

デジタル安全保護回路のソフトウェアに起因する 共通要因故障への対応の考え方について

2019年12月4日
原子力エネルギー協議会

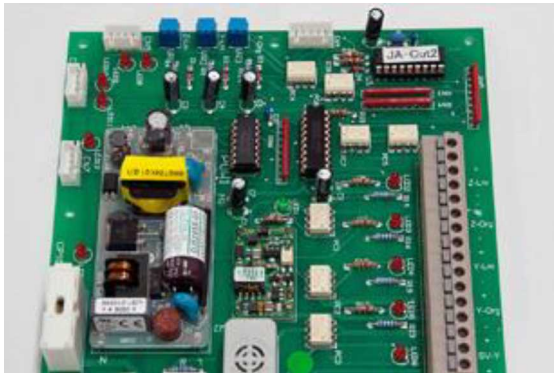

はじめに

- 安全保護回路は、設計基準事象に対する原子炉の安全機能を確保するために重要な設備であり、この信頼性を高め、原子炉の安全確保を確実にすることは、ATENAとしても重要と考えている。
- 本資料では、安全保護回路の信頼性向上の取り組み、並びに、本検討会合の課題であるデジタル安全保護回路のソフトウェアCCFのリスクに関するATENAとしての考え方を述べる。

1. デジタル安全保護回路の信頼性向上の取り組み

デジタル化の意義

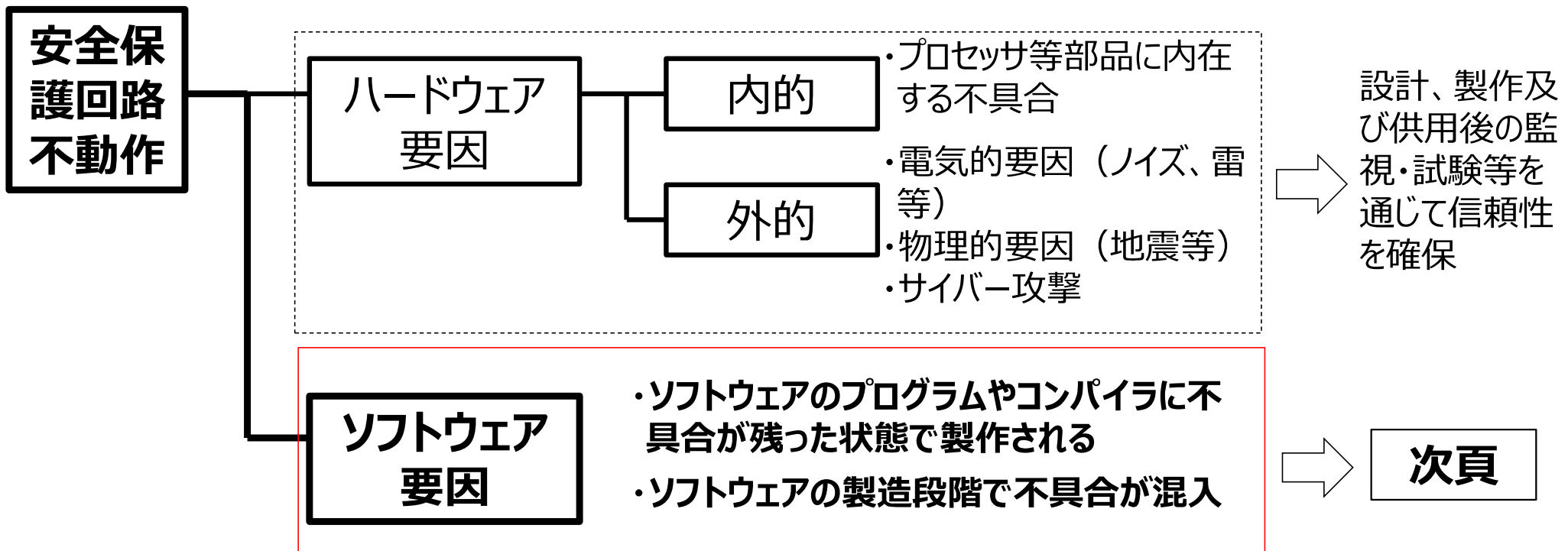
- 原子力産業界は、これまで、アナログ方式による安全保護回路に対し、信頼性向上や保守性の向上の目的でデジタル化を進めてきた。

		アナログ装置	デジタル装置
安全保護回路		 <p>【特徴】部品数多い、消費電力大（劣化影響）</p>	 <p>【特徴】部品数少ない（マイクロプロセッサ使用）</p>
		デジタル化 →	
信頼性	論理演算方式	(例) 1 out of 2 twice	2 out of 4
	ハードウェア故障* (アンアベイラビリティ)	$10^{-4}/\text{demand}$ 程度	$10^{-6}/\text{demand}$ 程度
保守性	経年変化	あり	ソフトは経年変化なし

* : トピカルレポート「デジタル安全保護系設備の基本仕様と設計プロセス」(HLR-113) のスクラム失敗確率より引用

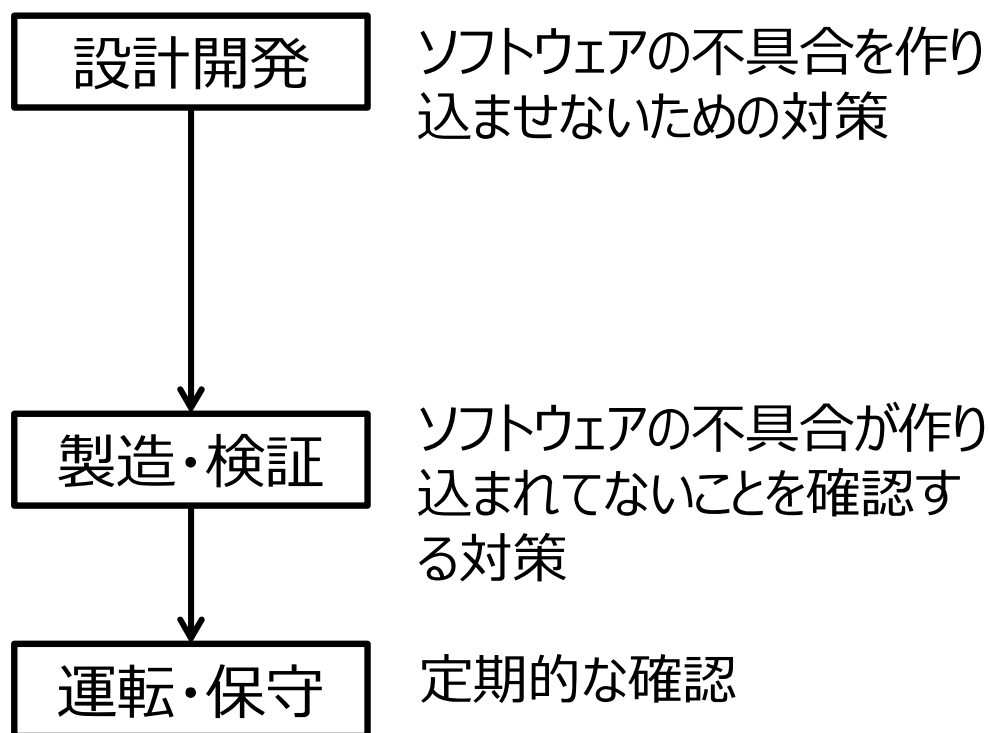
ソフトウェア故障に対する信頼性向上対策（1/2）

- デジタル化に伴い、ハードウェアの信頼性は向上する。
- 一方、デジタル安全保護回路は、アナログ回路と異なり、ハードだけでなくソフトウェアに起因する故障（不具合）が内在する可能性あり。このため、デジタル安全保護回路は、ハードだけでなく、ソフトウェアの故障の防止の取り組みを行うことで、安全保護回路全体の信頼性を確保してきている。



ソフトウェア故障に対する信頼性向上対策（2/2）

- ソフトウェアに起因する故障への対応として、故障発生要因を踏まえ、設計開発段階より、以下のような対策を講じている。



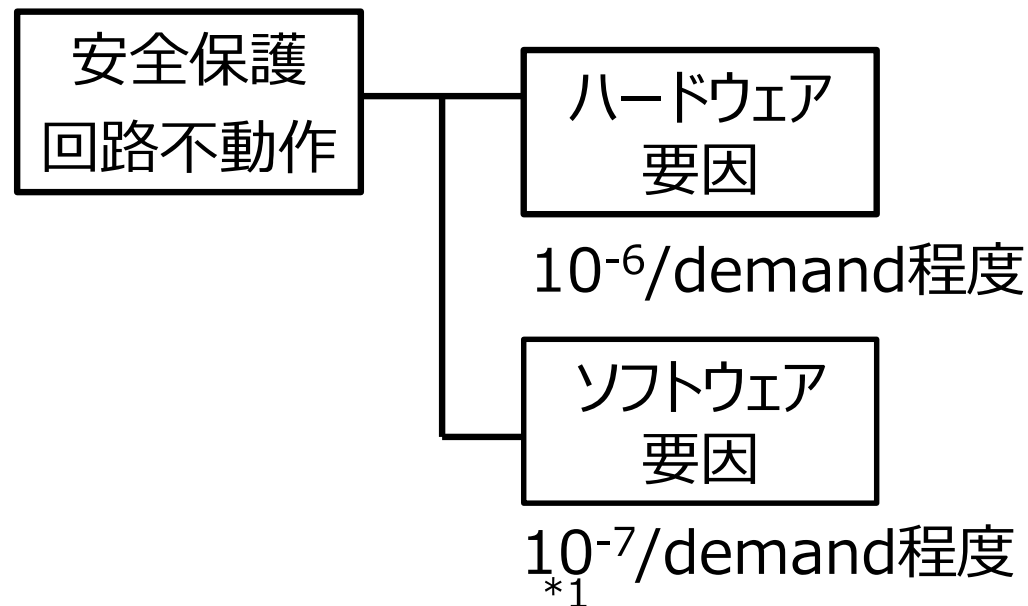
- ソフトウェアの構造の単純化
- 視認性の向上（プログラム言語）
- コーディング作業の人の介在の不要化
- FMEA評価に基づき自己診断機能の設計
- 各段階で、第三者による図書ベースの確認（検証）*
- 各段階で、第三者による図書ベースの確認（検証）及び設計の妥当性確認（V&Vの実施）*
- 定期検査時、マスターROMによるコンペアチェックを実施
- 安全保護系機能試験・設定値確認試験の実施
- 自己診断機能の実施、ソフト・ハードの健全性確認

*：設置許可基準規則24条6項の要求への対応として実施

2. ソフトウェアCCFリスクの考え方

デジタル安全保護回路の信頼性について

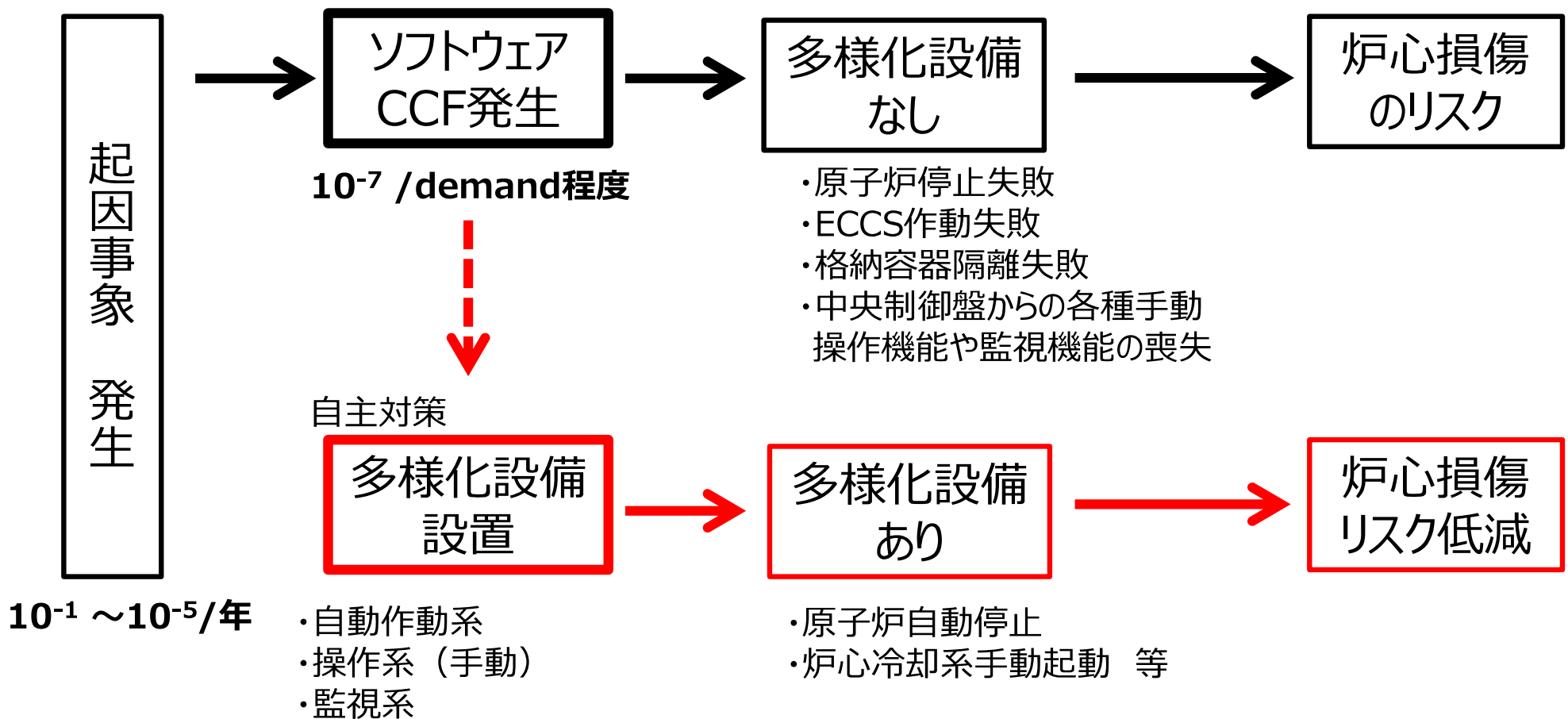
- 安全保護回路内では、供用中、10msec～200msec程度の周期でデマンドが発生しているが、ソフトウェアCCFに起因する故障は、これまでのデジタル安全保護回路の稼働期間中で一度も発生していない。
- ソフトウェアに起因する故障は、以下のとおり、 $10^{-7}/\text{demand}$ オーダー程度の水準にまで低減されている。このため、ソフトウェアCCFが発生する可能性は極めて小さく、ソフトウェアCCFは、プラント設計基準として想定するよりも、設計上の残存リスクとして捉えることが適切と考える。



*1：EPRIレポート（1016731）における米国の20年間の安全系デジタル故障の要因分析結果（総故障の2%がソフトウェア要因故障）を踏まえ、保守側に、総故障の1割をソフトウェア要因故障と設定。

ソフトウェアCCFへの備え

- ソフトウェアCCFが発生した場合に想定される安全機能への影響を踏まえ、これまでの国内プラントにおけるデジタル安全保護回路の設置にあたり、ソフトウェアCCFに対する自主的な緩和対策として、多様化設備を備えてきた。



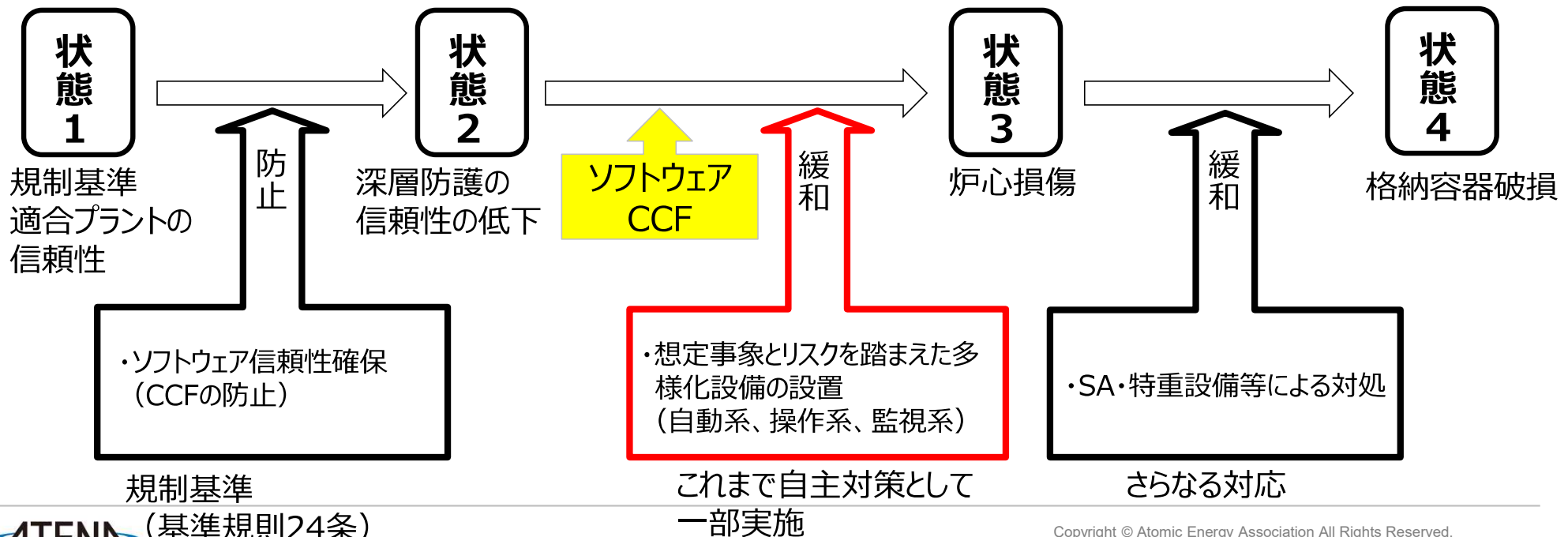
ソフトウェアCCFに対する多様化設備の有効性

- 過渡事象又は事故とソフトウェアCCFが同時に発生した場合、安全保護回路が機能喪失した状態で過渡事象又は事故に対応する必要がある。このような状況下で、自主対策で設置している多様化設備で対応を実施した場合、下表のような結果となる。
- 大中破断LOCAに関しては、決定論的評価の観点からは課題があるものの、起因事象発生頻度（ 10^{-5} /年程度）及びソフトウェアCCFの発生確率（ 10^{-7} /demand）との重畳であることを踏まえると、残存リスクは十分小さいと言える。

事象		BWR	PWR
制御棒系	過渡	手順上制御棒操作はノッチ操作であり、評価想定 の連続引き抜きは実施しない	原子炉停止：自動停止により対応可能。 炉心冷却：補助給水系の自動作動により対 応可能。
	事故(RIA)	制御棒引き抜け時にはラッチ機構があるなど、制御 棒落下のシナリオが現実的には想定し得ない	
過渡（制御棒系以外）		原子炉停止：自動停止により対応可能。 炉心冷却：炉心損傷までの時間余裕あり。 HPCFの手動操作により対応可能。	
事故（LOCA以外）			
事故 (LOCA)	小	原子炉停止：自動停止により対応可能。炉心冷 却：過渡と同様、手動操作により対応可能。ただ し、過渡と比べて時間余裕が小。	原子炉停止：自動停止により対応可能。 炉心冷却：高圧注入系の手動操作により対 応可能。
	中	同上	炉心冷却：手動操作により対応不可。
	大破断	炉心冷却：小中破断LOCAと同様、手動操作に より対応。ただし、小中破断LOCAと比べて更に時 間余裕小。	

ソフトウェアCCF対策（残存リスクに対する考え方）

- ソフトウェアCCFの残存リスクに対する対応の考え方については、以下のとおり。
 - ◎ 状態 1 ⇒ 2（ソフトウェアCCFの発生）の防止のため、デジタル安全保護回路に係る信頼性確保対策を実施する。
 - ◎ 状態 3 に至るような残存リスクをゼロにすることはできないため、当該リスクレベルが適正水準になるよう、状態 3 ⇒ 4 に係る緩和戦略も考慮の上、状態 1 ～ 3 全体で効果的な対策を検討する。



3. デジタル装置規制に関する海外の動向

デジタル装置規制に関する海外の動向

- 米国規制は、ソフトウェアCCFに対する評価に関する審査方針を定めている。また、これまでの供用実績等を踏まえ、ソフトウェアの信頼性や安全上の重要性にフォーカスした審査方針とするよう近代化を図っている段階にある。

【（参考）米国のデジタル規制経緯】

- 1979年 Westinghouse社の安全保護回路にCCFの懸念があるため、多様性評価（D3評価）を行うことを、審査方針として規定。
- 1990年代 第三世代炉でデジタル装置を導入する動向にあることを踏まえ、DC審査の方針として、デジタル装置のソフトウェアCCFの発生防止及び万一の発生に備えた多様化対策を求める方針を定めるとともに、既設プラントにも展開。
- 2000年代 オコニー発電所のデジタル化審査。この審査経験等を踏まえ、審査方針に、最適評価の概念（単一故障を想定しない、非安全系のクレジットを可とする等）が追加。
- 2016年～ 規制の近代化対応として、以下の観点から審査方針の見直しを検討中。
 - ソフトウェアの信頼性を元に、CCFの考慮を排除することを可とするプロセスの導入
 - 安全上の重要性の考慮（グレーデッドアプローチ）
 - 多様化設備に代わる措置の扱い（例：運転監視(LBB)を前提とした大破断LOCA向け設備対策の除外）
- 米国以外を見ると、多様化設備を考慮する必要がある対象起因事象については、炉心損傷頻度への寄与度を踏まえ、大破断LOCAを除外する等の絞込みを行っている国（英国他）が見られる。

米国のデジタルI&C規制に関する議論状況（11/22 ACRSの状況）

◎米国規制諮問会議（ACRS：Advisory Committee on Reactor Safeguards）の結果

日時 11/21（木）10時～14時頃 出席者：ACRS、NRR、NEI、EPRI

内容 以下のとおり、規制当局及び産業界がプレゼン。特に、ソフトウェアの信頼性や、ソフトウェア故障＝「CCF」とならないようにするためのポイントについて議論が行われた。

- NRC：デジタルI&Cに関する標準審査計画（SRP）であるBTP7-19の改訂ドラフトを紹介（主な改訂ポイントは以下のとおり）。また、今後、2020年第三四半期に最終改訂版を発行することを目指し、BTPの見直しを進め、パブコメやACRSの付議を行っていくことを説明。
 - グレーデッドアプローチの導入（I&Cの重要度を踏まえ、ソフトウェア信頼性の確認方法を分類。深層防護評価までを行うのは、安全上重要なカテゴリーのみ。）
 - CCFの考慮を除外可とするプロセスの追加（設計の属性（多様性）の違いを考慮 等）
- NEI：適切なCCF対策を行えば、必ずしも多様化設備を設置する必要はないことについて議論することが重要であり、具体的には、以下のアイテムが重要との意見を提示。
 - ソフトウェア品質確保プロセス（設計等）、同時故障を誘発するトリガー、運転経験
 - ソフトウェア設計（設計要求、属性、設計プロセスの品質保証等）
 - 産業界のベストプラクティスの活用
- EPRI：過去のデジタルI&Cに関する研究成果（デジタルI&C故障の要因分析結果、信頼性向上活動の効果、リスクインサイトの活用可能性等）を説明。

4. 今後の議論の進め方

今後の公開会合における議論の進め方について

- 今回、現状のデジタル安全保護回路が有するソフトウェアの信頼性の水準を示した。
- また、ソフトウェアCCFが発生した場合のプラント安全への影響や多様化設備の有効性について、今回は概略評価を示したが、別途安全解析を実施の上、詳細な評価結果を示す。
- 今後、これらの評価結果や、規制化に伴う以下のような影響も踏まえ、深層防護全体でバランスが取れた効果的な安全対策を検討することが重要と考えている。
 - デジタル安全保護回路から多様化設備への配線等分岐に伴う回路全体の更なる複雑化の影響（追加的に考慮すべきリスクを生み出す虞）
 - デジタル安全保護回路未導入プラントのデジタル化判断への影響

【今後の議論の進め方（提案）】

- ATENAとしては、上記のとおり、現状のデジタル安全保護回路の信頼性も踏まえ、深層防護全体で見て、デジタル安全保護回路に対しどのような対策を講じることが安全の観点から効果的か考え方を整理するので、次回以降の会合にて議論したい。

参考資料

デジタル安全保護回路の ソフトウェア信頼性向上施策について

1. ソフトウェア信頼性向上施策

- ・安全保護回路：

安全保護系を構成する装置のうち、安全保護回路（論理演算機能（作動（起動）回路））及び設定値比較回路とする

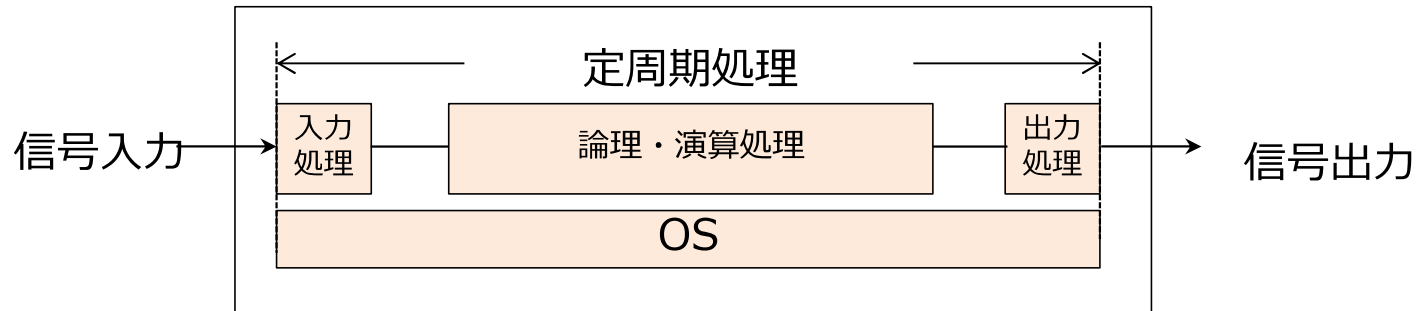
- ・ソフトウェアCCF：

安全保護回路に実装されているソフトウェアの不具合によって、多重化された安全保護回路の機能が喪失する事象

3つの施策によりソフトウェアの設計・製作・運用の高信頼度を担保

- (1) 高信頼設計・製作
- (2) 自己診断による異常検出
- (3) 工場試験・定期的な試験・保守

高信頼設計・製作



ソフトウェア構造（例）

(1) 設計・製作

a. OS

- ・定周期処理
- ・スケジュール管理だけのシンプルな構成
- ・信頼性のあるOSを使用
- ・非同期処理（I～IV系）

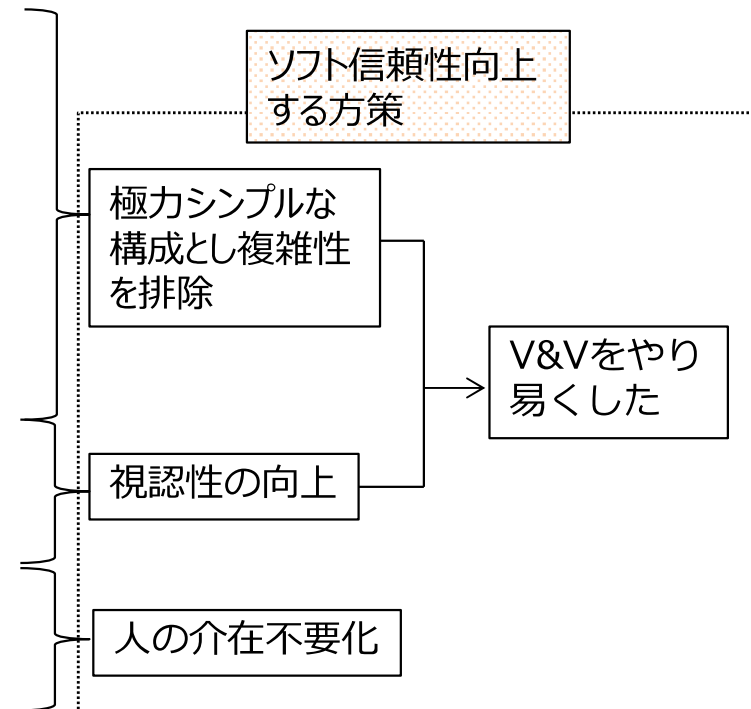
b. アプリケーションソフトウェア

- ・シングルタスク（マルチタスクなし）
- ・割り込みなし

c. 言語

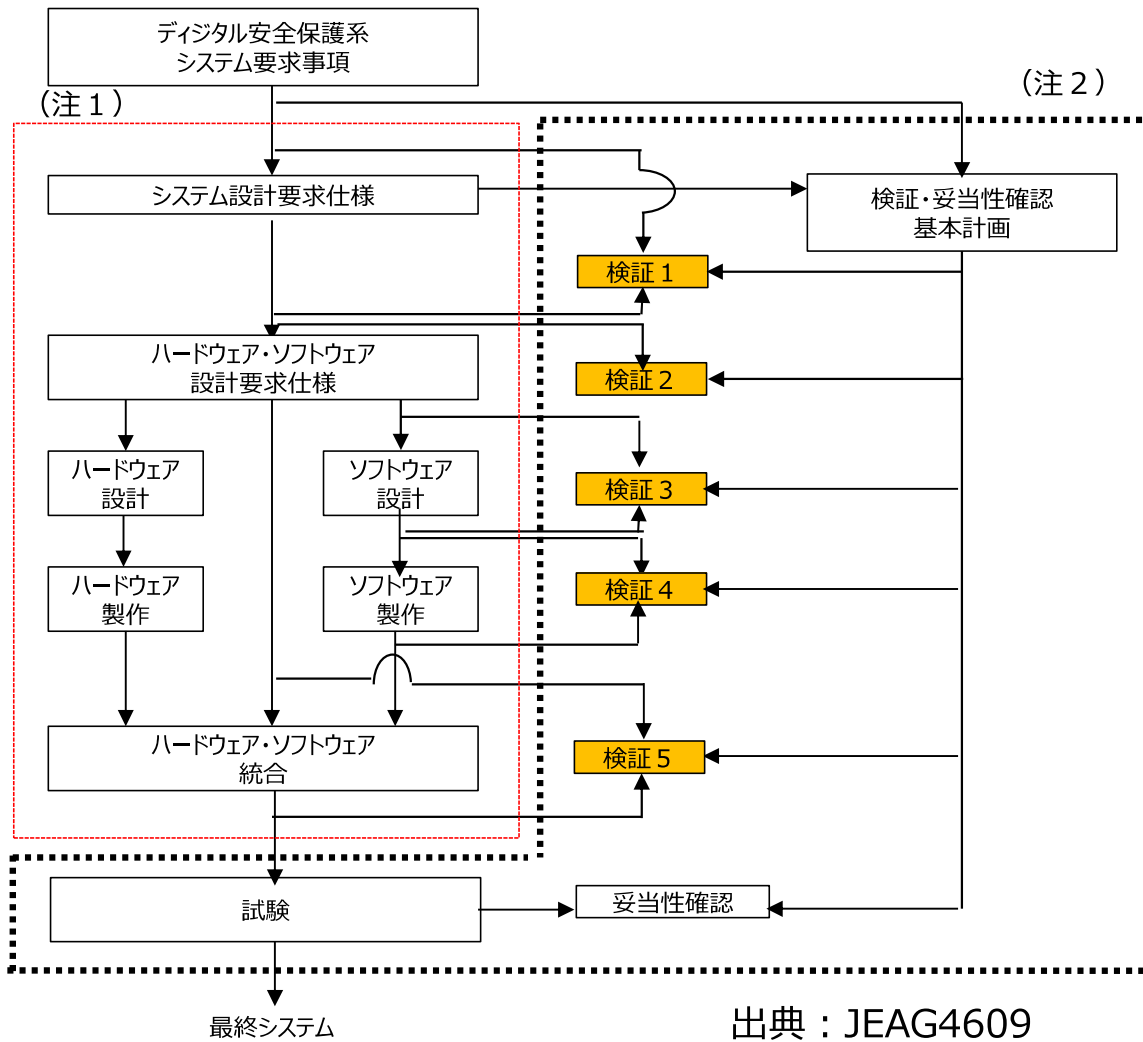
- ・POL（Problem Oriented Language）の採用
- ・可視化言語（画面上でAND/ORのマクロを結線）
- ・POLで作成した制御回路を自動的に機械語へ変換する（コーディング作業不要）

d. 自己診断によるソフト異常検出



V&Vの実施

デジタル安全保護回路におけるCCF対策に加えて、V&Vを実施



・各設計段階で第3者による図書ベースの
確認（検証）

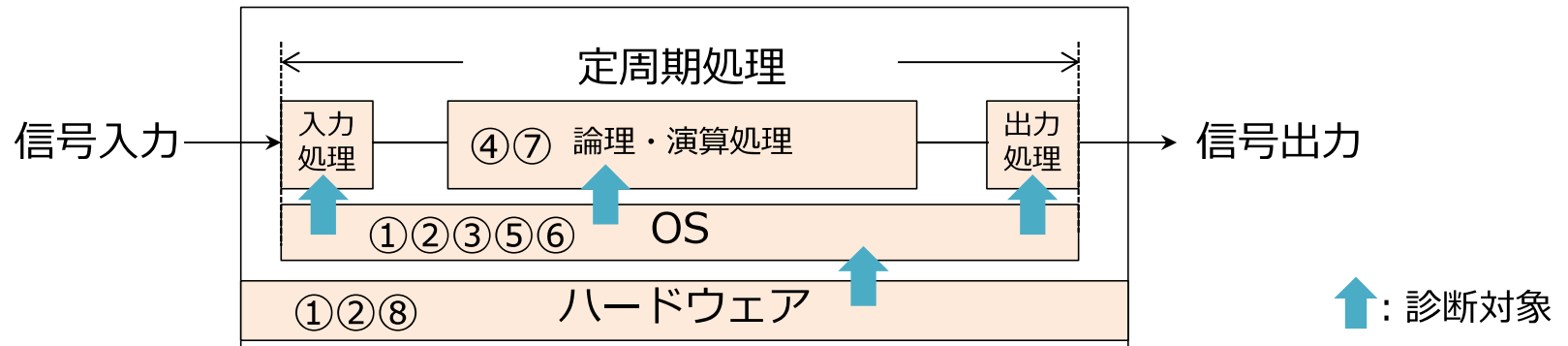
検証1・・・システム設計基本仕様検証
検証2・・・ハードウェア・ソフトウェア設計要求仕様検証
検証3・・・ソフトウェア設計検証
検証4・・・ソフトウェア製作検証
検証5・・・ハードウェア・ソフトウェア統合検証

(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

自己診断による異常検出

自己診断機能により異常動作を早期検知し、警報による告知とともに他装置への影響防止が可能



診断箇所	No.	診断機能	診断対象	診断内容	検出部	警報発報
マイクロ プロセッサ部 (CPU+メモリ)	①	ウォッチ ドッグタイマ	OS : アプリケーションの周期監視 ハードウェア : OSの周期監視	プログラムの演算異常検出	ハードウェア OS	○
	②	パリティ チェック	メモリ	メモリの異常検出	ハードウェア	○
	③	ゼロ除算	アプリケーション	ゼロ割演算が発生した場合の演算の異常検出	OS	○
	④	相互診断	アプリケーション (制御系間)	独立2重系システムにおいて、1系と2系の入力・出力の偏差監視	アプリ ケーション	○
通信部 プロセス 入出力部	⑤	誤り検出 コード	伝送信号	データ伝送時の送受信状態のチェックを行い伝送異常検出	OS	○
	⑥	伝送受信中断	伝送信号	データ伝送信号を一定時間内に得られない場合の伝送路異常検出	OS	○
	⑦	合理性 チェック	入力信号	入力信号が所定レンジを逸脱した場合の異常検出	アプリ ケーション	○
共通	⑧	構成機器の 異常診断	構成機器	ハード機器の異常検出	ハードウェア	○

工場試験や定期的な試験・保守

(1) 開発・検証

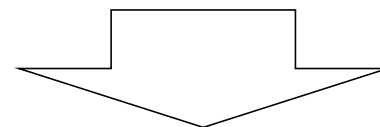
- a. ハードウェア検証
 - PLD等を含めたハードウェアとして全機能試験
- b. ソフトウェア検証
 - 構造試験(White Box Test)
 - 性能試験 (処理性、応答性、制御性)
- c. ハードウェア・ソフトウェア組合せ検証
 - ハードウェアと組み合わせた状態で、カード、ユニットの全機能を確認

(2) 製造・検証

- a. 工場試験 (単体試験、組み合わせ試験)
 - ・模擬信号入力によるインターロックの動作確認
 - ・構成制御試験 (制御系切替等)
- b. 現地での確認
 - ・ソフトウェア復元 (工場出荷ソフトウェア)
 - ・インターフェイス試験 (補機動作等)
 - ・系統試験、起動試験

(3) 定期的な試験・保守

- a. 定期検査時の確認
 - ・マスターとのコンペアチェック (ロジックに変化がない事の確認)
 - ・模擬信号による機能試験 (スクラム等)
- b. 月例テスト (サーベランス) による確認
 - ・安全保護系論理回路の機能検査を実施

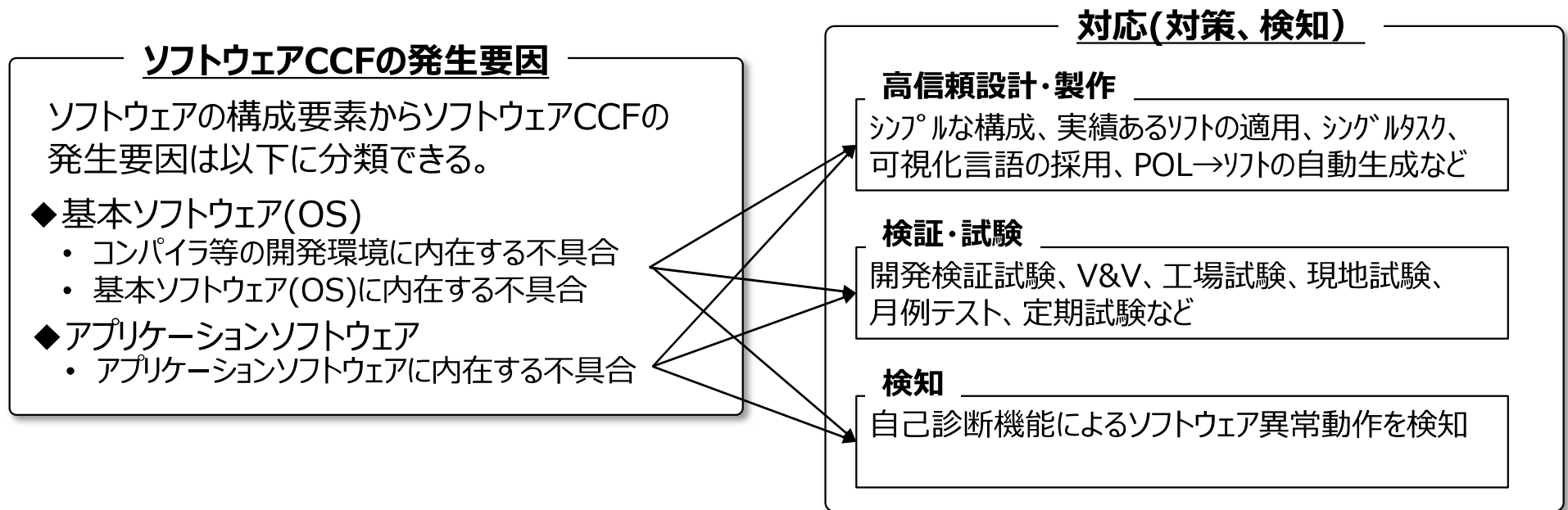


・ソフトウェアが工場出荷時の状態を保持していることを確認。
 ・現地試験や定期検査時にインターロック動作を確認。

2. ソフトウェアCCFの要因と評価

ソフトウェアCCFの要因と評価

(1) ソフトウェアCCFの発生要因とそれを低減するための対応（対策、検知）と、自己診断を考慮すると、**ソフトウェアCCFが起きる可能性は極めて低い**と言える。



(2) 運転実績に基づく信頼性評価

多重化された制御装置（原子力安全保護系、原子力常用系、火力）の国内運転実績は、 6.8×10^8 時間程度におよび、この間ソフトCCFは発生していない。仮に、0.5回が発生したとするとソフトCCF発生頻度は、 6.4×10^{-6} /年と評価できる。