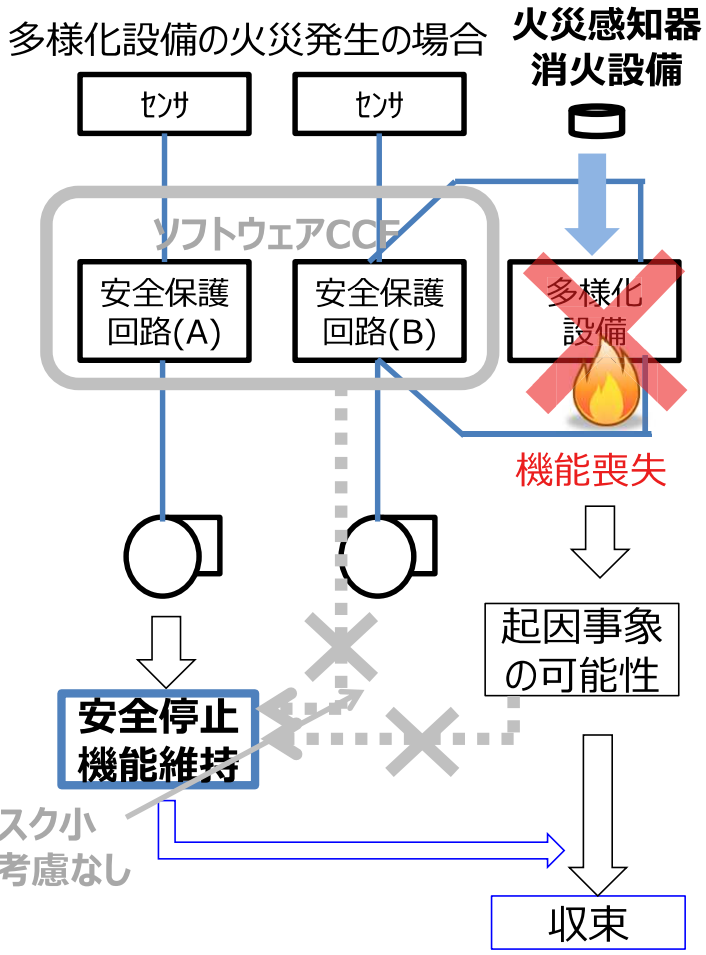
1系統の安全停止機能を確保

（DB設備の規制要求）

多様化設備の場合



DB設備で安全停止機能を確保



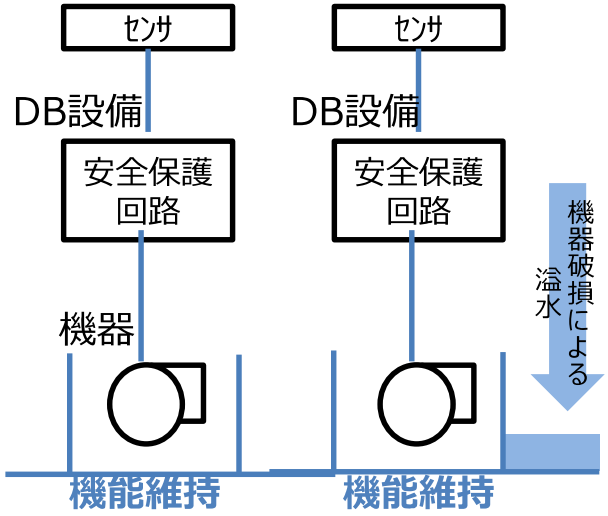
火災を感知し消火を行うことにより、分離されたDB設備への悪影響を防止する

ソフトウェアCCFは考慮せず、DB設備を期待し安全停止機能を確保

内部溢水防護の考え方

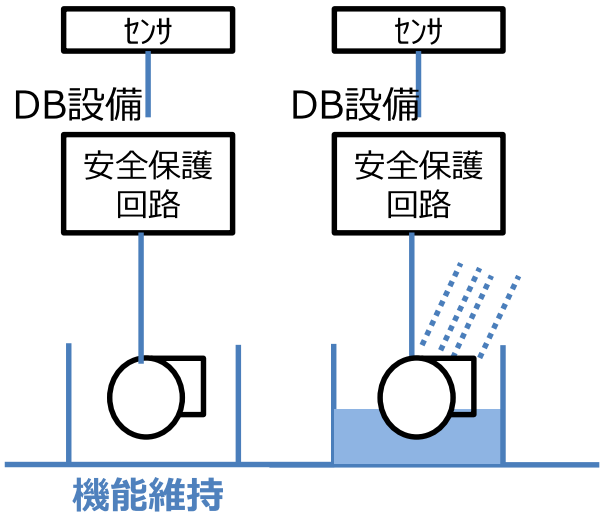
設計基準事故対処設備の場合

機器想定破損による溢水の影響



堰設置等の対策により、同時に安全停止機能を損なわない

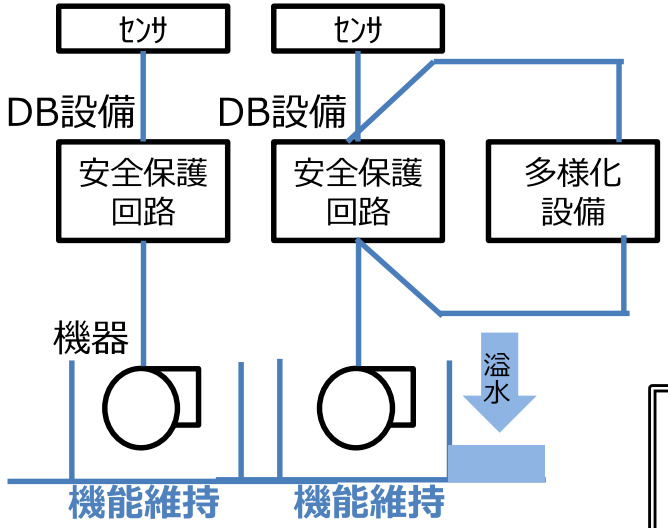
消火水による被水の影響



被水防止の対策により、同時に安全停止機能を損なわない

多様化設備の場合

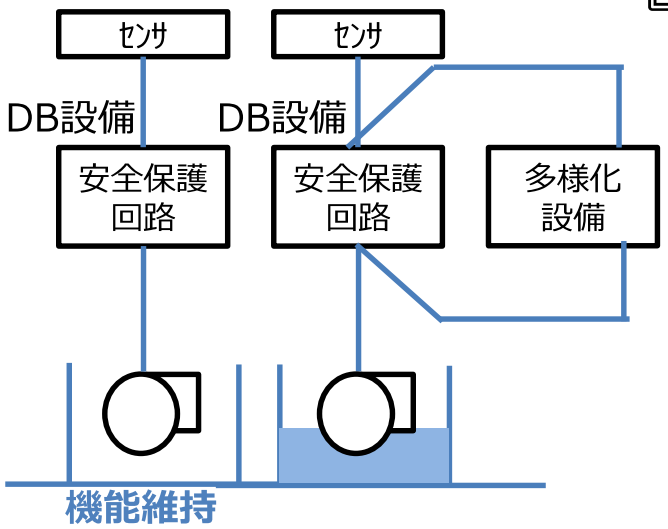
機器想定破損による溢水の影響



DB要求と同じく、1系統のDB設備の安全停止機能を確保する

ソフトウェアCCFは考慮せず、DB設備を期待し安全停止機能を確保

消火水による被水の影響



2．デジタル安全保護回路に対する代替機能

【規制骨子案　抜粋（10/30公開会合）】

・ソフトウェア起因の共通要因故障により、多重化されたデジタル安全保護回路がその保護機能を喪失した場合において、

A）安全保護回路とは異なる動作原理の機構により、

B）原子炉停止系統及び工学的安全施設を

C）自動的に、又は原子炉制御室から手動により作動させることができること。

【補足】「A）安全保護回路とは異なる動作原理の機構」とは、**ソフトウェアを用いることなく作動させることができるものなど、ソフトウェアに起因する共通要因によってデジタル安全保護回路と同時にその機能を喪失するおそれがないもの**をいう。

【要求事項の考え方（意見）】

A）は、**ソフトウェアを用いた設備であっても、ソフトウェアに起因する共通要因故障によってデジタル安全保護回路と同時にその機能を喪失するおそれがないものについては、代替機能に含まれ**るものと考える。

＜具体的な構成例＞

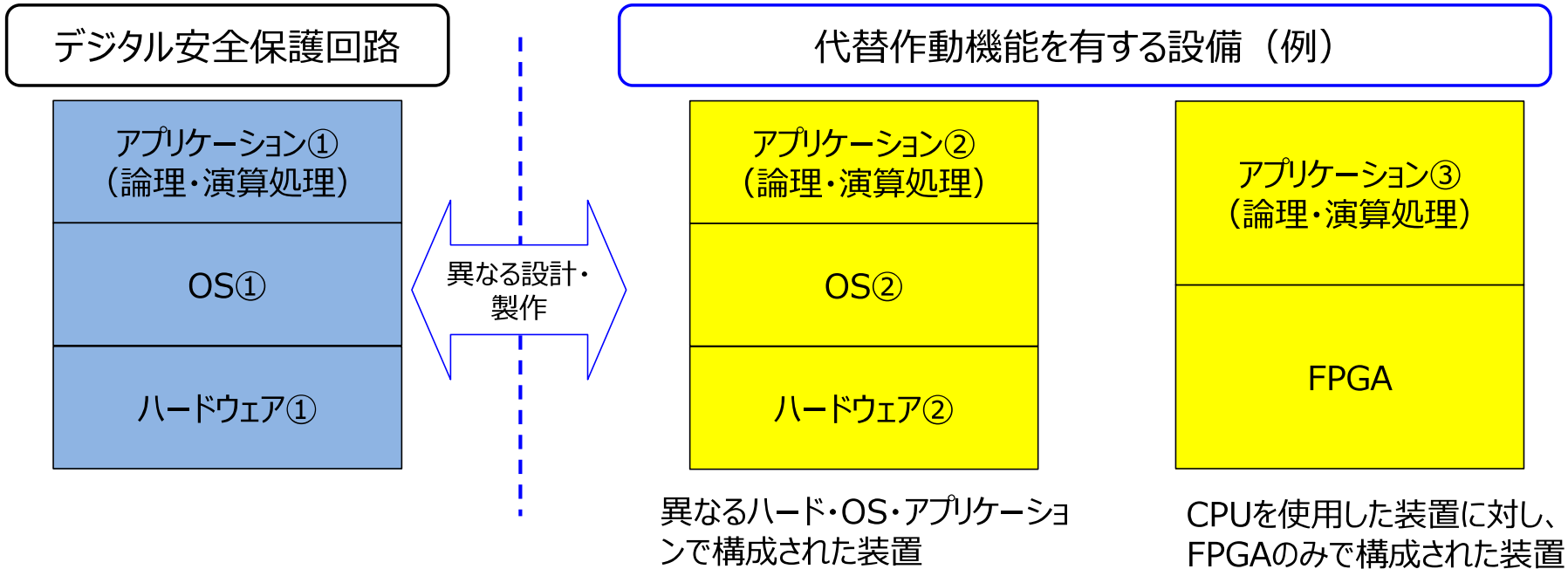
①デジタル制御回路を使用していない機器　（例：ハードワイヤード）

②デジタル制御回路を使用しているが、デジタル安全保護回路とは共通部分を有しないもの

次頁

2．デジタル安全保護回路に対する代替機能

デジタル安全保護回路と**共通の設計の部分が無い**デジタル制御回路であれば、代替作動機能を有する設備として適用可能と考えられる



＜参考＞米国デジタルI&C審査基準で示されている、ソフトウェアCCFを除外することを認めるクライテリア（BTP7-19 rev.8　3.1.1より抜粋）

- 多重性を担う**他の機能と多様性**が図られている（**異なるデジタル技術の採用**）
- **共通又は共有化されたリソース（例：電源、メモリ、バス、通信モジュール等）を持たない**
- 使用される技術は高い信頼性があり、期待される期間において継続的に利用可能である
- 継続的な運転可能性を検証するために、定期的なサーベイランスクライテリアが使用される