原子力規制委員会了承文書
（2020FY-27）
令和2年7月8日
（議題4資料4）

発電用原子炉施設のデジタル安全保護回路に係る共通要因故障対策の今後の対応について

令和２年７月８日
原 子 力 規 制 庁

１．経緯

発電用原子炉施設のデジタル安全保護回路に係る共通要因故障対策については、「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」（以下「デジタル検討チーム」という。）において、これまで4回の検討会合を開催した。

原子力規制庁は、令和2年3月11日及び令和2年3月23日の原子力規制委員会において、これまでの検討チームにおける検討結果を報告するとともに、デジタル安全保護回路に係る共通要因故障対策として満足すべき水準（以下「対策水準」という。）の案を原子力規制委員会に諮った。

原子力規制委員会は、第73回原子力規制委員会（令和2年3月23日）において対策水準について了承し、原子力規制庁に対してその取扱いを検討するよう指示した。

【これまでの原子力規制委員会の議論】

○デジタル安全保護回路に係る共通要因故障対策は、品質確保措置の要求やSA対策における有効性評価により現状において災害防止上の支障はないといえるが、更なる信頼性向上を図る観点から対策水準の見直しの検討を行う。

○見直す場合の対策水準は、事務局案（別添１の３．（１））のとおりとする。

○審査の形式で確認してはいないものの、デジタル検討チームの会合で聴取したところによれば、既存の実用発電用原子炉施設は事業者の自主設備によって新たな対策水準の大部分を満足していると考えられる。また、対策水準を完全に満足するため、現在設けられている自主設備に加え、BWR（ABWR）については警報機能の強化が、PWRについては安全注入の自動作動化が必要との方向は、妥当と考えられる。

２．今後の対応について

（１）新たな対策水準については、主に次のような論点があると考えられる。

○新たな対策水準の位置付け

○新たな対策水準を満足するための事業者の取組

○新たな対策水準が十分に満足されない場合の対応

（２）今後の対応

事業者は、デジタル検討チームの会合において本件への対応に必要な期間を具体的に示すなど、自律的かつ計画的に取り組む意向を表明している（別添１の３．（２）③及び別添２の２．（４））。そこで、当面の対応として、事業者から別添１の３．（１）

の内容を事業者自らの自主的取組でどのように実現されるのか公開の会合で提案を受けることとする。必要に応じて、進捗の状況を公開の会合で把握し、その結果を原子力規制委員会に報告する。また、（１）の論点についても引き続き検討する。

なお、継続的な安全性の向上については、「継続的な安全性向上に関する検討チームの設置について（令和2年7月8日原子力規制委員会資料３）」に基づき検討チームを設置して検討を進めることとしている。

＜添付資料一覧＞

別添１　発電用原子炉施設のデジタル安全保護回路に係る共通要因故障対策の強化について（検討チームにおける検討結果の報告）（令和元年度第69回原子力規制委員会資料４）　一部抜粋

別添２　発電用原子炉施設のデジタル安全保護回路に係る共通要因故障対策の強化について（第2回）～検討チームにおける検討結果の追加報告～（令和元年度第73回原子力規制委員会資料２）　一部抜粋

別添３　令和元年度第73回原子力規制委員会議事録　一部抜粋

別添１（令和元年度第69回原子力規制委員会資料４　一部抜粋）

発電用原子炉施設のデジタル安全保護回路に係る共通要因故障対策の強化について（検討チームにおける検討結果の報告）

令和2年3月11日
原 子 力 規 制 庁

1. 経緯と概要

発電用原子炉施設に用いられる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対策については、昨年9月13日に行われた第29回原子力規制委員会（以下「前回委員会」という。）において今後の取組方針が了承され、検討チームを設置して現行規制の見直しを検討することとなった[1]。その後、ATENA（原子力エネルギー協議会）や事業者、メーカー等の参加を得て計4回の検討チーム会合を開催し、現行規制を見直す場合の具体的な要求事項や経過措置について事業者意見を聴取しながら検討を進めてきた[2]。

これまでの検討チーム会合での議論等を通じて、現行規制の見直しの方向性について概ねの整理ができたことから、今般その結果を報告するとともに、原子力規制委員会の了承を得て、今後本件検討結果の規制上の取り扱いを具体化する作業を進めることとしたい。

2. 前回委員会で確認された事項

（1）現行規制の概要と現状認識

現行規制においては、ソフトウェア処理の簡素化や可視化、自己診断機能の実装、ライフサイクルを通じた品質管理、検証及び妥当性確認（V＆V）の実施といった、様々な品質確保措置が要求されており、これらを的確に実施することによりソフトウェア起因のCCF[3]が発生する可能性は十分低く抑えられている。さらに、SA対策の有効性評価を行う際には、安全保護回路がデジタル式であるか否かを問わず、何らかの理由により安全保護回路が原子炉停止系統又は工学的安全施設を自動的に作動させることができない場合でも重大事故等に対処できることを確認しており、現状においても災害防止上の支障はない。

その上で、事業者は、こうした要求事項を満たすだけでなく、ハードワイヤード機構（以下「Hw機構」という。）によるバックアップ設備を自主的な対策として別途設けている。

（2）継続的改善に向けた取組

近年、国内では、従来はアナログ式であった安全保護回路をデジタル化して取り替える事例が増えてきている。また、海外では、特に新設炉において、PLD（Programmable Logic Device）といった新たなデジタル技術を適用する事例も見られる。IAEAは、昨今のデジタル技術の進展や利用の拡大を踏まえて新たなガイドを策定し、I&Cシステムやアーキテクチ

[1] 第29回原子力規制委員会（令和元年9月13日）　資料1－1
[2] 「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」（開催履歴及び参加者は別紙3参照）
[3] Common cause failure（共通要因故障）

ャの共通要因故障について、多様性を確保することによってその影響を緩和できるようにするべきとしている。

これらを踏まえ、原子力規制委員会は、更なる信頼性向上を図る観点から現行規制の見直しに向けて検討を進めるよう原子力規制庁に指示した。本件検討に当たっては、検討チームを設置して事業者からの意見（経過措置に関するものを含む。）を聴取しつつ、今年度内を目途に具体的な要求事項の整理等を行うこととされた。

3. 検討チームにおける検討結果

前回委員会で了承された取組方針に基づいて、事業者意見を聴取しながら現行規制を見直す場合の具体的な要求事項や経過措置を以下のとおり整理した。

（1）具体的な要求事項

デジタル安全保護回路を設ける場合には、次に掲げるところにより、代替作動機能を有する装置（以下「代替作動機構」という。）を設けなければならないものとする。ただし、ソフトウェアに起因する共通要因故障が発生するおそれがない場合又は代替作動機構を設けることなく下記②の要件を満足する場合には、この限りでない。

①安全保護回路とは異なる動作原理の機構により、原子炉停止系統及び工学的安全施設を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ものとすること。

- 「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故障によってデジタル安全保護回路の安全保護機能と同時にその代替作動機能を喪失するおそれがない系統、機器その他の機構をいう。

②運転時の異常な過渡変化又は設計基準事故が発生し、かつ、安全保護回路の安全保護機能が喪失したときにおいても、発電用原子炉施設の安全性が損なわれることを防止することができるものとすること。

- 「運転時の異常な過渡変化又は設計基準事故が発生し、かつ、安全保護回路の安全保護機能が喪失したとき」とは、運転時の異常な過渡変化又は設計基準事故が発生した場合において、デジタル安全保護回路がソフトウェアに起因する共通要因故障によってその異常な状態を検知することできないとき又は原子炉停止系統及び工学的安全施設を自動的に作動させることができないときをいう。
- 「発電用原子炉施設の安全性が損なわれることを防止することができる」とは、最適評価により設計基準事故時の要件[4]を概ね満足すること又は炉心の著しい損傷を防止することができることをいう。

③共通要因によって安全保護回路の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、適切な措置を講じたものとすること。

[4] 許可基準規則第13条第2号を参照。

➢ 「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と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。

④外部電源が利用できない場合においてもその代替作動機能が損なわれるおそれがないものとするほか、重要安全施設[5]と同等の信頼性を確保したものとすること。

（2）経過措置

発電用原子炉施設のデジタル安全保護回路に関しては、現在、上記2.（1）のとおり、規制上の措置及び事業者による対策が講じられており、現状において災害防止上の支障はない。

このため、上記3.（1）の要求事項を規制に取り入れることは、更なる信頼性向上の観点からは効果があるが、安全上緊急の必要性まではない（現行の基準により災害防止上の支障はない）ことから、これを既存の発電用原子炉施設に要求する場合には、設置者が当該要求事項に的確に対応するために必要な期間を合理的に見積もって経過措置を設定しておくことが適当である。

そこで、検討チーム会合では、事業者に対して、現在自主的に設置しているHw機構が上記（1）の要求事項をどの程度満足しているか概略評価し、今後必要となると見込まれる追加対策の概要及びその追加対策の実施に要する概ねの期間について説明するよう求めた。事業者からは、別添1の資料を用いて概要以下のとおり説明があった。

① 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が、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、自主的に設置しているHw機構によって、殆どの過渡・事故に対して炉心損傷防止が可能である。

② 一方、大中破断LOCA[6]とソフトウェアCCFの重畳については、現状のHw機構では炉心損傷に至るおそれがある。このため、このような場合でも炉心損傷防止ができるよう、次のような追加対策を講じる。
・ABWR…運転員が早期に事態を認知できるよう、警報機能を強化する。
・PWR…現状のHw機構による手動操作に加えて、安全注入機能の自動化を図る。
なお、現状のHw機構で炉心損傷防止ができない場合でも、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。

③ これらの追加対策の実施に要する期間は、事業者ごとに異なるが、概ね2年程度を要すると想定している（設備改造は1回の定検で工事可能と想定。審査に要する期間は含まれていない）。産業界として、ATENAのガバナンスのもと、自律的に且つ計画的に取り組んでいきたい。

審査の形式で確認したわけではないが、検討チーム会合で聴取したところによれば、事業者が上記②の追加対策を講じれば上記3.（1）の要求事項を満足すると考えられ、事業者はかかる対策を現に講じる方針であると認められ、また、その実施に要する期間も不合理なものではないと評価できる。

---

[5] 許可基準規則第2条第2項第9号を参照。
[6] Loss of coolant accident（冷却材喪失事故）

4. 今後の予定

上記3. のとおり、現行規制の見直しの方向性について概ねの整理がなされ、これに対応するための産業界の取組姿勢も確認することができた。今後、原子力規制庁において、経過措置を含め本件検討結果の規制上の取り扱いを具体化し、改めて原子力規制委員会にお諮りすることとしたい。

（別紙）

別紙1　第29回原子力規制委員会資料1－1（令和元年9月13日、原子力規制庁）（抜粋）

別紙2　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会合資料1（令和2年1月29日、原子力エネルギー協議会）

別紙3　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会合開催履歴及び参加者

別添２（令和元年度第73回原子力規制委員会資料２　一部抜粋）

発電用原子炉施設のデジタル安全保護回路に係る共通要因故障対策の強化について（第2 回）
～　検討チームにおける検討結果の追加報告　～

令和2年3月23日
原子力規制庁

1. 経緯

発電用原子炉施設に用いられる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対策について、原子力規制庁は、今月１１日の第69回原子力規制委員会[1]においてこれまでの検討チーム[2]における検討結果等を報告した（別紙1）。その際、検討チーム会合で事業者側が示した追加対策の内容を原子力規制庁が要約して報告したが、その要約では追加対策の必要性に係る炉型による違いが明確でなかったことから、今後規制上の取り扱いを議論していく前提として、その内容を適切に補充して再度説明するよう指示を受けた。

2. 事業者側が示した追加対策

御指摘を踏まえ、検討チーム会合で事業者側が示した追加対策の内容を適宜再整理すると次のとおり。

（1）想定事象

ソフトウェアに起因する共通要因故障（CCF）により安全保護機能が喪失している状態で、単一の過渡事象又は設計基準事故（いずれも全事象が対象）が発生するものと仮定する。

（2）主な評価条件等

原子炉停止系統及び工学的安全施設は、デジタル安全保護回路を経由しない自動又は手動信号で起動させることができる（自主設備であるハードワイヤード機構（Hw機構）の故障は想定しない）。安全設備の単一故障は想定しない。

プラントの運転状態や原子炉制御室での運転員による操作時間は現実的に想定する。現場操作は現実的な時間余裕の範囲内で想定する。

（3）評価結果

①ABWR

通常運転時に上記（1）の想定事象が発生した場合には、アナログ式の代替制御棒挿入回路の起動信号により自動スクラムができる。その後、事態を認知した運転員が自主設備であるHw機構を用いて高圧炉心注水系を手動で起動し緊急炉心冷却を行うこととなるが、この手動操作が遅れれば炉心損傷に至るおそれがある。

冷却材喪失事故以外の場合には、事象発生から炉心損傷までの時間余裕が約30分～１時間程度あることから、現状のままでも炉心損傷を防止することができるが、給水配管の

[1] 第69回原子力規制委員会（令和2年3月11日）資料4
[2] 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

破断による冷却材喪失事故（最も厳しいケース）が発生した場合には、事象発生後14分程度で燃料被覆最高温度（PCT）が1200℃に達するおそれがある。

このため、運転員が早期に事態を認知できるよう、警報機能を強化する。これにより、事象発生後10分程度以内に運転員が事態を認知して高圧炉心注水系を手動で起動することができることから、確実に炉心損傷防止を達成することができる。

なお、上記（1）の想定事象のうち、原子炉起動時における制御棒の異常な引抜きについては、制御棒の引抜き操作は核計装指示値等のパラメータが静定したことを複数人で確認しながら少しずつ手動で行なうため、ソフトウェア起因のCCFにより計器類の指示に異常が生じた場合に運転員がこれに気付かず誤って連続的に引抜き操作をすることは現実的に想定し難いが、仮に誤引抜きが行われた場合でも運転員が所定の操作ボタンから手を離すだけで直ちに引抜き操作を中断することができる。

②PWR

上記（1）の想定事象のうち、早期に対処する必要があるものについてはアナログ式の自動回路を、10分程度の時間余裕があるものについては運転員による手動操作機構を自主設備として用意しており、現状のままでも炉心損傷を防止することができる。ただし、大中破断LOCAとソフトウェア起因のCCFの重畳については、その発生頻度が極めて小さいとして自主設備の対象外としており、現状のままでは炉心損傷に至るおそれがある。

具体的には、アナログ式の自主設備により原子炉圧力低で自動トリップはするものの、事象発生後1分程度（大破断LOCA時）でPCTが1200℃に達するおそれがある。現状の自主設備には高圧注入系を手動で起動する機構しか用意されておらず、時間余裕の範囲内で安全注入系を作動させることは現状では困難と見込まれる。

このため、現状の自主設備による手動操作に加えて、安全注入機能の自動化を図る。これにより、アナログ式の自動回路により時間余裕の範囲内で高圧／低圧注入系が自動起動することから、確実に炉心損傷防止を達成することができる。

③共通事項

現状のHw機構で炉心損傷防止ができない場合でも、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。

（4）実施時期

工事実施時期は事業者ごとに異なるが、安全解析に2年程度を要し、設備改造工事は1回の施設定期検査期間内で可能と想定し、次のとおりとする。（なお、審査に要する期間は含まれていない。）

対象プラント：デジタル安全保護回路を導入済み及び導入予定のプラント

- 再稼働済み又は2023年度までに再稼働するプラントは、2023年度以降最初の施設定期検査時
- 2023年度以降に再稼働するプラントは、再稼働時期まで

3. 今後の予定

今後、原子力規制庁において、経過措置を含む規制上の取り扱いを具体化し、改めて原子力規制委員会にお諮りする。