

2020年1月29日「第4回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」公開会合資料より抜粋

デジタル安全保護回路のソフトウェアCCF の影響評価と対策

2020年1月29日
原子力エネルギー協議会

目次

1. はじめに	
(1) デジタル安全保護回路のソフトウェアCCF対策検討の位置づけ	3
2. 影響評価	
(1) 想定事象	4
(2) 評価方法	4 ~ 5
(3) 影響評価 (予備評価)	5
3. デジタル安全保護回路のソフトウェアCCF対策	
(1) 対策の検討	7
(2) 対策の選択	8
(3) BWR及びPWRの対策	9 ~ 12
4. ATENAの取り組み方針	
(1) ATENAの取り組み方針	14 ~ 15
(2) 安全対策の検討／実施／運用の自律的プロセス (例)	16
(3) 実施時期の考え方	17
(参考) ATENA技術課題の解決プロセス	18

添付資料1 BWRの影響評価について

添付資料2 PWRの影響評価について

1. はじめに

(1) デジタル安全保護回路のソフトウェアCCF対策検討の位置づけ

デジタル安全保護回路のソフトウェアCCF対策については、

- ① ソフトウェアCCFは、ソフトウェアに対する信頼性向上の取り組み（高信頼設計、設計・製作時のV&V、定期試験等）により、十分な発生防止対策が取られており、ソフトウェアCCFが発生する可能性は極めて低く抑えられていること（12/4のATENA会合資料）
- ② 過渡及び事故の発生時に、ソフトウェアCCFが重畳発生する可能性はさらに低いものの、事象発生時の影響が大きいことから影響評価を実施したところ、自主で備えた多様化設備は、殆どの過渡事象及び事故に対し、有効であるとの結果が得られた。
（添付資料1及び2）
- ③ なお、上記ソフトウェアCCF対策により炉心損傷が防止できない場合でも、格納容器破損防止対策により環境への大量の放射性物質の放出は防止することができる。

以上より、安全上の緊急性は高くないと考えるものの、深層防護を重視し、対策の検討を実施した。

2. 影響評価 (1/2)

(1) 想定事象

ソフトウェアCCFにより安全保護機能が喪失している状態で、単一の過渡・事故事象（いずれも全事象が対象）を想定する。

(2) 評価方法

過渡及び事故と「ソフトウェアCCFによる安全保護機能の喪失」が重畳発生した場合に、現実的な評価により、多様化設備の有効性を評価する。

主要な評価条件（例）を下記に示す。

- ・デジタル安全保護回路を経由しない自動もしくは手動起動信号で、原子炉停止系及び工学的安全施設は利用可能
- ・安全設備の単一故障は想定しない
- ・外部電源喪失事象以外の事象では外部電源は利用可能
- ・外部電源喪失及び給水流量の全喪失事象以外の事象では給水系の運転は継続する
- ・サポート系（冷却水・空調）については、起因事象が発生する前の作動状態を維持する
- ・現実的な評価をする際に必要に応じて、ベストエスティメイトコードを使用する

2. 影響評価 (2/2)

(2) 評価方法 (前頁からの続き)

- ・ 事象発生前の初期状態としては、ノミナル条件 (出力、水温など) とする
- ・ 制御棒誤引き抜き過渡・落下事故において、運用を考慮した現実的な制御棒価値を想定する (BWR)
- ・ 中央制御室での運転操作時間は現実的に考慮する (10分ルールは適用しない)
- ・ 時間余裕の範囲で現場操作を想定する
- ・ 多様化設備の性能を確認する観点から多様化設備の故障は想定しない

(3) 影響評価 (予備評価)

BWRの影響評価は添付資料1を、PWRの影響評価は添付資料2を参照

3. デジタル安全保護回路のソフトウェアCCF対策

(1) 対策の検討

・影響評価の結果、ソフトウェアCCFと過渡・事故が重畳した場合でも、以下の対策により事象の収束は可能である。

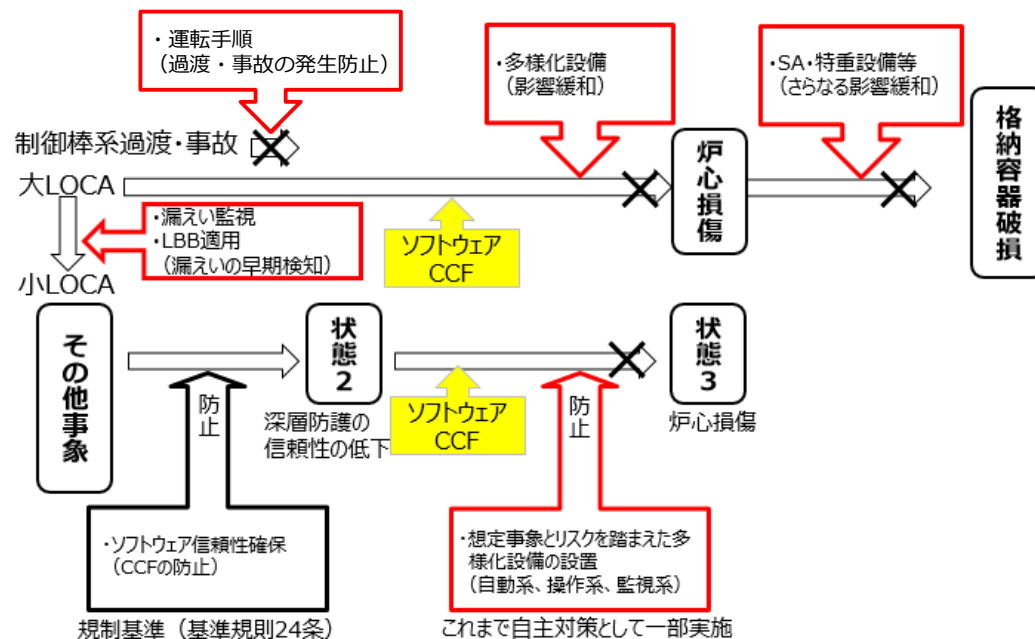
・評価の過程で抽出された対策は以下のように、深層防護の幅広い階層に渡るものとなる

【対策1】警報等の事象発生時の認知手段の充実（早期検知）

【対策2】事象発生時の手順の整備（認知・判断・行動）

【対策3】BWRの起動時の制御棒の異常な引き抜きの発生防止・緩和（運転員による手動引抜阻止の教育と徹底）

【対策4】PWRの大LOCAの発生防止・緩和
（LBB適用、注水系自動起動、SA設備による格納容器破損防止）



(2) 対策の選択

○抽出した対策の選択に当たっては、以下のような観点を考慮する

- a. 深層防護のバランスに配慮すること
- b. 実行可能な対策であること（費用対効果があること）
- c. 当該対策の実施により安全性を阻害する要因を持ち込まないこと
- d. 国際的な対策水準を考慮すること

○これらを考慮した場合の代表プラントに対する対策は以下ようになる

【対策1】【対策2】は早期検知と迅速な対応の観点から重要であり、上記の観点を満足する必須対策となる

【対策3】運転員による制御棒操作手順の順守で確実に発生防止が図られ、かつ監視により事象発生の影響緩和が可能である

【対策4】は既に格納容器破損防止対策がとられているものの、影響緩和としてより前段の炉心損傷防止を重視し、SI自動化を対策とする

BWR (ABWR) 対策方針・対策

1. 対策方針

デジタル安全保護回路のソフトウェアCCFと過渡・事故の重畳を想定し、デジタル安全保護回路が機能喪失した場合においても、多様化設備により安全停止機能を損なうおそれのない設計とする。

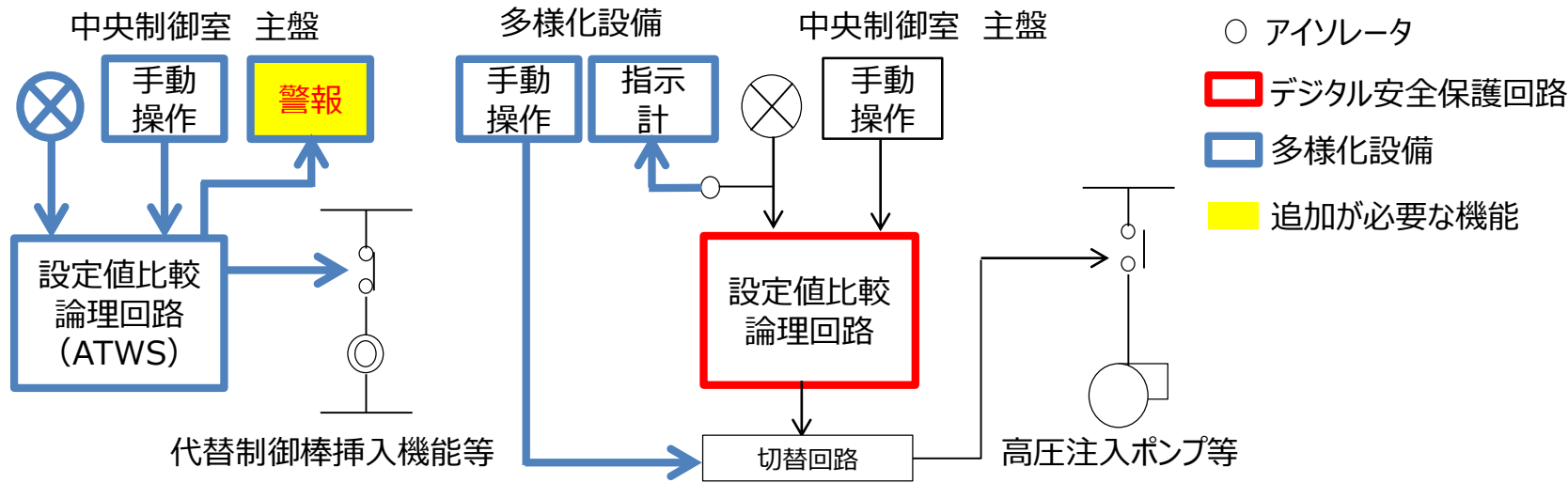
2. 対策

手順書整備の他、以下の対策を採用する。

警報機能： ARI作動
 原子炉水位低
 原子炉圧力高

(3) BWR及びPWRの対策 (2/4)

BWRの 設備対策案



自動機能	手動操作	指示計	警報
<ul style="list-style-type: none"> 原子炉スクラム※ 原子炉再循環ポンプトリップ※ 	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 原子炉水位 原子炉圧力 ドライウエル圧力 主蒸気隔離弁の状態 主要な隔離弁の状態 高圧炉心注水系起動状態 高圧炉心注水系系統流量 	<ul style="list-style-type: none"> ARI作動 原子炉水位低 原子炉圧力高

黒字：既設のバックアップ機能

赤字：追加が必要な機能

※：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。

(3) BWR及びPWRの対策 (3/4)

PWR対策方針・対策

1. 対策方針

デジタル安全保護回路のソフトウェアCCFと過渡・事故の重畳を想定し、デジタル安全保護回路が機能喪失した場合においても、多様化設備により安全停止機能を損なうおそれのない設計とする。

2. 対策

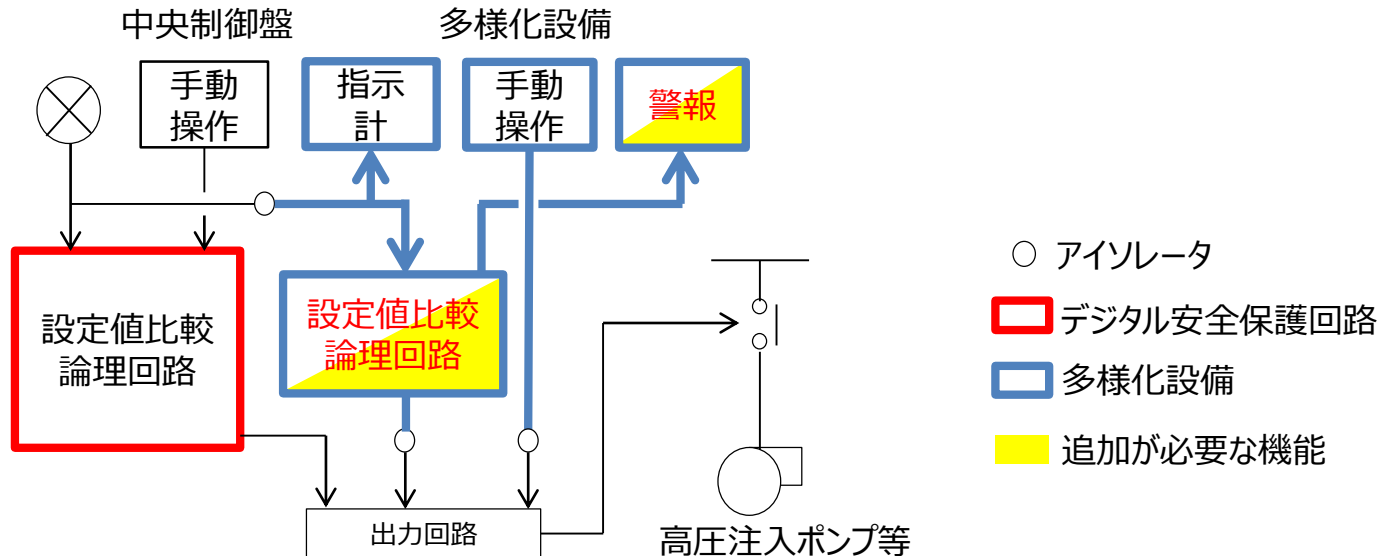
手順書整備の他、以下の対策を採用する。

自動機能： 自動SI「起動」

警報機能： 加圧器圧力異常低 (SI作動)

(3) BWR及びPWRの対策 (4/4)

PWRの設備対策案



自動機能	手動操作	指示計	警報機能
<ul style="list-style-type: none"> 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※ 主蒸気隔離※ 高圧/低圧注入系起動 	<ul style="list-style-type: none"> 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 主蒸気隔離 高圧注入系起動 格納容器隔離 	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 多様化設備作動 加圧器圧力低 (原子炉トリップ等) 加圧器圧力高 (原子炉トリップ等) 蒸気発生器水位低 (原子炉トリップ等) 蒸気発生器水位異常高 加圧器圧力異常低 (高圧/低圧注入系作動)

黒字：既設のバックアップ機能

赤字：追加が必要な機能

※：新規規制基準施行後は、重大事故等対処設備として扱っている。

4. ATENAの取り組み方針

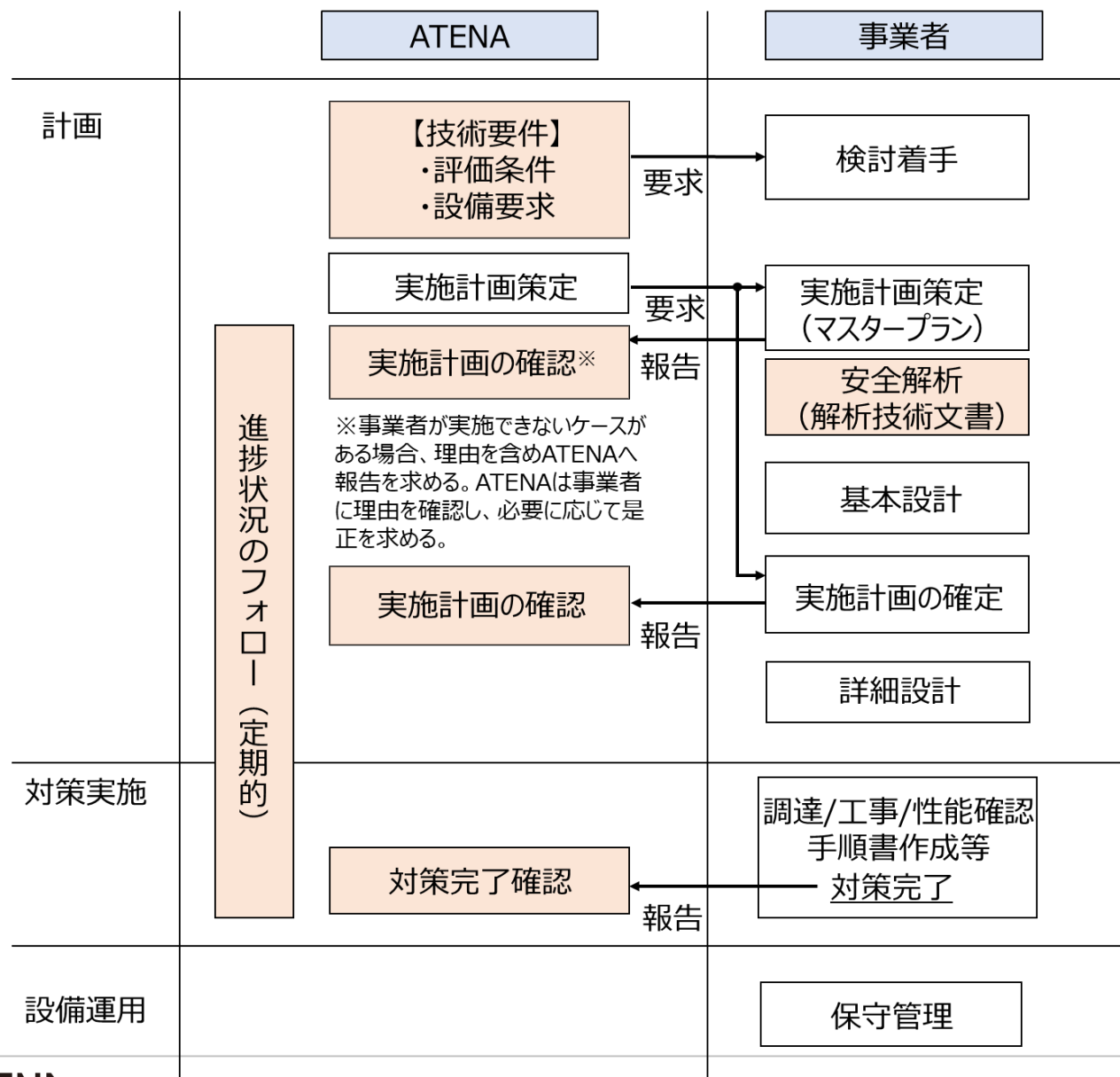
(1) ATENAの取り組み方針 (1/2)

1. これまでのソフトウェアに対する信頼性向上の取り組みにより、ソフトウェアCCFが発生する可能性は極めて低く抑えられている。
また、深層防護の観点から過渡・事故発生時にソフトウェアCCFが重畳する場合を想定したとしても、決定論的安全評価手法で評価すると、これまで自主対策で備えた多様化設備によって、殆どの過渡・事故に対して、炉心損傷防止が可能であると評価される。
2. 一方、大中破断LOCAとソフトウェアCCFの重畳については、現状の多様化設備では炉心損傷に至ると評価される。これらの炉心損傷の発生確率は十分低いものの、会合での議論や国際的な対策水準を踏まえ、炉心損傷防止を重視し、更なる対策を行うことが適切であるとの結論に至った。
3. その他の安全性向上対策も輻輳する中で、産業界として安全上の優先度を考慮し、自律的に且つ計画的に取り組んでいく。

(1) ATENAの取り組み方針 (2/2)

4. 産業界が自律的に取り組む場合、ATENAのガバナンスのもと、16 に示すプロセスで進めていく。
 - (1) ATENAは、評価条件と設備要求（以下、「技術要件」という）を纏め、安全解析及び基本設計を各事業者が合理的且つ早期に対応できるようにする。
 - (2) ATENAは各事業者へ実施計画の提出を要求し、実施計画を公開する。また、進捗をフォローし、進捗状況及び対策完了状況を公開する。
5. ATENAは、海外動向も参考にしながら、多様化設備へのデジタル設備の適用性等を含め技術的検討を継続していく。

(2) 安全対策の検討／実施／運用の自律的プロセス（例）



凡例： 公開情報

進捗状況のフォロー（定期的）

NRAは、ATENAの公開情報、または原子力規制検査や安全性向上評価届出のプロセスを通して、事業者の安全対策の実施状況や内容確認が可能。

(3) 実施時期の考え方

1. ATENAは、技術要件を2020年5月末を目途に作成し、各事業者へ提示すると共に公開する。
2. BWR及びPWR事業者は、技術要件を基に安全解析に着手し、それぞれ解析技術文書として纏める。その結果に基づき、各事業者は具体的に実施する対策を確定するとともに、詳細設計及び対策設備の調達を行う。
3. 工事実施時期は事業者毎に異なるが、再稼働時期を踏まえて、以下とする。
(安全解析に2年程度要すると想定。設備改造は1回の定検で工事可能と想定。)

対象プラント：デジタル安全保護回路導入済プラント及び
導入予定プラント（部分デジタル化プラントも含む）

- ・再稼働済み、もしくは
2023年度までに再稼働するプラント；2023年度以降の最初の施設定検時
- ・2023年度以降に再稼働するプラント；再稼働時期までに実施

(参考) ATENA技術課題の解決プロセス

ATENAは、以下のプロセスで技術課題を解決する。

- ATENAが取り組む課題については、ステアリング会議にて決定する。
- 課題の技術検討は、産業界の専門家で構成したワーキンググループで行う。
- 取り纏めた検討結果（安全対策）をステアリング会議で決定し、各事業者は決定内容にコミットする。また、ATENAは技術レポート等を公開する。
- ATENAは安全対策の実施を各事業者に要求し、各事業者は現場の対策を実行する。
- ATENAは各事業者の対策実施状況をフォローし、公開する。