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
故障等に関する検討チーム
第３回会合議事録

令和元年12月4日（水）

原子力規制委員会

（注：この議事録の発言内容については、発言者のチェックを受けたものではありません。）

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３回会合

１．日時

令和元年１２月４日（水）１４：００～１５：４４

２．場所

原子力規制委員会　１３階Ｂ・Ｃ会議室

３．出席者

原子力規制委員会

山中　伸介	原子力規制委員

原子力規制庁

大村　哲臣	審議官
山田　知穂	核物質・放射線総括審議官
遠山　　眞	技術基盤課長
西崎　崇徳	技術基盤課　企画調整官
成田　達治	技術基盤課　課長補佐
山田　創平	技術基盤課　係長
小木曽　善一	技術基盤課　技術参与
川﨑　憲二	実用炉審査部門　安全管理調査官
照井　裕之	実用炉審査部門　安全審査官
村上　玄	実用炉審査部門　管理官補佐
今瀬　正博	システム安全研究部門　原子力規制専門職
関根　将史	システム安全研究部門　技術研究調査官
佐藤　滋朗	核セキュリティ部門　管理官補佐

原子力エネルギー協議会

富岡　義博	理事
谷川　尚司	部長

宮田　浩一　　部長

佐々木　茂夫　　副部長

東京電力ホールディングス株式会社

遠藤　亮平　　原子力設備管理部　設備技術グループ　課長

上村　孝史　　原子力設備管理部　原子炉安全技術グループ　マネージャー

関西電力株式会社

池田　隆　　原子力事業本部　電気設備グループ　マネジャー

田中　裕久　　原子力事業本部　原子力安全部門　安全技術グループ　チーフマネージャー

東芝エネルギーシステムズ株式会社

福本　亮　　原子力電気システム設計部

三菱重工業株式会社

内海　正文　　ＩＣＴソリューション本部　電気計装技術部　マネージングエキスパート

株式会社日立製作所

伊藤　孝広　　原子力電気システム設計部　主任技師

４．議題

（１）　発電用原子炉施設におけるデジタル安全保護系のソフトウエアに起因する共通要因故障対策について

５．資料

資料１　　現在検討中の代替作動機構（ＤＡＳ）に関する要求事項の案について～事業者からの主な追加質問とその回答～（原子力規制庁）

資料２－１　デジタル安全保護回路のソフトウエアに起因する共通要因故障への対応の考え方について（原子力エネルギー協議会）

資料２－２　多様化設備に対する主な意見（原子力エネルギー協議会）

資料２－３　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チーム第１回会合時のご質問回答（原子力エネルギー協議会）

参考１　発電用原子炉施設におけるデジタル安全保護系のソフトウエアに起因する共通要因故障対策について～多様化設備に係る要求事項の整理～（第１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資料１）

参考２　発電用原子炉施設におけるデジタル安全保護回路のソフトウエアに起因する共通要因故障対策について（令和元年度第２９回原子力規制委員会臨時会議資料１－１）

６．議事録

○山中委員　定刻になりましたので、ただいまから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3回会合を開催します。

本会合の議題は、発電用原子炉施設におけるデジタル安全保護系のソフトウエアに起因する共通要因故障対策についてです。

本会合では、まず原子力規制庁から、現在検討中の代替作動機構（DAS）に関する要求事項の案について追加の説明をし、続いて原子力エネルギー協議会（ATENA）から要求事項の案に対する意見等について聴取いたします。

それではまず原子力規制庁から、資料について説明を始めてください。

○西崎企画調整官　原子力規制庁の西崎です。

お手元の資料を御覧ください。通しページを振ってございますので、以降通しページの番号で御案内いたしますが、通しページの2ページでございます。この資料は前回の会合からこれまでの流れをまとめたものでございまして、1.のはじめにのところを御覧ください。

前回の会合では、私ども規制庁から、現在検討中の代替作動機構、以下DSまたはDASと略称いたしますけれども、こちらに関する要求事項の案をお示しいたしました。事業者側からの御質問を受けまして回答をいたしております。

それから今回の会合におきまして、事業者意見、これは経過措置に関するものも含みますけれども、こちらを聴取し、議論をするということになっておりました。その際、事業者側から前回お示しをした、そしてやりとりをしたわけですが、それだけでは全てを理解することが難しいということで、さらに質問できる機会を設けてほしいということで申し出がございました。

そこで私どもとしては、理解を深めることはこういった議論をする上で有意義であろうと思いまして、これまでに計4回の面談を行いまして、追加質問に対する回答を行っております。

以下、この面談でどういった御質問があって回答しているかというのを御紹介したいと思います。

2.でございますけれども、この面談で追加質問を受けたわけでございますけれども、その質問は主として前回の会合でのやりとりを、さらに詳細に確認する趣旨のものでございまして、特に新しいものはなかったと思ってございますけれども、主な質問と回答について御紹介したいと思います。

三つございますけれども、最初の問いは、判断基準を過渡・事故の全事象に対して炉心の著しい損傷防止としているのはなぜかと、こういった御質問でございます。これ前回会合でもやりとりがありましたけれども、その際もお答えしているんですけれども、改めてこの紙に書いてございます。

DASの有効性を確認する際には、運転時の異常な過渡変化及び設計基準事故の評価において有効に機能するものとしているデジタル安全保護回路が、ソフトウエア起因の共通要因故障によって、その機能を喪失するものと仮定をいたします。したがってこれは設計基準を超えるものではありますけれども、判断基準をその全事象に対して炉心損傷防止としている理由につきましては、安全保護回路が機能喪失をして、停止系・工安設を作動できなくなった場合に、DASがその機能を代替して、これらの設備を作動させるものでございますので、DASの有効性を確認する際には安全保護回路と同等の条件を課することが、安全上適当であろうと考えているからであります。

その上で炉心の著しい損傷防止を判断する具体的な基準としてお示ししているのは、この最適評価により現行基準13条2号の要件、いわゆるDBAの要件を概ね満足することを例示をしているというところでありまして、このことが、炉心損傷防止が達成できることを適切に確認できる他の判断基準、例えば37条であれば、SAの炉心損傷防止基準がありますけれども、そういった他の基準によることを否定するものでもありませんし、またこのソフトウエアCCFを設計基準に追加することを意味するものでもございません。

それから問2、二つ目でございます。

過渡・事故の全事象としているけれども、このRT・ESFを構成する機器の故障や誤作動が起因となって発生するものについてはどのように評価するのかと、こういった問いでご

ざいます。

このDASというのは、繰り返しになりますが、安全保護回路が機能喪失してRT・ESFを作動できなくなった場合に、代替してこれらの設備を作動させるものでありますので、このDASが作動させることとなる機器の全てが利用できないものとすると、当然DASの有効性を確認することができません。このため、RT・ESFを構成する機器の故障や誤作動が起因となって発生する各事象におきましては、DASが代替作動させることとなる機器の故障や誤作動が起因となることを想定する必要はなく、それ以外の構成機器の故障や誤作動が起因となって当該事象が発生するものと仮定して、DASの有効性を確認する必要性がございます。

問3、デジタル安全保護回路に用いられるソフトウエアとは異なるソフトウエアをDASに用いることは可能かと、こういった問いでございます。

DASに用いられるソフトウエアと、デジタル安全保護回路に用いられているソフトウエアとが、そのプログラムに未知の誤りや意図しない脆弱性が共通して存在する可能性がないことその他ソフトウエアCCFが生じるおそれがないことが明らかである場合には、御質問のようなものも可能であろうというふうに考えております。

これが4回の面談であった主な質問と回答でございますけれども、加えて3.はデジタル安全保護回路及びそのバックアップ設備の現地確認についての記載でございます。

私どもは、この検討チームにおける議論、検討に資することを目的といたしまして、先月15日、東京電力の御協力を得まして柏崎刈羽1号炉及び6号炉を現地確認しております。

1号炉はアナログのもの、6号機はフルデジタルのものでございます。中央制御室に設置されております安全保護回路やその関連機器や計器類、それからバックアップとして自主的に設置されておりますハードワイヤード設備などの現地確認を実施いたしております。

そのときに、現場で働かれている方から幾つかお話を聞きましたので、3点ほど御紹介をしたいと思います。軽微なものではございますけれども、不具合というのはアナログよりもデジタル式のほうが多いという印象があるということ。それから6号機に関してデジタル技術の進展は目覚ましいので、概ね10年ごとにシステムの大幅な更新を実施しているということでありました。

一方、アナログ式のほうなんですけれども、アナログ式だからといって信頼性が低いとか、そういうことではなくて、実際に、アナログ式の安全保護系は建設当時から大幅な取り換えを行っていないということでございました。御紹介しておきます。

規制庁からの説明は、以上です。

○山中委員　それでは、次に原子力エネルギー協議会（ATENA）から、要求事項の案に対する意見等について聴取したいと思います。

資料について説明をお願いいたします。

○原子力エネルギー協議会（富岡）　それではATENAの資料1というものについて御説明したいと思います。

前回の会合で実際に安全解析を行ったり、それからその対策の工事に必要な経過措置期間というようなものを議論していくというようなことがあったかと思いますけれども、今現在安全解析を実施しているところでして、それを踏まえてさらにその安全解析から出てくる、判断される対策ということも判断した上で、それに必要な経過措置期間ということをお示ししようと思っていますので、それについては、いましばらくお待ちいただければというふうに思います。

一方この資料1は、デジタル安全保護系のソフトウエアに起因する共通原因故障というようなことの問題に対して、どのような考え方の筋道で考えたらいいのかということをきちんと整理しておくということが非常に重要だと思っております。安全設計においては、安全設計を考える上で考え落としがないかどうかというようなことを確認しながら進めることが非常に大事ですので、この資料でその考え方の筋道を固めていきたいということを意図して出しているものでございます。

具体的には、安全保護系のソフトウエアに起因する共通要因故障と、そもそも独立であるべき安全保護系が共通要因故障でFailするというようなことは、まずデザインベースの範囲ではあってはならないようなことなんですが、さらにそれを考えたとして、一体どういう安全対策を講じていけばいいのか。その問題は一体どういう性質の問題で、どういうプラントに影響があって、それを対処していくにはどういうふうにしてやったらいいのかというところの、考え方の筋道をきちんとしておくということが非常に重要だと思っておりますので、この資料を用意いたしました。これについてちょっと御説明させていただきたいというふうに思います。

○原子力エネルギー協議会（谷川）　ATENAの谷川でございます。

資料2-1について以下御説明いたします。5ページに行っていただきまして、ATENAの基本的な考え方については、安全保護回路は、これはもう重要な設備でありまして、この信頼性を高めて安全確保を確実にするということは、ATENAとして非常に重要だと考えてお

ります。

本資料では、安全保護回路の信頼性向上に取り組み、並びに課題でありますソフトCCFのリスクに関する考えを述べたいというふうに考えております。

7ページに行っていただきまして、デジタル化の意義というのを、もう一度簡単に御説明したいと思いますけれども、これは信頼性向上や保守性の向上を目的にデジタル化を進めてきたということでございます。どれぐらいアナログに対してデジタルが、信頼性が向上したのか。

アナログも当然ながら信頼性は高いんですけれども、例えばアナログでは1 out of 2 twiceの回路が、デジタルでは2 out of 4を組んだ場合には、アンアベイラビリティで言うと2桁ほどよくなるという結果が載っております。また、経年変化はアナログではどうしてもありますけれども、デジタルのソフトのところは経年変化はないということで、保守性の向上にもつながるということになります。

8ページに行っていただきまして、デジタル化に伴ってハードウエアの信頼性は向上するわけですけれども、ハードウエアだけではなく、ソフトウエアに起因する故障が内在する可能性があり、このためにソフトウエアの故障防止に取り組みを行ってきたと、それによって全体の信頼性の確保をしてきたということであります。ハードウエアの故障の要因は内的要因、外的要因あって、これが試験などによって信頼性を確保してきたということでございますけれども、ソフトウエアについてはプログラムやコンパイラに不具合が残った状態で製作される。あるいは製造段階で購入するというモードがありまして、それに対する対応を次ページ以降に進みます。

9ページに行っていただきまして、故障への対応としまして、故障発生要因を踏まえて開発段階から運転保守まで対策を打ってきたということであります。設計開発段階ではソフトウエアの不具合をつくり込ませないための対応ということで、ソフトウエアの構造を単純化する、視認性を向上した言語を適用する。人の介在を不要にするようなコーディング作業、介在を不要化する。それからFMEA評価に基づいた自己診断機能を設けるということと、次の製造・検証段階と同じですけれども、不具合がつくり込まれていないことを確認するための対策として、V&Vをきちんと実施するということ。それから運転・保守段階では、これはもうマスターロムといいまして、製造段階でつくった状態と今の装置が同じだということを、機械語のレベルできちんと確認をするということと、機能試験とか設定値確認試験を行う、それから運転中は常時自己診断を行い、健全性を確認するということ

を行っております。

次にソフトウエアCCFリスクの考え方について、11ページで示します。安全保護回路の中では、常時10msec～200msec程度の周期でジョブを行っているということになります。そういうジョブの中で、ソフトウエアCCFに起因する故障は1度も発生していないということであります。

じゃあどれぐらいの信頼性かということですけれども、EPRIのレポートにハードウエアとソフトウエアの故障の比率というのがありまして、総故障の2%がソフトウエア故障ということですけど、保守的に1割がソフトウエア故障ということで先ほどの10^{-6}/demandがハードウエアだとすると、ソフトウエアの要因の故障は10^{-7}程度、1桁ぐらい低いところにあるだろうということで、安全保護系の回路が不動作になる可能性としては、ソフトウエアのCCFにより、そういうことが起こる可能性は、これは十分に低くて、設計上の残存リスクとして捉えることが適切であろうというふうに考えております。

12ページに参りまして、そういう低いもののソフトウエアCCFが起こったときにどうなるかということをしっかり踏まえた上で、対策をしていく必要がありますけれども、起因事象が発生しまして、ソフトCCFが発生すると。そうしますと、原子炉停止失敗、あるいはECCS作動失敗ということで、炉心損傷のリスクが大きくなっていくということであります。

ソフトウエアCCFの発生頻度は十分低いとは思っておりますけれども、それに対してこれまで自主的な対策設備を設けてきたということで、それによりまして多様化設備が働きまして、原子炉を自動停止、あるいは炉心冷却系の手動起動が行えるようになりまして、そして炉心損傷のリスクを、大幅に低減することができているというふうに考えております。

次のページに行っていただきまして、そういう多様化設備の有効性について、過渡または事故とソフトウエアCCFが同時に発生した場合に、どこまでの事象に対応できているのかということを、現状の設備に対して検討した結果が下記の表になります。

まずBWRですけれども、制御棒系の過渡・事故でありますけれども、これは例えば連続引き抜きは実施していないんですけども、実際の手順は抜き操作なんですけれども、評価想定は連続引き抜きをしているとか、あるいは制御棒引き抜けのときにはラッチ機構でとまるようになってはいるんですけども、制御棒落下するというシナリオでやっているというところがありますので、そういうところについて少し検討していく必要があるのかなと

いうふうに思っております。

それから過渡・事故、それから小LOCA、中LOCAに対しましては、自動停止により対応可能だということと、炉心冷却についてはHPCFの手動起動で対応できる。当然ながら過渡よりも事故、あるいは小LOCAよりも中LOCAのほうが、時間的余裕が小さくなってくるという特性はありますけれども、基本的には対応可能だと。大破断LOCAになりますと、同じような自動停止と手動で、高圧系を立ち上げるということですけれども、これもやはり中LOCAに比べて、さらに時間的余裕は小さくなっていくというのがBWRの結果といいますか、評価でございます。

PWRにつきましては制御棒系の過渡、それからLOCA以外の事故、それから小LOCAに関しましては自動停止により停止が行われるということと、高圧系の補助給水系の自動作動、あるいは高圧注水系の手動作動により対応は可能であるということですけども、中LOCA、大破断LOCAになりますと、事象が早いということもありまして、手動操作での対応は非常に厳しいというふうに現在見ているところであります。

一方、中破断LOCAに関しましては、これは決定論的な評価は、課題はあると思っておりますけれども、もともと発生頻度が10^{-5}/年というふうに小さいということと、ソフトCCFの発生確率も10^{-7}/demandと、非常に小さいという、重畳事象であるということを踏まえると、残存リスクは、これは十分小さい状況にあるのではないかというふうに考えております。

14ページに行きまして、じゃあそういうソフトウエアCCF対策、これから安全解析をきちんとやって、結果を出していくということなんですけども、その解析の結果をもとにして、対策を考えていくというフェーズに入っていくわけなんですけれども、まず状態1から当然CCFの発生を防止して状態2への遷移を抑えるというところ、それからそれでもCCFが発生した場合に、対策設備でそれを緩和していくということ。それでも炉心損傷を超える場合には、さらなる対応ということで、今SA設備などによって対処していくという、これは深層防護の基本的な考え方だと思いますけれども、これから安全解析の結果をベースにして検討を行う場合にも、真ん中の緩和系だけではなくて、プリベンションをどうしていくのか、あるいはさらなる対応をどうしていくのかということを、しっかりバランスのとれた検討をしていきたいというふうに考えております。

次にデジタル装置の規制に関する海外の動向について御説明したいと思います。

米国の規制は、ソフトウエ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、近代化を今検討しているという段階にあります。もともとCCFの定義ですけれども、1979年のsWestinghouse社の安全保護回路にCCFの懸念があるということで、多様性の評価を行ったというのが最初でありまして、それから1990年に第三世代の炉、例えばUSA BWRなどで、デジタル安全保護系を導入することに対して、デザイン・ティサーティフィケーションの審査の中でいろいろ議論がされてきたと。

多様化対策を求める方針などがここで定められてきたということと、2000年代に入りまして、オコニーのPWRの発電所においていろいろ議論があったわけですけども、ここでは最適評価の概念、単一故障を想定しないとか、非安全系のクレジットを可能とするというようなところが追加されたという経緯があるわけですけども、2016年になって規制の近代化の対応として、ソフトウエアの信頼性をもとにして、CCFの考慮を排除することを可能とするプロセスも導入されつつあるということ。

安全上の重要性の考慮、安全系とそれ以外の系統に分けて、グレーデッドアプローチをとるというやり方、それから多様化設備にかわる措置、これはダイバーシティというのは装置だけではなくて、人間の操作というものもダイバーシティに入ってくるわけですけれども、例えばLBBを前提とした大LOCA向けの設備対策の除外なども議論されているところだというふうに認識しております。米国以外を見ても、英国、フランス、フィンランドにおいて、決定論的な解析から大破断LOCAを除外する等の絞り込みを行っている国も見られるという状況であります。

それから17ページに行きまして、先々週行われました米国の規制諮問会議、ACRSにおいても、これまでのスタンダード・レビュープランであるBTP7の改訂ドラフトが紹介されました。これも来年度に最終改訂版が出される見込みだということです。その中で先ほども挙げましたグレーデッドアプローチとか、CCFの考慮を除外可とするプロセスが追加されるということ。

また民間としても、NEIが適切な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ということの議論が重要であるということで、ガイドをつくってやるとかいうことをやっている。ソフトウエア品質プロセスとか、設計要求とかで対応できないかということを検討している。EPRIもCCFの要因分析ということを見ているというのが米国の最新の状況でございます。

19ページに行きまして、今後の議論の進め方ですけれども、今回は安全保護回路が有するソフトウエアの信頼性というのがどれぐらいの数字に行くのかというところの水準を

示したものと考えております。ソフトウエアCCFが発生した場合のプラントの安全への影響とか、多様化設備の有効性については、現在完全解析を行っておりますので、次回詳細な評価結果を示すことができるというふうに思っております。

今後これらの評価結果など、あるいは規制化に伴う影響も踏まえまして、深層防護全体でバランスがとれた対策を検討することが重要だと考えておりまして、どんな影響かというと、安全保護回路から耐火設備には、安全保護回路の改造がどうしても発生しますので、複雑な系になったり、信頼性が損なわれないかというおそれの検討とか、デジタル安全保護回路導入のプラントで、デジタルの判断に対して何か影響が出ないだろうかということも踏まえた上で、今後安全対策を提案していきたいというふうに考えております。今後の進め方としては、安全保護回路の信頼性も踏まえて、深層防護全体で見て、どういう対策を講じることが一番効果的かということで、次回の会合で議論させていただきたいというふうに考えております。

それから次の参考資料ということですけども、次回も御説明した内容もありますので、簡単に説明したいと思います。

23ページ、右下行きまして、ソフトウエア信頼性の向上策というのは設計・製作の信頼性、自己診断による異常検出、それから工場試験・定期的な試験によってしっかりやるということで、高信頼性を保っております。

24ページに行きまして、ソフトウエアの構造がございますけれども、OSに対しては定周期処理、非常にシンプルな構造にしているということ。それから他産業でも使って問題が出ていないOSを使用しているということ。それからOSの上に乗っているアプリケーションに対しては、シングルタスクで割り込みなしをしているということで、極力シンプルな構成として複雑性を排除しているということと、言語としてはPOLを用いまして、画面上でAND/OR回路を結成するという形で設計ができるようにしております。

視認性を向上するということで、これによりましてV&Vを非常にやりやすくしたと、間違いを発見しやすくしているということと、POLで作成した専用回路を自動的に機械語に落とすということで、ここで人の介在を不要化しているということで、全体的に信頼性を上げていると。

25ページはV&Vの話なんで、これ前回説明したので省略いたします。

26ページは、じゃあ自己診断で異常検出をどのようにやっているかということですけれども、これはハードウエア、OS、その上に乗っかるアプリということですけども、一言

で言いますと、ハードウエアがOSの動きを監視して、OSがアプリケーションの動きを監視するということで、異なる区分が別の区分のやっていることをしっかり監視するような形のことをやっておりまして、それが1～8番まで書いてある診断をやっている。診断対象も例えばアプリケーションの周期監視だったり、OSの周期監視とか、伝送の状態をやっていると。それで異常があったときには、ハードウエアがOSの異常を検知しているハードウエアが警報を発する。OSがアプリの異常を検出したら、OSがannunciatorを出すということで、正常なところが警報を出すということで、確実に告知できるようにしているということであります。

27ページへ行きまして、開発・検証段階ではそれぞれハードウエアの検証、ソフトウエア、OSの検証、それからハードとソフトを組み合わせた検証を行い、製造検証段階では単体試験、組み合わせ試験でインターロック動作確認をすると。現地に行ってもソフトウエアを復元して同じような試験をやる。

定期的な試験、定期検査においては先ほども言いましたけれども、ロジックに変化がないことを機械語のレベルで確認をするということと、模擬信号を入力して起動試験を行うということ、月例テストでもやるということで、ソフトウエアが工場出荷時の状態を保持していることの確認をするとともに、インターロックの動作についても、具体的に信号を入れて確認をしているということをやっております。

以上の話をまとめたものを29ページに示しておりまして、ソフトウエアCCFの要因というのは、OSに内在する不具合、あるいはコンパイラなどに内在する不具合、アプリケーションソフトウエアに内在する不具合などもあるとは思いますけれども、それに対して設計・製作段階での対応に検証、それから自己診断による異常検知と、その3本柱でソフトウエアについてつくり込まない、あるいは起こったとしても、それを検知するということで対応してきたということであります。

ではどれぐらいの信頼性が実績としてあるのかということですけども、これは多重化された制御装置、原子力の安全保護系、あるいは常用系、それから火力などで適用されたものの国内の運転実績は、約7億時間程度に及びまして、この間、ソフトCCFは発生しておりません。仮に0.5回発生したとすると、ソフトCCFの発生頻度は6.4×10^{-6}/年というふうに評価されますので、十分信頼性が高くて、ソフトウエアCCFが起きる可能性は極めて低いということは、もう言っていいのではないかというふうに思っております。

それから次に、多様化設備に対する主な意見ということで二つほど、火災、溢水に対す

る意見と、デジタル安全保護回路に対する代替機能に対する意見について御説明したいと思います。

32ページが火災、溢水に対する意見でありまして、前回の会合において共通要因によって安全保護回路と同時に、代替作動機能が損なわれるおそれがないという手段を講じることということで、補足のところに火災により設計基準事故等が発生する場合には、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な設計にすることという補足が書いてあります。

それを踏まえた意見としては、ソフトウエアCCFは非常に発生する可能性は小さい、残存リスクであるということなんですけれども、シングル系ということもありますので、火災から発生する起因事象ということを考えますと、それ自身にさらにソフトCCFを考えると、対応する設備がなくなってしまうということもありますので、火災、溢水が発生しても、これDB設備で安全停止機能を確保するということと、多様化設備自体が火災・溢水の影響を受けたとしても、これもDBの設備で影響防止を図っていくということが基本だというふうに思っております。

次のページ、33ページに簡単な考え方を示しておりまして、左が設計基準事故の対応設備の場合は、当然DBは安全保護回路A、Bがあった場合に、当然火災があっても離隔距離をとってありますので、片方がやられてももう片方で収束をするということです。多様化設備の場合は、例えば安全保護回路Bに多様化設備がついていて、安全保護回路Bの近くで火災が発生して、ここから分岐した多様化設備、その影響で機能が喪失するという事象が発生した場合に、さらにそれが起こって起因事象が起こったというのに、さらにソフトウエアCCFを重畳して考えますと、安全保護回路Aのほうも動作しなくなるということになりますので、それはやはりシングル系では対応できなくなるということで、こういう過程は必要ないだろうというふうに考えております。

それから次のページは内部溢水でも同じ話でございます。CCFが重畳することを、溢水などと重畳して考えないということでございます。

それから次のページが、安全保護回路に対する代替機能について示したものであります。これも前回の資料には安全保護回路と異なる動作原理の機構ということで、要求事項の考え方としては、ソフトウエアを用いた回路であっても、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、代替機能に含めていいのではないかというふうに考えておりまして、当然ハードワイヤードでの物はソフトはないということ

ですが、ソフトを含むものでも共通部分を有しなければよいのではないかというふうに考えておりまして、それが36ページに絵を示しております。

デジタル安全保護系がハードウエア①・OS①・アプリケーション①という場合に、代替作動機能を有する設備が異なるハードウエア・異なるOS・異なるアプリケーション、設計、製作したものであれば、これは代替機能を有するというふうに評価していいのではないかというふうに考えておりますし、当然ながらPGAを使う場合はこれはマイクロプロセッサとは物理的に異なるものだということと、その上にアプリケーションも異なるものだということが言えると思いますので、これも代替機能としての適用が可能だろうというふうに考えております。

それから次の資料2-3ですけれども、これは第1回会合時にいただいた御質問に対する回答でございます。

38ページに行きまして、どんな御質問だったかということですけれども、多様化設備がどのように接続されるのかを具体的に示してほしいという話と、デジタル安全保護回路の異常検知について、詳細を示してほしいという二つの御質問に対して回答したいと思います。

40ページに行きまして、多様化設備の構成ですけども、BWRとPWR、若干違うので比較して示しております。まず原子炉スクラムトリップですけども、BWRの場合は中央制御室、主盤の上に手動操作ボタンが二つありまして、そのボタンを押しますとスクラムソレノイドの電源がそれぞれA系、B系がoffになりまして、スクラムが入ると。これは赤の部分です。これがデジタル安全保護回路になりますので、そこは通らずに直接A系、B系に信号が行く形になります。

PWRにつきましても基本的には同じでありまして、まず中央制御室の主盤に手動操作のボタンがありまして、原子炉トリップ遮断器器を解放する形の操作ができるということと、多様化設備にも手動操作ボタンがありまして、出力回路を通してそれができるということと、もう一つはセンサから分岐した信号を用いまして、設定値、比較回路、自動化の回路を通して自動的にトリップに行く回路、これも安全保護、デジタルの部分、ソフトウエアの部分を通らない出力回路を通ってトリップが行われるということでございます。

それから41ページに行きまして、MSIV閉鎖につきましても、BWRは主盤の上から手動隔離が出力回路を通して行えるということと、PWRにつきましても多様化設備、あるいは自動設備、センサから分岐した信号を用いた自動化設備により、出力回路を通してMSIV閉が

行われるというところであります。

それから工学的安全設備、高圧注水系の起動ですけれども、BWRは指示系はセンサから分岐した指示系、多様化設備についておりまして、手動操作は切りかえ回路、中操にスイッチがついていまして、スイッチを切りかえることによって、手動操作でHPCFポンプを起動することができるということです。

PWRにつきましても、センサから分岐した指示系が中操にあるということと、多様化設備の操作スイッチがありまして、出力回路を通して直接高圧注入ポンプの起動に行けるということで、そういう形で信号を分岐して、ソフトのロジックを通らずに直接起動できるような対策を行っているということでございます。

それからATWS対策設備ですけど、BWRにつきましては、これはセンサから最後の末端のところまで、ダイバースで設計をしております。上にあるのが安全保護系の原子炉緊急停止系のところですけれども、下にあります青い部分、これがアナログでつくっておりますATWS対策設備でありまして、異なるセンサを用いて異なるスクラムパイロット弁ですか、異なる部分を信号を与えて、そこで代替制御棒を挿入するという回路を取っております。これは自動的に制御棒が挿入できるようにしております。PWRは先ほど示したものと同じように、センサからの信号を分岐して自動的に出力回路を通してタービントリップなどを行える形にしているということでございます。

44ページ以降、参考がついていますけども、少し細かい話になりますので、割愛させていただきます。

それから50ページに参りまして、2番目の自己診断と異常検知の警報の関係について御説明いたします。

これは先ほど簡単に自己診断について御説明しましたけれども、これはプロセス値の入力から設定値比較、論理回路出力ということまでの、安全保護系に含まれるそういう機能といいますか、各機能に対してどういう故障が発生するのかという分析をしまして、それに対して自己診断機能を設けております。異常が発生した場合にはそれを検知して警報を発報するという機能を有しております。これは後でまた細かく御説明します。

自己診断機能は異常発生箇所と異なる検出部、先ほど示しましたようにハードはOS、OSはアプリケーションという形で、異なる部分で、検出部で監視するということで、万一異常があってもそれをきちんと検知して中央制御室に警報として告知することができます。万が一警報設備に対する伝送異常が発生した場合には、逆に受信側の設備で異常を検知で

きますので、そういう異常があったということは警報の発報により運転員は認知できるということになります。

52ページに行っていただきまして、これが緊急停止系の構成（例）でございます。左側にありますプロセス入力値、アナログ信号が入ってきたものをA/D変換をして、それを伝送をして設定値比較回路に持っていくと。真ん中に比較というのがありますけど、ここでスクラム設定値に達したかどうかをチェックして、達した場合にはまたそれを伝送して、論理演算部に持ってきて、論理演算というところで2 out of 4を組むと。そこでスクラムが成立しますと、インターフェース、I/Fと書いてありますところでスクラムのロジックのところに持っていくということであります。

それぞれ上に書いておりますプロセス値入力、あるいは工学単位変換など、A～Kまでのいろいろ機能を有しておるわけですけれども、それぞれに対して異常診断を行っているということと、そこで異常が見つかった場合には、論理演算部の真ん中に伝送という機能がありますけれども、これをネットワークに乗せて計算機のメッセージとして表示をしたり、大型表示盤に警報表示をすると、原子炉は保護回路以外の設備で警報を表示するという対応をしております。先ほど申し上げましたけど、万一伝送異常が発生した場合には、この保護回路以外の設備で、その伝送異常を見つけることができるということでございます。

53ページはちょっと細かくて申し訳ないんですけれども、先ほど示しましたA～Kまでの機能に対して、どういう項目の異常診断をしているかということと、それが診断対象は何なのかと、入力信号なのか、コンバータなのか、CPUなのかということと、それをどこで検出しているのか、ハードウエアなのか、OSなのかというのが示してありまして、運転員の告知が何によってなされるのか。あとそこはV&Vとか試験でチェックしているのかということと、それがきちんとされているのであれば、ソフトCCFとしての異常が未検出で残存する可能性はどうなのか。×というところは、これはもう極めて小さいだろうということでございます。

54ページも同じような表が載っておりますけども、もしあるとすればOSの異常、コンパイラの異常があって、例えば周期動作、ウオッチドッグタイマによる異常、それからCPUの命令チェックとか、いろいろやっているんですけども、それをすり抜けていくようなもの、もしあるとすればこういうところかなという感じです。それも可能性といいますか、想定というぐらいでありまして、実際にこういう事象が起きているわけでは決してござい

ません。

以上でATENAの説明を終わります。

○山中委員　それでは質疑に移りたいと思います。質問、コメントございますか。

○照井安全審査官　規制庁の照井です。

まず通し30ページの資料2-2から確認させていただきたいんですけども、今、多様化設備に対する主な意見ということで2点挙げられていて、一つが多様化設備の信頼性確保の考え方と、デジタル安全保護回路に対する代替機能ということで御意見として挙げられているわけですけれども、この二つ挙げられている御意見というのは、我々のほうの資料1の問2と問3に相当するものだと思っているんですけれども、そうすると我々資料1、通しの3ページですけども、今ここに考え方を示させていただいていますが、この考え方を踏まえた上で、御意見というのは解消されているのかどうかというのをお伺いしたいんですけれども。

○東京電力HD（遠藤）　東京電力ホールディングスの遠藤と申します。

そういう意味では、1点確認させていただきたいんですけども、3ページのところで後半のところだと思うんですけども、まず火災影響を踏まえた場合の、DASが代替作動させることとなるRT・ESFの構成機器の故障や誤作動が起因となることを想定する必要はないということは、例えばHPCFのバックアップ設備の火災は想定する必要はなくて、そこが火災のときはB系でカバーできるからいいですよと。そういう認識でよろしいですか。

○照井安全審査官　規制庁の照井です。

あくまで評価上、DASの機能を評価するときに、DASが、動かすための機器を壊したことでもって起因事象が発生するということを想定すると、当然DASが動かなくなるわけですから、そこについてはそのDASが有効に機能するかということが確認できなくなりますので、おっしゃるとおりC系のDASの機能を評価するという意味で、バックアップしているC系の故障を想定する必要はないということになります。

例えば、そちらの資料で言うところの、通しの33ページの絵で言いますと、真ん中の絵を使いたいと思いますけど、真ん中の絵で言うと、多様化設備が動かそうとしている機器の機能喪失によって起因事象が発生するという場合は、当然DASも死んでいるので、DASの機能は見れませんということで、それは評価としては見なくていいですということになります。

一方で、今この絵で言うとA系のほう、A系のほうの火災で起因事象が起きるというこ

とになれば、そのときにはCCFが発生をして、DASによってその過渡事故に対して対処できるということを確認できれば、DASというのは有効に機能するということが確認できるわけですから、そういう評価はしてくださいと、そういう意味になります。

○東京電力HD（遠藤）　東京電力ホールディングスの遠藤です。

理解できました。承知しました。それであれば、大体考え方は、認識は合っているかと思います。

○東京電力HD（上村）　東京電力ホールディングスの上村でございます。

今の質問に関連してなんですけれども、これからLOCA解析なり、いろいろお示しをしていくんですけども、今のお話は配管も同じことが生じるんです。例えば今事故解析ですとHPCF破断というのを想定していて、そのHPCF破断というのと、このハードワイヤードで期待している系統の配管ですよというふうになると、注水できる系統なくなっちゃうんですけど、そこも重ねる、重ねないというのは、現時点で何か御意見なりお持ちなんでしょうか。

○照井安全審査官　規制庁の照井です。

今の御質問は、動的機器とかDASが持つ制御ケーブルだけじゃなくて、もともと動かそうとしている補機側の、ある種、静的機器の破損という意味でいいですか。

○東京電力HD（上村）　そうです。

○照井安全審査官　恐らく多分ABWRでやると、大LOCAとしてはHPCF系の配管破断を想定しているわけですね。そこでDASで動かそうとしている高圧系の配管破断を想定すると、当然DASの機能を見れないわけですから、そこは見なくていいということになりますけど、これで御回答になっているでしょうか。

○東京電力HD（上村）　はい、十分です。ありがとうございます。

○山田統括審議官　今の議論なんですけども、HPCF系の配管が破断して起因事象が発生したときに、それは設計基準事故ですよね。そのときに設計基準事故を収束しますかというときに、単一故障を想定して、それ収束するんでしょうか。

○東京電力HD（上村）　東電の上村です。

御質問は通常の、今の安全解析という御趣旨ですか。なのでHPCFには期待していない、低圧注水系側での注水で冠水を維持したまま、PC値は1,200℃を超えないという結果になっています。

○山田統括審議官　ですね。ですからそうだとすると、一番最初のほうに話があったDAS

に期待しなくても事故は収束できるような場合にいくんだと思うんです。

ちょっと先走っているんですけど、33ページの多様化設備の、ここでいろいろ議論が展開されていますけれども、これもちょっと違和感があるのは、DASの回路のところ、火事で機能喪失しましたといったときで、それで起因事象が発生しましたと書いてあるんですけども、そうしたときには基準上は、この起因事象が発生して、Transientが起きているとすると、単一故障を想定して事象を収束させてくださいという要求になっているので、そもそもここでA系1本だけしか残っていませんよという仮定で御説明されているんですけれども、そもそも前提がそういうことは基準上許されていない状況になっているものを持ってきて御説明されているように見えるので、議論に違和感があって、ここで御主張されていることは、よく理解できないんですけど。

○東京電力HD（上村）　東電の上村ですけども、事故解析の件でいいますと、今の事故解析、LOCA解析はHPCFの配管を破断の仮定をして、もう1個は、もう片一方でHPCF、2系統ありますから注入できるところを、そこを単一故障想定で使えないという想定をして、低圧で入れるということをしております。

それはネットワークで動くんですけど、そのネットワークがデジタルのCCFで動かない場合に、炉心損傷防止を達成してくださいというのが、前回の会合での御要求だったというふうに認識をしていますので、DASに期待をしないと、これはクリアできない事象になるんです。

だから低圧系が注水しますという今の解析が、低圧系の自動起動インターロックがデジタルのCCFによって起動しなくなるので、そのかわりとして何らかバックアップでの対応ができますかということを問われていると。

○山田統括審議官　規制庁の山田です。

今のお話を伺っていると、HPCFと低圧の注入系が、共通要因故障で両方とも落ちる設計になりますということですか。

○東京電力HD（上村）　東電の上村です。

デジタルのCCFを前提にすると、ECCS、工学的に作動させるためのインターロックは使えないという前提になるので、そのもの自身が使えないのではなくて、そのもの自身をキックさせるための信号が出ないということです。

○山田統括審議官　とすると、高圧系と低圧系が同じデジタル安全保護系で動かされていますということを御主張になられているんですか。

○東京電力HD（上村）　東電の上村ですけど。

いえ、これはCommon Cause Failureですから、Common Causeでよくわからないけども、最後残るアンノウンによって全てのインターロック、安全保護に関するデジタルのインターロックが動かないという前提に立ったときに何ができますかというのが、今の議論です。

○山田統括審議官　Common Causeで低圧系と高圧系が一緒に落ちるような制御系になっていますということですか。

○東京電力HD（上村）　Common Causeというのは、そういうことですね。

○東京電力HD（遠藤）　東京電力ホールディングスの遠藤です。

基本的には高圧系も中圧系も同じ制御回路で制御するようになっています。それが多重化されていて、今回の共通要因故障というのは、その多重化されたものも全て機能しないということを前提としているというふうに認識しております。

○山田統括審議官　御説明されていることは理解できましたが、それはこちらで想定していることとの関係で、皆さん理解ができたでしょうか。

○東京電力HD（上村）　東電の上村ですけど、こちらからすみませんが、今までその認識は共通のもと、議論が進んでいますので。

○西崎企画調整官　規制庁、西崎です。

我々もそういう認識で議論してきたかと思います。

それで、もしよろしければ今問2の話だったんですけど、問3については。今と関連すると思うんで。RPS、安全保護回路とDASが異なるソフトウエアの場合の考え方をお示ししているんですけれども。

○東京電力HD（遠藤）　東京電力ホールディングスの遠藤と申します。

その点についても1点確認させていただきたいと思っていまして、今日お示しいただいた資料の中では、共通要因故障が発生しないということが前提になっておりますけども、そこの前提がどうかというところを少し具体的に、要はデジタルだから全部一緒で、共通要因で、必ず一緒に落ちますというところはちょっと行き過ぎかなというふうに考えておりまして、資料の36ページに示させていただいたように、基本的にはソフトウエアは設計・製作という段階での問題点というところだと思いますので、設計・製作が異なる部分であれば、共通部分というのは基本的にはないだろうというふうに考えています。

ですので、これポンチ絵なのであれですけど、ハードウエア・OS・アプリケーション、それぞれ違ったところで設計されて、違ったところで製作されたものであれば、共通要因

故障が同時には起きない。一つ一つは起こり得ると思うんですけども、それが同時には起きない。

同時に起きなければ、片側は機能として維持されると、そういう解釈は問題ないのではないかな。今回の議論の中では問題ないのではないかなというふうに考えていまして、もう少し具体的に言うと、ほかのメーカで設計・製作していて、共通部分がないと言えるところは、代替機能として採用しても問題ないのではないかというふうに考えていまして、その辺の共通要因というところの解釈を少し補足いただければと思います。

○照井安全審査官　規制庁の照井です。

資料1に書いたとおりのことなんですけれども、基本的に今そちらの資料で示されている、ややポンチ絵で色を変えているので、違いますよという感じを出されているんですけど、結局我々のほうの資料の考え方、答えのほうに書かせていただきましたけど、当然そのソフトウエアに起因する共通要因故障が生じるおそれがないということが、それは疎明できれば、それは妨げられるものではないというふうに考えていますけれども、ただ今おっしゃっていた、例えばメーカが違いますということで、本当に共通要因が起きないのかとか、そこに関する疎明をしていただくということはセットだというふうに考えております。

○東京電力HD（遠藤）　東京電力ホールディングスの遠藤です。

そこは具体的な部分なので、なかなかお示しいただくのは難しいのかもしれませんけども、結局そこが結構ポイントなんだと思っていまして、共通要因が起こらないということは当然大切な部分なんですけど、それがどういう要因か、デジタル一くくりになっちゃうと、どれも全部同じになってしまうので、そこは審査の中でという議論なのかもしれないんですけど、もう少し具体的な整理をさせていただけたらなというところが、事業者として考えているところです。

○照井安全審査官　規制庁の照井です。

基本的には、最終的には審査の場でというところでの議論になろうかとは思いますけども、先ほど例で挙げられたメーカの違いということですけれども、直接デジタルという話じゃないのかもしれないですけど、審査の中では、例えばメーカが違っても全く同じような解析の誤りがあったりとか、メーカが違って実施時期も違ってというときにでも、それは全く同じ、今言うそれこそ共通要因のような、同じような間違いをしているということも実際に起こってはいるので、そこはやはりメーカの違いだけでは本当に起きないのかと

いうことは、セットで示していただきたいというふうには考えております。

以上です。

○東京電力HD（遠藤）　東京電力ホールディングスの遠藤です。

ということは、一応メーカが違いますよという説明だけではなく、その中身も含めて御説明させていただいて、そこの説明性が確保できればという認識でよろしいですか。

○川﨑安全管理調査官　規制庁、川﨑です。

基本的にはその認識で構わないと思っています。ただし、先ほどからも照井が言っているように、そこは完全に立証する必要があります。CCFとは何かというのを立証してください。特定してください。けど、そういったものが特定できないということから、今回こういう議論があるわけだし、諸外国でもいろいろ議論して、じゃあどこまでだったらいいのかというのを議論しているわけです。

ただ、それは世界的にも共通のものというのは、まだきちんと固まっているという認識はないです。なので、将来の芽を摘むわけではないです。そこはできれば、今後はそういったこともあるだろうとは思っているんですけれども、現状、我々この検討の中ではそういったものが出てくるということは想定していないです。

○東京電力HD（遠藤）　東京電力ホールディングスの遠藤です。

だから現実的にはないと思っていらっしゃるということですか。

○川﨑安全管理調査官　現実的にはというか、現状において、それが立証できるとは思っていません。ただし、将来的にできるのであれば、それは立証していただきたいということです。

○東京電力HD（遠藤）　東京電力ホールディングスの遠藤です。

承知いたしました。理解いたしました。

○山田統括審議官　規制庁の山田です。

議論の入り口の整理になるかもしれないので、申し上げておいたほうがいいかなと思うんですけども、我々のほうから示している資料1の問1のところで、今回の議論が、過渡と設計基準事故に加えてCommon Cause Failureによりデジタル安全保護系が機能喪失するというのを設定基準ですと申し上げているのではないということは重々御認識いただいていると思うんです。

ということは、これを想定するというのは、設計基準を超える話というのが、まず共通認識になっていると思うんですけども。設計基準として、設計基準事故とCommon Cause

Failureのデジタル安全保護系の機能喪失を想定する必要がないことは、Common Cause Failureの発生確率が非常に小さいということで説明していただけると思うんですけれども、設計基準を超えるものとして、Common Cause Failureを重ねることを考えるべきか、考えるべきでないかというのは、深層防護の3層と4層といっていいのか、3層の中のａ、ｂといっていいのかわかりませんけれども、そこの線引きをどうするかという議論なので、Common Cause Failureが起きにくいですよというだけで、深層防護の壁を要らないという議論をするのは、非常にある種哲学論的なところまで行く、それくらい起きないですよということについての議論を、しっかりしないといけない話だと思いますので、今Common Cause Failureについて、起きませんよということを、るる御説明していただいて、我々も起きにくいということについて、否定をしているつもりは全くないんですけれども、その結果として何を主張しようとしているのかというのは、私が申し上げた二つで全然レベルが違う話になるので、そこはちょっと区別して議論をしたほうがいいかなというふうに思います。

○山中委員　いかがですか。

○西崎企画調整官　規制庁、西崎です。

今のに関連して、私も申し上げたかった点を述べたいと思うんですけれども。これ、設計基準を超えるものというふうに資料1でも書かせていただいていますし、ソフトウエアCCFを設計基準に追加するものでもありませんよということも書いているので、ここは共通理解だと思っています。違っていれば言ってほしいんですけど。

それで、例えば昔の資料なんですが、通しページの77を御覧いただければと思っていまして、これは前回の会合でも配付したものでございますけれども。これは1年半前に技術情報検討会で配付された資料でありまして、その当時公開もしておりますけれども、その2.の評価のところです。

これは国内外を比較したものでございますが、日米で比較した結果の評価として、2段落目ですけれども、CCFの発生防止策については、海外に比べて遜色はないと我々は思っていまして、現状でCCFの発生する可能性というのは十分低く抑えられていると、そういうふうに思っているんですけれども、違いがあるというと、影響緩和策を重視する、そういう要求が海外であるのに、我々は発生防止だけをしていればいいじゃないですかという基準になっているので、ここは手当てをする必要がありますねと。

すなわち発生防止策は十分できているんだけれども、それでもなお発生すると仮定し

ての緩和策というのを検討すべきじゃないかと、そういうことでございまして、同じようなことが、通しの67ページを御覧いただければと思うんですが、これは今年の9月の資料でございますが、1.(1)現状と国内動向というところの中段に改めて書いてあるんですけれども、現行基準の要求するソフトウエアの品質確保策が的確に講じられることにより、CCFが発生する可能性は十分低く抑えられていると考えられるというのが、この検討の出発点なんです。

ですから、今の御説明はCCFの発生確率が非常に低いということを御説明されているんですけども、それ自体は理解しています。その水準がどうかということをあまり議論してもしようがないと思っているんです。その水準が如何であろうとも、リスクは決してゼロにはならないという前提のもとで、なお残存するリスクに対して手当てをしていこうという、そういう信頼性向上対策を今やろうとしているわけですから、そのリスクがどれぐらい小さいかを議論しても、本質ではないんだろうと。

確かに小さいであろうとは思いますけれども、その上での話ということを改めて申し上げておきたいと思います。

○原子力エネルギー協議会（宮田）　原子力エネルギー協議会、宮田です。

どうもありがとうございます。今の議論、非常に大事だと思っていまして、まさに深層防護そのものの議論だと思っています。

我々もデジタル安全保護系ソフトウエアのCCFは非常に起こりにくいという認識、ただしゼロであるということは証明できないということを踏まえて、これが発生したと仮定したときの影響評価について、しっかりと見ていきたいと。

その影響評価に当たっては、当然プラントの通常の状態というか、変に保守的なものを仮定しちゃうと、本当のレスポンスがわからないので、それはいわゆる実力評価とか最適評価とか、そういう言い方されていますけれども、そういうものを今きちんとやっているところです。

じゃあそれに対して、ここはこういうレベルで済んでいるので、特段対策は要らないけれども、ここはもう少し手当てしたいねというものがあれば、当然それを考えますし、その対策の仕方についても、いろんなレベルで考えられるであろうというふうに思っていますので、これは次回にきちんとその考え方も含めて、お示しできればというふうに思っております。

○西崎企画調整官　規制庁、西崎です。

承知しました。

それで、というお話を冒頭も伺って。今安全解析を実施中で、その結果を踏まえて対策の要否、あるいは対策の中身ですね、そういったことを判断した上で、経過措置の議論をしたいということで。確かに、どういった対策が必要かがわからないと経過措置の議論もできない、ということだろうと思うんです。

そこは理解をしているんですけれども、二つありまして。一つ目は、そうはおっしゃるんですが、この資料1、資料2-1ですか、例えば通しの19ページ、ここに書かれていることの趣旨がいまいち理解できないのでありまして、もう一度確認をしたいんですけれども。例えば下線を引いてあるところでいきますと、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、どのような対策を講じることが、ということなんですけども、釈迦に説法で恐縮ですけれども、これ各層ごとに考えていくべき話で、前段に期待したり、後段があることを前提に議論するんじゃなくて、それぞれの層で考えていくということだろうと思うんです。けれどもその、ここに言われている、いろいろ考え方を整理するので次回以降議論したいと言われている中身がよくわからないので、ここの言葉尻を捉えてやるのはよくないのかもしれませんけれども、もう一度、次回以降、何をされようとされているのかというのを御説明いただければと思います。

○原子力エネルギー協議会（宮田）　原子力エネルギー協議会、宮田です。

まず基本的には影響評価をさせていただきたいと思っています。これは全事象についてお見せしたいと。

それにそれぞれの事象の影響がどの程度のものであるかということを見極めた上で、それらに対する対策、有効な対策としてどういうものがあるのかということをお示ししたい。その上で対策にもいろんな対策がありますので、時間がかかるものもあれば、割合時間がかからずにできるものもあるだろうというところをお示しできればなというふうに思っています。

○西崎企画調整官　規制庁、西崎です。

承知しました。

それで次回以降ということなんですけれども、その検討というのはどれぐらい時間がかかると思っておけばよろしいですか。要するに次回以降というのはいつごろなのかということを、事務局としては心配しているんですけれども。今月とかそんな。

○東京電力HD（上村）　東電の上村ですけど、今月末を目途に、短い期間での解析なので、

どこまでお示しできるかはありますけれども、全体像が見えるまではお示しをするというつもりで、今動いております。

○西崎企画調整官　規制庁、西崎です。

承知しました。

ということで、そうしますと今月中にもう一度会合を、という御意見かなというふうには思いますが。ただ、解析結果を示していただくということの目的は、対策の程度を見て、それから経過措置を議論する上での参考資料というか、ベースとなるところだと思ってはいますけれども、具体的な対策が我々の要求事項に、規制化されたときに当てはめとして正しいかどうかとか、それで審査がオーケーかどうかというところを判断するものでもないので、そこら辺は前提として御理解いただければと思います。それはよろしいですか。

○東京電力HD（上村）　東電の上村です。

それも目的の一つですけど、まず今までもデジタルに対しては、ハードワイヤードによるバックアップの設備を設けてきていて、それが今現状で、どこまでカバーできているんでしょうかというところをお見せするのも、一つミッションだというふうに思っていますので、それも踏まえてどういう対策、どういう進め方にしましょうかという議論が進めていければ、いい方向に向くんじゃないかなと思いますので、その準備を進めたいと思います。

○西崎企画調整官　わかりました。

それと、またこの通しの19ページで少しお伺いするんですけれども。小さい丸で書かれているところの二つ目なんですけれども、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があるんじゃないか、ということが書かれているんですけれども。この意味がちょっとよくわからないので、確認をしたいということでありまして。

というのは、さっき申し上げたように、設計基準を考えるときは、CCF対策というのは今要求していることをちゃんとやっていただいているし、かつ、それ以外のところもさっき縷々御説明ありましたけれども、発生防止対策としてはしっかりやられているんで、デジタルであろうともアナログであろうとも、どっちでも基本的には我々の安全要求は満たしていると。そこに差異はないと思っているんです。ですから、別に今アナログのものをすぐデジタルにしてくださいということではないですから、アナログがだめだと言っている気は全然ないんですけれども。ですからデジタル化をしようとする判断が鈍ったから、

何の影響があるのかというのは、ちょっとよくわからないんですけれども、そこら辺、解説いただければと思います。

○原子力エネルギー協議会（谷川）　ATENA、谷川です。

これは、やはり米国でもデジタル化に当たってはいろいろ検討が必要だし、対策設備も必要になってくるということで、デジタル化が少し遅延している部分もあるかに聞いております。

国内でも、まだデジタル化していないプラントもありますし、そこでデジタルを少し躊躇するようなことになってはいけないなというふうに考えておりまして、その辺りも、いろいろ考慮しながらというふうなことも、あわせて考えたいということでございます。

○西崎企画調整官　規制庁、西崎です。

ちょっと言葉尻を捉えるようなんですけれども、躊躇しちゃいけないと言われていることの趣旨なんですけれども。それは、電力会社各社は別として、ATENAさんとしてはやはりアナログはだめでデジタルに進めるべきだと。それがおさまるということですか。

○原子力エネルギー協議会（谷川）　いえ。アナログも信頼性が高いのですけれども、デジタルのほうがさらに信頼性は高いというのが、一番最初に冒頭御説明した内容でございまして、やはり信頼性を高めるにはデジタル化というのは、一つの方向性じゃないだろうかというふうに思っているところでございます。

○西崎企画調整官　わかりました。

○東京電力HD（遠藤）　東京電力ホールディングスの遠藤と申します。

すみません、少し補足させていただきます。

デジタル制御技術というのは、アナログから進歩してきたもので、技術としてはすぐれた部分がたくさんあるんだと考えています。今日ちょっと柏崎のときのアナログのことが記載されていますけれども、軽微な故障というのも自己診断機能があるからこそ見つかる故障であったり、すぐれた部分がたくさんあります。それは数値には現れません。ただ今回のCCFという観点は、我々も30年ぐらい前から議論をしてきて、カバーをしようという取組をしているわけですけども、そこが致命的な欠陥だとは考えていませんで、課題の一つだとは思いますけれども、今回の議論のように、きちんとカバーはしていかないといけないと考えていますけども、デジタル制御技術はすぐれたところで、今後の原子力業界の計測制御技術の中でも軸になっていく技術だと。

これが致命的な欠陥だという話になって、アナログからデジタルに変えるとか、デジ

タルを採用することをやめることはないんですけど、ちょっと躊躇してしまうようなことにはしたくないと考えていまして、そういうところでもきちんと今回議論させていただいて、この先デジタルがなくなっていけば、それで信頼性なり安全性なり、このCCFという形ではよくなったとしても、全体としては必ず信頼性向上という観点でもよくないかなと、業界としては進歩が下がっていってしまうというところがありますので、そういう意味も踏まえて、まずはデジタル制御技術は今後も事業者としては使っていくんだと、そういうところも踏まえた建設的な議論をさせていただきたいというところも踏まえて、こんな書き方もさせていただいたところです。

以上です。

○川﨑安全管理調査官　規制庁、川﨑です。

先ほど宮田さんからお伺いした話で、ちょっと確認だけさせていただきます。13ページ開いていただきまして、簡略評価の結果のほう書いてあって、制御棒系の事象については実際の手順の話ですとか、その事象が起きる、起きないという、そういう入り口をオミットしているんですけど、先ほど言われたように、ちゃんとその影響評価としては今後示していただくということでよろしいですよね。

○東京電力HD（上村）　東京電力ホールディングスの上村です。

正直なところ悩んでいます。悩んでいて、ここで評価をしなければいけない対象は、デジタルのCCFが起きたときに、どんなものをバックアップとして用意すればいいんだろうかという目安を見るためのものが目的の一つとしてあります。

制御棒系の過渡は、これは、過渡解析上は臨界近傍になったときに連続引き抜きでということをやっています。RIAの事故と書いてある側、これはCRが分離して落下しますということをやっています。過渡側でいくと、もう連続引き抜きをするということをマネジメントで防止をされているわけなんです。なので、デジタルでのCCFのバックアップとしての役割が手順上の中で織り込まれているということを踏まえると、この事象に対してハードウエアの有無とか影響の有無を考える対象にすべきかどうかというのは、すごく悩んでいます。

事故のRIAも同じくです。CRには落下したらラッチがかかって、ABWRですと210mmでとまりますので、これ反応度が入らないんです。こうしたハードの防護というものがあるので、そのデジタルとしてのCCFに対する対応可否を議論する土台に乗せるべきものじゃないのかなというところで悩んでおりまして、今このような記載にさせていただいております。

そこは御議論なのかなとは思っていますけれども。

○川﨑安全管理調査官　規制庁、川﨑です。

あまりそこは議論の余地はないのかなと思っていて、というのは、これそもそも大LOCAを除外できるんじゃないかという議論とつながると思うんですけれども、そもそもの安全保護系というのが、こういった事象にも対処できる能力を持っているわけです。その代替設備の能力を見る以上、有効性を見る以上は、当然こうした事象も含めて見るべきだというふうに考えています。

○東京電力HD（上村）　東電の上村です。

14ページに先ほど冒頭の各層でというお話がありましたけど、確かに制御棒カットとか制御棒落下というのはいわゆる状態1、2の間を防ぐための手段で、今議論しているのは2と3を防ぐための手段という意味じゃ、確かに質は違うと思いますけど、じゃあ実際に対策を施すかどうか、その判断のときにそこをどう考えるかというのは、少し議論が要るんだろうなとは思っています。

○川﨑安全管理調査官　規制庁、川﨑です。

そこまで実際にやる、やりませんという話というのは、個別具体の審査になりますので、この検討会合の1回目のときにも個別具体の適用例について、そこは載せるのはやめましょう、議論するのはここの場ではないですという話、していたとおりなので、それは今後この規制化されたとか、そうした後に議論をしていけばいいかなとは思っています。

○東京電力HD（上村）　東電の上村です。

ありがとうございます。

趣旨、重々理解しましたし、今回でより深まりました。安全として恐れているのは、欲を張ってハードウエアのバックアップを増やすが余り、増やすとこれは誤起動のリスクを上げることになる。せっかく信頼を高めたデジタルというものの信頼性を逆に下げることというのはすごく恐れています。だからこそ前回の資料においては、現実的な評価でというふうにおっしゃっていただいていると思いますので、その趣旨をきちんと理解をした上で、次回お示しをしたいと思います。

○川﨑安全管理調査官　規制庁、川﨑です。

了解しました。

○山中委員　そのほかいかがですか。

○小木曽技術参与　技術基盤課の小木曽と申します。

今日御提示いただいた資料の中で、信頼度のデータが二つ出ております。一つがEPRIのデータ、それからもう一つが日本のデータと。それで、EPRIのデータのほうは1%の故障という話なんですが、これEPRIのレポートを見ると、実際は一つのイベントが発生していると。

それで、米国のようにかなりデジタル制御に対して、NRCがいろんな指針、あるいは業界基準、かなり整備されている中で、一つにしろCommon Cause Failureが起きたという、そういう報告があったというのはものものすごい重大なことじゃないかなと認識しております。

ですから、やはりこういうような米国のこういう事例はきちんと分析して、Common Cause Failureはなぜ起きたのか、それをよくお示しいただかなきゃいけないんじゃないかと思います。

それで、EPRIのデータはイベント数に対するパーセンテージで、それで今回最終的にdemandに対する10^{-7}という数値になっているんですが、そのプロセスもちょっとよくわからないということ。それから日本側のデータは約10億時間、これに対して事象が全く起きていませんということで、回数をつくらなきゃデータにならないから0.5回という、そういう想定をされているんですが、0.5回という、そういう想定というのは非常に違和感を感じるんです。もしやるとすれば1回じゃないかと。

それで、今日の規制庁のほうから出した最初の資料のところで、柏崎の現場でそこの担当の方とディスカッションしたときに、デジタルシステムというのは、技術革新はすごく進んでいるんで、10年に1回ぐらいは交換していますと、そういうことをおっしゃったというふうに記録に残っているんですが、仮に10年に1度ずつ変えていくとすると、10億時間ですか、そこの間でも、やはり10年に1度のリプレイスを前提にしたデータじゃないかと。

ということは逆に言いますと、古典的な故障率データでメンテナンスをすれば、またその時点で故障率がゼロとは言わないですが、かなり回復すると。それでまた落ちていくと。ただしその古典的なそういう故障率の考え方は、多分ソフトウエアには適用はできないと思うんですが、これ10年に1度交換する、そういう対象システムに対して、今後どういうデータ整理をされていくかと、そういうところを少しクリアにさせていただきたいと思います。

○東芝エネルギーシステムズ（福本）　東芝エネルギーシステムズの福本と申します。

まず10年に1回更新していくということなんで、私現場にいなかったので、どういうことを想定されて、現場の方がおっしゃったかわかりませんけども、私の理解は総じて安全保護回路だけではなくて、ほかの常用系のデジタルも全部含めると、平均してそのくらいの更新頻度になっているというふうに理解しました。

その上で、どのくらいの年度、実績があるかという考え方ですけども、当然更新するときには全く新しいものは入れませんで、ちょっとこういう言葉を使わせていただきますけれども、実績のあるファミリーのものの部品の供給性とか、そういうものを踏まえまして新しくしないと、もう部品がついてこないとか、そういうものがあるんで、改定ということでやらせていただいていますけど、そういう意味では全く新しいものを入れないということなので、そういう意味で同じファミリーのソフトウエア的にはほとんど同じようなものを使っていますから、そういう観点で実績10億時間というようなものは、そういうふうな同じファミリーのものをずっと通じて累積した結果、このぐらいの実績になっているということでございます。

ですからある意味では、特定のところだけで見るよりは、もう少し更新も入れた評価になっていますので、更新を入れた同じファミリーの中で累積しても、ソフトウエアに起因するCCFはなかったというふうに整理をしてございます。それでお答えになっていますでしょうか。

○小木曽技術参与　ありがとうございます。日本のデータに関しましては了解です。

EPRIのデータについてはどうでしょうか。

○東芝エネルギーシステムズ（福本）　東芝エネルギーシステムズの福本でございます。

EPRIのデータは我々も見てございまして、INPOに登録してあるデータをベースにしていますので、もともとの類似なところまではまだ行き着いていませんけども、今CCFがあったという御指摘なんですけど、我々の理解はCCFには至らなかった。CCFにポテンシャルがあるものがサーベイランステストで見つかったというふうに理解をしております。そういう意味ではCCFに至ったということではないということは申し上げておきたい。それがサーベイランステストで見つかったという事実も申し上げておきたいと思います。

見つかった内容は、我々の理解はテストモードをしているときに、起動信号が入ったときに、もともとの上流側の設計と、それからテストの不備の組み合わせで、サーベイランステストでやるまでは見つからなかったというふうな事象と理解しておりますので、御指摘のようにEPRIのところを我々は見ているかという御指摘に関しては、まず見ています

ということと、それの解釈については今述べたとおりでございます。

以上です。よろしいでございましょうか。

○小木曽技術参与　ありがとうございました。

○山中委員　そのほか、相互に確認しておきたいこと、ございますか。どうぞ。

○原子力エネルギー協議会（谷川）　ATENA、谷川です。

本日の資料1の2ページ目の問1の真ん中、一番最後のパラグラフです。「最適評価により現行基準第13条第2号の要件を概ね満足することを例示している。」ということですけども、この「例示」というのは前回の第1回会合の資料の補足で、それが例示されているという趣旨でよろしいでしょうか。

○西崎企画調整官　規制庁、西崎です。

ごめんなさい、場所の話ですか、資料の中でどこで、という。

○原子力エネルギー協議会（谷川）　そうです。どこでという。

○西崎企画調整官　そうですね。通しの65ページでございますが、炉心損傷防止できるとは、という、そうですね、補足で書いてあると、そういうことです。

○原子力エネルギー協議会（谷川）　わかりました。

○西崎企画調整官　それでよろしいですか。

○原子力エネルギー協議会（谷川）　ありがとうございます。

○西崎企画調整官　規制庁、西崎ですけれども、引き続き。ということで、ここまでの私の質問したやつの再確認なんですけれども、次回評価結果とともに対策の要否であるとか、対策の中身の概要をお示しされて、それで、したがって経過措置がこんなふうに必要なんですと、そういった議論につなげていくということで理解しているんですけど、それは本来は今回、経過措置も含めて御意見、ということだったんですけれども、経過措置についても次回にできるという理解ですか。

○原子力エネルギー協議会（谷川）　ATENA、谷川ですけども、次回はやはり、解析にまだ少し時間がかかるということもありますので、解析とそれをベースにした対策設備の概要というところにとどまるかなと思っておりまして、それを踏まえた経過措置に対する考えというのは、次回はちょっと難しいかなと思っておりまして、できれば次々回というような形にしていただければありがたいかなと思っております。

○西崎企画調整官　規制庁、西崎です。

わかりました。一応そういった御意向をお持ちだということですね。

それは、いずれにしても次回、どういったものが出てくるかによって、その後の議論は変わってくるかと思いますので、まずはじゃあ次回ということで。それを今月中にやるということで、調整を今後させていただければと思います。それで、前回は会合間の間にさらに確認したいことがあるんで、面談で確認させてくれという御要望があったと思うんですけれども、今回いかがですかね。我々としては相当程度、御理解のための質問には回答したと思っているんですけど、まだ必要でしょうか。

○原子力エネルギー協議会（谷川）　先ほどの制御棒の話とかも、解析をいろいろやっていく中で、あるいは対策設備を検討していく中で、やはり面談で確認したいということが多分出てくると思いますので、ぜひこれまでどおり必要が生じたら面談で確認させていただくということは考えていただければというふうに思っております。

○西崎企画調整官　了解しました。

○山中委員　そのほかいかがでしょう。どうぞ。

○山田統括審議官　規制庁の山田です。

細かいところで教えていただきたいと思っての御質問なんですけど、12ページの四角囲いで、アメリカのデジタル規制経緯というのが書かれているところの、一番下の多様化設備に係る措置の扱いのところで、例としてLBBを前提として大LOCAは除外するというふうなことが書かれているんですけれども、ここでの議論というのはどういうのが論点なのかが、もしわかればということなんですけれども。多様化設備が対象としている設備の状況というか、事故・過渡の対象から、このLBBを前提とした大破断LOCAを除こうとしているのか、それともCommon Cause Failureが起きるのと大LOCAが重なる確率を考慮して、これは除外しましょうという議論なのか、どちらなのかということで、伺っています趣旨は、昔から大LOCAを設計基準から除こうという議論は、アメリカでずっとやっていて、結局ACRSでぽしゃってしまったので、今これを再チャレンジしようとしているのか、それとも全く別の議論をしようとしているのかというのが、わかれば教えていただければと思って。

○三菱重工（内海）　三菱重工の内海でございます。

今のお話なんですけれども、確かに昔から大LOCAというのは、やはり扱いづらい事象であるという議論は産業界等、例えばNRCとかの間でもあったのは事実なんですが、ごく初期のころに認可された標準設計プラントの中に、たまたま当時のNRCとメーカのやりとりでLBBが十分検知できるので、大LOCAに至る前にプラントを止める運転要領にしておけば、そっちにはいかないからというようなことで、認可された例が実は1個あったんです。

ただその後、NRCとしては基本的には全ての事象について評価しろというポジションで規制を行っておりますので、そういう意味では今のNRCのポジションというのは、非常にはっきりしている。だから確率で落とすとか、そもそも評価対象外の事象にするということは、NRCは基本的には考えていないです。

ただ既に認可した事例がありますので、それはそういう産業界としてもそこに何かブレークスルーは見たかったということで、NRCと議論をした結果だと思いますが、最新のドラフトの審査要領、スタンダード・レビュープランの中のプランジング的な役割、ポジションの中では、そういうNRCが既に認めている運転員の運転操作によって、その事象の発生そのものを防止できるような手段があった場合には、それも全体としてもD3解析と言われているCCFとの重ね合わせの評価の中で、ケース・バイ・ケースで議論することは可能であるというふうな記載があります。

ということで、それはどこにもLBBという言葉は一言も書いていないんですが、基本にあるのはそういうことの今までの経緯を踏まえて、そういう一文をNRCの方に書いていただいたということだと思います。

○山田統括審議官　規制庁の山田です。

ありがとうございました。要するにプラクティカリー・エリミネートできるかどうかという議論が成立すれば除外できますよというのが、NRCのポジションになっているということですね。

わかりました。ありがとうございました。

○山中委員　そのほか確認したい点、ことはございますか。よろしいですか。

今日大分議論がかみ合ったかなと思うんですが、次回までに極めてリスクは小さいんだけど、リスクを考えてその影響を評価しますと。防止策まで提示をしていただくという、そこまで次回までにお願いできるということでよろしいでしょうか。

○原子力エネルギー協議会（富岡）　ATENA、富岡ですけど、そのように進めていただければというふうに思います。

先ほども山田審議官からございましたが、非常に確率は低いんだけれども、深層防護の観点から、あえてそれを仮定して、安全解析でその影響を評価してみるという趣旨であります。

その設計基準事象を超えたところの部分ですので、その安全解析の評価ですとか、判断ですとか、そういったことをどういうふうに置くのかというようなことを含めて、それ

に対して、じゃあどういう安全対策があり得るのかというようなところを、次回お示ししたいというふうに考えています。

先ほどもありました、その仮定でいろいろと、今回資料1でお出しいただいた、大変我々の理解が進むということもあります。このような点について疑問な点などがあれば、引き続き面談のほうで確認させていただきたいということでございます。

○山中委員　あとよろしいでしょうか。よろしいですか。

それでは本会合で予定していた議題は以上でございます。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3回会合、これで閉会させていただきます。