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１回会合議事録

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１回会合

１．日時

令和元年１０月３０日（水）１５：００～１６：５０

２．場所

原子力規制委員会　１３階Ｄ・Ｅ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
平野　雅司	総務課国際室　地域連携推進官
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
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
丸山　直紀	安全規制管理官(核セキュリティ担当)
奥　博貴	核セキュリティ部門　管理官補佐
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（ATENA）

富岡　義博　　理事

示野　哲男　　事務局長

谷川　尚司　　部長

福光　裕之　　部長

佐々木　茂夫　　副部長

株式会社日立製作所

原　勲　　原子力制御システム設計部　主任技師

東芝エネルギーシステムズ株式会社

加藤　守　　原子力電気システム設計部　電気システム第三担当　参事

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

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

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

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ェアに起因する共通要因故障対策について

５．資料

資料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ェ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～（原子力規制庁）

資料２　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（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ェ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資料１－１）

参考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

検討チームの設置について（令和元年度第３３回原子力規制委員会資料６）

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1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ェ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、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ェアに起因する共通要因故障対策について具体的な要求事項の案を説明し、その後、原子力エネルギー協議会（ATENA）から、産業界の現状や今後、見解等について聴取いたします。

それでは、まず、技術基盤課の遠山課長から、資料について説明を始めてください。

○遠山課長　技術基盤課の遠山です。

まず最初に、資料の確認に入りますが、本日はお手元のiPadに資料を入れております。

その1ページ目が表示されていると思いますけれども、今日、使います資料は、まず資料1として、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ェ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～という規制庁のものでございます。続きまして、資料2、これは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として、原子力エネルギー協議会の資料です。そのほかに、過去2回の規制委員会の資料を参考として二つつけております。

資料については、右下に青い数字で通しページをつけておりますので、適宜、この数字で参照することといたします。

それでは早速、最初の資料1について御説明をいたします。

ページの右下3ページですが、本件の背景と経緯は、先ほど山中委員からも御紹介ありましたけれども、これは本年の原子力規制委員会の重要課題として挙げられている課題であります。そして、第29回原子力規制委員会において、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取組方針を了承されまして、最近の国際的な動向も踏まえ、信頼性向上の観点から、現行規制の見直しを検討することとしています。また、引き続き、第33回原子力規制委員会におきまして、本日、皆様お集まりいただいているこの検討チームの設置が了承されまして、今日、第1回の会合を開くことになったとい

うことであります。

続きまして、右下の4ページ、検討の方向性ですけれども、この検討チームでは、2点の方針で規制要求の具体化、整理などを進めていきたいと考えています。まず①番目は、デジタル制御方式の安全保護回路を設ける場合には、ソフトウェアに起因する共通要因故障対策として、デジタル安全保護回路とは動作原理の異なる別の手段、ここでは多様化設備と呼びますけれども、これを設けるように新たに要求することとし、許可段階からその基本設計方針を確認するというものです。

二つ目は、多様化設備は、運転時の異常な過渡変化又は設計基準事故の発生時に、そのソフトウェアの起因する共通要因故障によって、デジタル安全保護回路が機能を喪失すると仮定しても、原子炉施設の安全性が損なわれないということを要求するものです。

具体的な要求の内容につきまして、担当のほうから御説明をいたします。

○西崎企画調整官　原子炉規制庁の西崎です。

それでは、お手元の通しページ、5ページ以降から御説明いたします。

いわゆる多様化設備の具体的要求事項をこれから御説明したいのですが、その前に、この資料の構成上、デジタル安全保護回路の定義について御説明いたします。

5ページの参考にございますように、現行規則では、安全保護回路について定義がございますけれども、デジタル安全保護回路についての定義がないので、この度、新たに定義を置いてはどうかと考えています。デジタル安全保護回路とは、安全保護回路のうち、ソフトウェアを用いることによってその安全保護機能の全部又は一部を作動させるものという定義にしてはどうかと考えています。

この「安全保護機能」という言葉ですけれども、下の矢印のところに書いてございますが、安全保護機能というものは、今の規則でも書いておりますけれども、子細に見ていきますと具体的な定義がないまま使われておりますので、先ほど御説明した安全保護回路の定義を引く形で、鍵括弧に書いてあるような定義規定を置いてはどうかと考えています。具体的には、過渡・事故の発生を検知し、停止系及び工安設を自動的に作動させる機能ということでございます。

次のページを御覧いただければと思います。ここから多様化設備についての話に移りますけれども、今、検討の方針で御説明があったように、今御説明したようなデジタル安全保護回路を設ける場合には、代替作動機能を有する装置、いわゆる多様化設備を設けなければならないということを考えています。

補足で書いてございますけれども、デジタル安全保護回路の一部がソフトウェアによって作動するものであっても、多様化設備を用いなくても判断基準を満足することが最適評価により確認できる場合には、この限りではないというふうに考えています。この判断基準でありますとか最適評価につきましては、後ほど御説明します。

7ページを御覧ください。多様化設備の具体的要求事項のその①として、まず想定する事象でございますけれども、繰り返し出ていますように、運転時の異常な過渡変化又は設計基準事故が発生したとき、これはすなわち安全保護回路の自動作動が要求されたときに該当しますけれども、そのときに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が喪失するというものを仮定するということでございます。

補足で書いておりますのは、より具体的にどういうことかというのを書いているんですけれども、過渡又は事故が発生した場合において、デジタル安全保護回路がその異常を検知することができないとき又は停止系及び工安設を自動的に作動させることができないとき、こういうことを仮定することになります。

次に8ページを御覧ください。多様化設備が持っている基本的な機能として、代替作動機能というのがございます。これを定義しないといけないんですけれども、ソフトウェア起因の共通要因故障によりまして、多重化されたデジタル安全保護回路が同時に安全保護機能を喪失した場合において、一つは、まず、安全保護回路とは異なる動作原理の機構によって、B)としては原子炉停止系統及び工学的安全施設を、C)としては、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と、こういった機能というふうに定義をしてはどうかと思っています。

補足に書いておりますけれども、異なる動作原理の機構といいますのは、代表的に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といったようなもので、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をいうということでございます。

9ページを御覧ください。次は信頼性の要求でございます。これも何度も出ておりますけれども、当然、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、今御説明した代替作動機能が損なわれるおそれがないように適切な措置を講じていただく必要があります。適切な措置を講じたものといいますのは、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に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などを指します。例えばということで、一番下に書い

てございますけれども、一例としては、ある想定される火災区域での火災で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に設計することというふうになります。

10ページを御覧ください。これは信頼要求の続きですけれども、これは当然ではございますが、外部電源が利用できない場合においてもその代替機能が損なわれるおそれがないものであることということで、いわゆる非発要求でございますけれども。それから、他のDB設備に要求される地盤、地震、津波、外部事象、こういったものの規定についても同様に適用又は準用していくということでございます。

補足で書いてございますのは、現行許可基準規則で言えば12条、こちらを適用するわけですけれども、そのうちの第2項、これは多重性でありますとか独立性の要求を規定しているものでございますが、これまで御説明したように、同種の要求内容を別に規定することとなるために、2項については適用しないというふうにしたいと思います。

11ページを御覧ください。多様化設備の成立性の確認についてでございますが、まず一つには、評価方法でございます。過渡又は事故が発生し、かつ、安全保護回路の完全保護機能が喪失すると、そういう仮定を置いた場合でも、要求された多様化設備が有効に機能することによって炉心損傷を防止できるということを最適評価により確認することとしてはどうかと考えています。

ここで最適評価ということなんですけれども、いわゆる添十解析の安全評価とは異なりまして、最適評価によって炉心損傷を防止できることを確認するわけですけれども、この際に、そこのa～dに書いていることを考慮してもよいというふうにしております。aとしては、安全保護回路自体は機能喪失しますけれども、その補機に当たる停止系統や工安設は利用することができると。それから、多様化設備そのものの単一故障は仮定をしない。それから、cとしては、運転員による現場操作を想定してもよいということ。それから、dとしては、これは安全保護回路の自動検知ができませんから、運転員の事態認知から手動操作までの時間、こういったものについて、評価に用いるモデルやパラメータについては現実的なものでよいということで、いわゆる10分ルールは適用しないというものでございます。こういった形で、より現実的な最適評価を行っていただくということでございます。

12ページを御覧ください。判断基準でございますが、これも先ほど御説明したように、そういった仮定を置いた場合でも、炉心損傷が防止できることということですけれども、その判断基準としては、いわゆるDBの判断基準でございますけれども、許可基準規則でい

えば、13条2号の要件を満足するということとしてはどうかと考えています。

それで、最後、13ページを御覧いただければと思いますが、今回は、今御説明した我々の検討中の案について、事業者から御質問、我々の今御説明した内容についての質問を受けたいと思いますが、その上で、御意見がある場合には、これは経過措置に関するものを含みますけれども、次回の検討チームで聴取をして、科学的・技術的に議論をしていきたいと思います。

ついては、議論を有意義に行うために、御意見をいただくときには、理由を付していただくと同時に、科学的・技術的な根拠ですね、妥当性を確認・検証することができる文献・データ、その他必要な書類をつけていただきますと、より議論がしやすいかなというふうに思っております。

それから、書いてございませんけれども、個別のプラントの審査において確認するようなことにつきましては、この場では取り扱わないことがございますので、その点は御了解いただければと思います。

私の説明は以上です。

○山中委員　それでは、質問、コメントを受けたいと思いますが、いかがでしょうか。

○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。

まず、8ページの代替作動機能に関する「異なる動作原理」というところなんですけれども、異なる動作原理の、ソフトウェアに起因するこれは共通要因故障ということなので、基本的には設計ミスとか、そういったところがポイントかと思うんですけれども、ソフトウェアとしては、違うソフトウェアを使っていれば、それは共通要因故障には至らないという認識でよろしいんでしょうか。

○照井安全審査官　規制庁の照井です。

今の違うソフトウェアであればということですけれども、ソフトウェアに起因するCCF（共通要因故障）要因、例えば設計ミスに関するものだったら、それを排除する対策をとられていれば、その要因に関するCCFというのは起きないかもしれませんけれども、じゃあ、本当にほかの要因、ソフトウェアCCFが何が起因で起きるかというのは、今、全ての要因で明らかになっているわけではないという状況下において、違うソフトウェアであればCCFは必ず起きないんですという証明ができるのであれば、それは多様性を持つもの、異なる動作原理というものということで、満たせるというふうには思いますけれども、そこについては、本当に異なるソフトウェアであれば、必ずCCFが起きないのかというとこ

ろの証明とセットになるのではないかというふうに考えています。

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。

承知いたしました。ただ、違うものであるということは、違うものであるということになりますので、何が結局、共通要因故障のきっかけになるかということが議論になるかと思うんですけども、そこは少し整理をさせていただく必要があるかなというふうに考えております。

以上です。

○山中委員　そのほか、いかがですか。

○原子力エネルギー協議会（谷川）　ATENAの谷川でございます。

まずは7ページのところで、想定事象のは書いてありまして、共通要因故障により安全保護機能が喪失するものと仮定するということで、確認ですけども、補足のところには、原子炉停止系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仮定するということがあるので、自動スクラムとECCS（非常用炉心冷却設備）の自動起動が両方とも失敗するケースを考えろというふうにとってよろしいでしょうか。

○照井安全審査官　規制庁の照井です。

基本的には御認識のとおりで、一応、書いてあるのは、安全保護機能というのは検知することができないときも含まれるんですね。そこは「又は」になりますし、例えば想定する過渡・事故の様態によっては、どちらかということもあり得るとは思いますけども、基本的にはスクラムが入って、その後、ECCSが起動してということになりますので、そのどちらもが動かないという状態にはなると思います。

○原子力エネルギー協議会（谷川）　次の質問が、8ページの代替作動機能のところで、C)の自動的に、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ということで、ここで言う原子炉制御室というのは、中央制御室のことを指していると。中央制御室から手動で作動させることが要件になるというふうな理解でよろしいんでしょうか。それとも、別のところを見ますと、現場というような記載もあったかのように思いますけども、その辺りはいかがでしょうか。

○照井安全審査官　規制庁の照井です。

基本的には、今、ここで書いているのは、原子炉制御室ということになりますけれども、今、評価上は最適評価でいいと言っているところもありまして、例えば事象が速いような

ものだと、判断基準との関係で間に合うかどうかという議論になるかとは思いますけれども、現場操作をして、間に合うということが立証できるのであれば、それは否定されるものではないというふうに理解をしています。

○原子力エネルギー協議会（谷川）　わかりました。ありがとうございます。

ATENA、谷川です。

たしか、11ページですね、添十解析とは異なり、最適評価により炉心損傷を防止できることを確認することということで、これは炉心損傷を防止するのはまさに事故の基準、確認ですけども、事故の基準を満足するようにという趣旨でよろしいでしょうか。

○照井安全審査官　規制庁の照井です。

判断基準のところは、通しページの12ページにも書いてありますけれども、ここで言う炉心損傷を防止できるものとするというところは、今の事故の基準ですね。基準規則でいうところの13条の2号の要件というものを満たすようにしてくださいと言っているものであって、少し蛇足的に補足をしますと、今、いわゆる安全評価でやっている添十の結果がありますね、その結果の範囲内におさめてくださいと言っているわけではなくて、あくまでも第13条第2号の要件の範囲内に満たしてくださいということを書いている趣旨でございます。

以上です。

○原子力エネルギー協議会（谷川）　ATENA、谷川です。

設計基準事故というのは、発生頻度が極めて低いと思っていて、なおかつ、後で御説明しますけども、このソフトCCF自身も非常に発生頻度が低いと思っていまして、それが同時に起こるということを仮定した状態で、なおかつ事故の基準を満足しろというのは、少し厳し過ぎるかなという気はするんですけども、その辺りの、こういう、その背景といいますか、考えについて御説明いただければと思うんですけども。

○照井安全審査官　規制庁の照井です。

今回、そもそも要求をしている趣旨は、既存のDB設計が悪いとか、そういう意味ではなくて、こういうソフトウェアCCFというものを仮定したときに、より信頼性を高めるために要求をしようということで、今やっているものでございます。

その上で、今、じゃあ、CCFを仮定する安全保護系というものは、DBA（設計基準事故）に対して機能を要求されているものですから、それについては、そのバックアップということであれば、同じくDBAに対して対処できるものである必要があるだろうということで

考えております。

今の頻度論の話ではあるんですけども、今、我々が考えているのは、先ほども申し上げたように、DBAが起きたときに、CCFが起きるということを仮定して、信頼性をより高めてくださいと言っているので、そこについて、頻度論というものでの議論、少し誤解を生むかもしれないんですけど、ある種、深層防護的に考えているところがあるので、そこについては頻度論ではなくて、DBAの全事象ということを今考えております。

以上です。

○原子力エネルギー協議会（谷川）　ATENA、谷川ですけれども。

諸外国を見ても、例えばLOCA（冷却材喪失事故）とCCFが発生しても事故の基準を満足しろというところはあまり見当たらないのかなというふうに思っておりまして、そこまでする必要が本当にあるのかな。というのは、運転中、例えば定検時においても、LOCA信号を入力したりして、作動状況の健全性は確認したりしているわけでありまして、そこで見逃されたのが、たまたまLOCAが起こったときに安全保護系が動作しなくなるというのは、非常に考えづらいといいますか、発生頻度が低い。だけども、ソフトCCFが起きないとは言えないので、自主的な設備として今まで設けてきたというのが経緯でありまして、それをいきなりDBAという基準を満足するようにということになりますと、やはりどうしても確率論というか、起こり得る事象、起こり得るといいますか、そこまでのことを要求するのかなというのは、どうしても産業界としては思ってしまうんですけども、いかがでしょうか。

○川﨑安全管理調査官　規制庁、川﨑です。

まず、ちょっと、自主的にそういった考えで備えつけているとおっしゃっていますけれども、今、そういうDBAの中でも頻度が低いと思われるような、大LOCAはそもそも今はつけていないんですよね、大LOCAに対しての代替設備というものはないですよね。

それと、あと、今、我々も、こういった安全性の向上といったことで、なので成立性については最適評価でもいいのではないかという提案をさせていただいているということです。

○三菱重工（内海）　三菱重工の内海でございます。

今のまさに議論なんですけれども、深層防護の強化ということで、こういった策をとるということなんですけれども、やはりそこで気になるのは、今のDBAの範疇というのは、やはり単一の機能喪失ということを前提にして、安全機能が確保できるかということを見

ているわけですけども、CCFというのは、これもちょっと正確な言葉を選ぶというのはちょっと難しいんですけども、諸外国の例を考えても、いわゆる設計の想定を超えた、要するにDesign Extension Conditionのような形で深層防護の中で見ているという例が非常によく見受けられます。その辺の考え方を取り入れられなかった理由というをもう一度お願いしたいんですけども。

○川﨑安全管理調査官　規制庁、川﨑です。

4ページ、戻っていただいて、我々もそこを、デジタルCCF、デジタルの話については安全評価上想定する単一故障として考えているわけではないです。今回のこの話というのは、確かにデザインベースと、それを超えるところに相当するという、そういった認識ではあるんですね。なのでそこには、もう一回さっきと同じ回答にはなってしまうんですけれども、その評価に当たっては、確認に当たっては、最適評価でもよいというふうに考えています。

○照井安全審査官　規制庁の照井です。

少し補足をさせていただきます。

繰り返しになってしまうかもしれないんですけれども、今、川﨑が申し上げたように、そもそも、いわゆる添十とかで言っている安全評価の単一故障として、このデジタルCCFというものを捉えているものではありません、我々も。それは、だから、そういう意味でいうと、今、既存のデザインベースの設計を超えている世界になっているんだろうなということも理解をしていますし、その上で、さらにより厳しい状況でいうと、今、重大事故等対策ということで新たに要求をかけていて、例えば今回の安全保護系の例でいうと、例えばLOCAでもそうですけど、LOCAでさらに補機まで、ECCS系まで使えなくて、注水ができないという状況下においても、大LOCAはCV（原子炉格納容器）側に行きますけど、中小であればLOCA時注水機能喪失ということで、炉心損傷防止ができることということはきっちり対策はできているということは確認をさせていただいているのですね。今、直ちに何か問題があるという立場に立っているわけではないというのは、まず御理解をいただきたいなというふうに思いますけれども。

その上で、今回のデジタルCCFが重畳した場合というのは、基本的には、今、SA（シビアアクシデント）で考えているような、補機まで死んでいるといって、新たに可搬で準備をしなきゃいけないとかというところの状態までを想定しているわけではなくて、今使える、補機としては使えるものを使って炉心損傷を防止してくださいと。その評価の基準と

しては、DBAの基準を使っていますけれども、評価のやり方については、ある種、最確評価でよくて、いわゆる安全評価でやっているような10分間を手動操作に期待しないとか、そういったところではなくて、そこはある種合理的に、事態認知から、このぐらいの期間で操作ができますというのであれば、それで説明をしていただければいいなというふうには思っていますけれども、そういう意味で、DBAの基準は、判断基準として、例えば1,200℃以下にしてくださいよとかという判断基準として、そういう数値として使っていますけれども、事象の捉え方としては、DBAとして捉えているというわけではないということです。

○三菱重工（内海）　三菱重工、内海です。

例えば今、重大事故の中に、例えばATWS（原子炉停止機能喪失事象）というものを今評価の対象にしていますけれども、そのほかのシナリオを見ても、何かきっかけとなる、起因事象に対して何か対処系が、CCFという言葉は必ず使っていないかもしれませんが、多重性を持たせて用意した安全機能が機能しなかったというような形で整理がなされていると思うんですね。そういうことを考えますと、今回お示しいただいたような方向性というのは、どちらかというと、やっぱり重大事故を扱う範疇の中なのかなというふうに考えます。

その一つの理由は、例えばATWS対策設備、これは、実際にじゃあ何を実現しているかというと、実は安全保護系がもし動かなかったことによってATWSが起こるという部分については、まさにソフトウェアCCFと同じような想定をしている。ソフトウェアCCFによって安全保護系が作動しないというものがもし考えられるとすれば、それは今、重大事故として考えているATWS事象になると。その妥当性は、重大事故としての評価の中で見ているということになるんですが、例えばこの代替の設備は、重大事故等対処設備になるんでしょうか。

○川﨑安全管理調査官　規制庁、川﨑です。

今、例えば審査の中で見ているもの、これが重大事故対処設備が一方で代替、DAS―多様化設備という位置づけも出てくるというのは、それは十分あると思っています。これを、質問のちょっと意図がわからなかったんですけれども、単純にDASと言わせてもらいますけれども、DASがSA設備として位置づけさせられるのかという御質問ですか。

○三菱重工（内海）　はい。

○川﨑安全管理調査官　それは否です。ただ、そういうふうに、そういう想定をしている

ものではないです。ただし、ただし、バックアップ設備として今準備している、今設計を行っているSA設備を使うということについては、我々は否定しているわけではないです。

すみません、規制庁、川﨑です。

例えばBWRでいうと、ARI（代替制御棒挿入回路）、これを多様化設備として、その成立性を示していただくということに対しては、我々はそういったことも想定はしています。

○東京電力HD（遠藤）　東京電力ホールディングスの遠藤です。

今お答えいただいたのであれですけども、要は今SA設備で使っているARIみたいなものは、この代替作動機能として期待してよくて、その説明として、設計基準兼SAみたいな形になるのかもしれませんけど、そういうふうに扱ってもよろしいという理解でよろしいですか。

○川﨑安全管理調査官　はい、まさにそのとおりです。

○原子力エネルギー協議会（谷川）　ATENA、谷川です。

11ページの評価方法に関する御質問ですけれども、最適評価と書いておりますけれども、普通、添十解析ですと、単一故障をさらに仮定するというところがあります。DGが起動しないとかというところがありますけども、それは最適評価という意味合いからすれば、そういう仮定はしなくていいということでよろしいでしょうか。

○川﨑安全管理調査官　規制庁、川﨑です。

まさに、その認識のとおりです。

○原子力エネルギー協議会（谷川）　ATENA、谷川です。

最適評価をするに当たって、例えば炉心のP.C.D.評価を行うときの仮定も、少し現実的なベースで見直してもよいという、そこまで踏み込んでもよろしいですかということですか。

○川﨑安全管理調査官　規制庁、川﨑です。

詳細は、また審査が始まるということになるかもしれませんけれども、基本的に、今、我々が想定しているのは、そういった形で、現実的な評価で実態として持てばいいというふうに思っています。これは、だからデザインベースを超えている部分なので、そこに、無用なという言い方はちょっとあれですけれども、過度な保守性というものは期待するべきではないというふうに我々は考えています。

○原子力エネルギー協議会（谷川）　ATENA、谷川です。

もう一つ、例えば破断箇所、例えばLOCAの破断する場所なども、例えば最も厳しいとこ

ろを選ぶ必要はないとか、そういうところはいかがでしょうか。

○川﨑安全管理調査官　規制庁、川﨑です。

今、そこは想定はしていないです。ただ、そういった、例えば今SAの評価で、LOCAの破断面積とかいろいろ議論、LOCAにしてもそうなんですけど、なってくるんだとは思う、そういうのは、今後の議論の対象にはなるとは思っていますが、現状では、我々はそこまでは想定しておりません。

○三菱重工（内海）　三菱重工の内海でございます。

ページの10の信頼性要求のところなんですけども、一番最初のところに、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という、「その代替作動起動」というのが、具体的にはどういうことをイメージして書かれているかというのを、もしよろしければ御説明いただきたいんですけど。

○照井安全審査官　規制庁の照井です。

ちょっと御質問の趣旨をとり切れているか、ちょっとわからないんですけれども、「その代替作動機能」と言っているのは、代替作動設備が有する代替作動機能になりますので、要は非常用発電機の要求だと、非発要求だと思っていただければよくて、外部電源ができないという状態において、例えば自動作動に期待をするのか、手動作動に期待するのかというのはありますけど、物を動かすためには、当然、制御用でも制御電源が要るわけで、それは非常用の制御の電源に接続してくださいねということの意図で書いているんですけど、よろしいですか。

○三菱重工（内海）　わかりました。そのというのが外部電源のことかと、外部電源って、要するに電源の確保ということについての代替機能、作動機能というふうに読んでしまったので。わかりました。ありがとうございます。

○照井安全審査官　規制庁の照井です。

すみません。書き方が悪くて申し訳ないんですけど、そのが受けているのは代替作動設備ですね。代替作動設備の代替作動機能が、外電が利用できない場合でも、その代替作動設備は機能を喪失しないでくださいねということの要求で書いております。

○東京電力HD（遠藤）　東京電力ホールディングスの遠藤と申します。

同じちょっと10ページの信頼性のところで、外部電源以外にも、地盤とか地震とか、ほかの条文のものの適用又は準用するというふうに御説明いただいたんですけども、基本的に、ソフトウェアの故障って、あまりこれらとは関係しないと思うんですね。それは一般

的にそういうところかと思うんですけども、これを期待するというところは、これらが起こったときに、なおかつCCFを考慮すると。要は重畳するということを考えると。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。

基本的には、その認識でよろしいかと思っています。というのは、過渡・事故というものの起因事象に、ここら辺に書いているような事象というのは、過渡・事故の起因事象になるようなものも含まれていると思っていまして、じゃあ、要因は、別に過渡・事故の発生原因が内的事象に限るわけではなくて、外的要因によって起こる可能性もあるという、そのときに、今、想定としては、もう過渡・事故が、起因を問わず過渡・事故が起きたときに、デジタルCCFが重畳するということになりますので、そのときに、多様化設備が同時に死んでいるという状況になると対処はできなくなるということなので、これらの事象についても、きちんと多様化設備はこれらの事象に対して機能を維持するように設計をしてくださいという要求で書いております。

○東京電力HD（遠藤）　東京電力ホールディングスの遠藤です。

趣旨は理解できました。ただ、ちょっと、そういう意味では、これは安全保護回路そのものは、これらの機能をきちっと満足できていますので、ちょっと一つ、見方としては、ちょっと厳しいかなというところはありますので、本当に必要なのかというところは、これからの議論の中で少し理解を深められたらなと思います。

以上です。

○山中委員　そのほか、いかがですか。

○関西電力（池田）　関西電力の池田でございます。

11ページのところで、過渡・事故とソフトウェア共通要因故障が発生した状況で、多様化設備が有効に機能することにより炉心損傷を防止できることを最適評価により確認するというふうに明記していただいていまして、これはちょっと確認なんですけども、今回、先ほどもお話あったとおり、SA設備にも期待していいような、DBをちょっと超えたような状況になっているという認識なんですけれども、炉心損傷防止までということではなくて、例えばCV破損を防止できるようにできればいいとか、そういった考え方もあるとは思うんですけれども、ここは炉心損傷防止という考え方で設定された、その考え方を御教示いただければと思います。

○川﨑安全管理調査官　規制庁、川﨑です。

まずは、デザインベースの設備は、一定程度、健全なんですよね。これって、要は3層からちょっと出ている状況ですと。これは単純にSAのところを見ていただいてもわかるんですけれども、基本的にSAも、何でもかんでもCV破損防止できればいいというものではないんですよね。炉心損傷の防止は免れられないというちゃんと合理的な説明があって、あれはCV破損防止のほうに回されているわけですよね。なので、それを考えれば、当然、炉心損傷防止にここはクライテリアを置くでしょうという考え方です。

○関西電力（池田）　関西電力の池田です。

承知いたしました。

○東芝エネルギーシステムズ（加藤）　東芝エネルギーシステムズの加藤です。

9ページで幾つか質問があるんですけども、まず、先ほどの共通要因を、ソフトウェア以外の共通要因も要求する必要があるのかというのは、先ほどの質問の内容でわかったんですが、その中の補足のところで、安全保護回路と分離をしろというふうに最初の段落は読めるんですけども、この分離というのは、IEEEの314で言っているような電気系分離を要求しているんでしょうか。その場合、実際には、最後のアクチュエータは同じものを動かそうとしているので、その分離に対して本当に意味はあるのかというところは一つあります。

それから、それに関連するところですが、その後に火災の話も出てきますけども、先ほどの、今度、安全保護回路の定義をしましたといったときに、安全保護回路って機能の定義はしたんですが、従来のJEAC4604ですとかで、センサからアクチュエータの端子のところまでが安全保護系ですよと言っているんですけど、そこと同じ範囲でいうと、ケーブルも今回の安全保護回路の多様化の要求に入ってくるんでしょうか。その場合に、ここの今、火災の要求がされていますけども、本当に火災の、単一の火災に対して、それの独立性まで、火災の影響軽減まで今回の多様化設備で要求しているというふうに読まなきゃいけないんでしょうか、というのがもう一つと。

あと、補足の一番最後に書いてあります、同時に機能喪失しないようにとあるんですが、この機能と言っているのは、従来の安全機能と同一の言葉でいいんでしょうか。その場合ですと、本来であれば、安全保護系そのものが多重化されている、なおかつ独立されているので、既にもう安全保護系だけでそれは担保できていると思いますけども、それ以上の要求をこの最後の1行ではしているのかどうかを確認したいと思います。

以上です。

○照井安全審査官　規制庁の照井です。

まず、誤解しないでいただきたいのが、ここに書いてある内容は、安全保護回路に対する要求ではなくて、多様化設備に対する要求ですということで、基本的な考え方としては、今、事象想定としては、過渡・事故が起きたときに、安全保護回路はCCFに使いませんという状態を考えているので、その状態に至っているときに、多様化設備が同時に死んでいられては当然対処はできなくなるわけで、そうならないようにしてくださいというのが、ここに書いてある趣旨になります。

○東芝エネルギーシステムズ（加藤）　東芝エネルギーシステムズの加藤です。

最後のですと、じゃあ、実際に単一の火災が起きたときに、それに応じて過渡が発生しましたといったところまで考えろということですと、最初の、これとは別のところで、多重化は考えなくていいと言っているんですが、実際、単一の火災で、多様化設備が死ぬという、なおかつ過渡が起きるという事象は考えられるので、そういう意味だと、多重化をせざるを得なくなってくるんですけども、そこまでの要求をしているということになるんでしょうか。

○照井安全審査官　規制庁の照井です。

先ほどの御質問にもありましたけど、最後、補機が一緒なので、アクチュエータ部分が一緒になって、そこまで分離してくださいというと、それは当然、補機まで分離しなきゃいけなくなるので、そこまでの要求をかけているものではないです。それは補機は一緒なので、完全に独立しなさいということは無理だと思っています。

それから、今お話にあったように、過渡の起因となる事象で多様化設備が死ぬと、過渡とか事故の起因となる事象で多様化設備が機能喪失するというのは、これは結局、今想定している状態を考えれば、過渡や事故の起因となる事象で一緒にDASが機能喪失しているということは対処不能になるので、そこに関しては設計上の配慮をしてくださいということの要求になります。

○東芝エネルギーシステムズ（加藤）　ということは、東芝エネルギーシステムズの加藤ですけども、最後のお話は、実際には安全保護系を多重化されていて、影響軽減で、どちらか助かればいいというところはあるんですけども、今回の多様化設備は、過渡が起きるような事象があるケーブルからは全て独立させろということになってくるので、かなり厳しい要求だとは思っています。

それで、だんだんちょっと離れていくんですけども、本来のソフトウェアの共通要因故

障というところからかなり離れていっているような気がするんですけども、そこまで要求してしまうと、完全にどこからも、どの設備からも完全に分離させないと、多分、成立しないんじゃないかとちょっと思っているので、それなりに厳しい要求かなとは思っています。

○照井安全審査官　規制庁の照井です。

ちょっと、その辺を具体的に、どこがどう、困るのかという言い方が正しいのかどうかわかりませんけれども、この後、第2回、3回か、次回検討チームの意見の場もあるので、もう少し、ちょっと今、具体的に何も根拠がない状態でここで議論していてもあまり深まらないと思うので、具体的にどういう、例えば今現状の設計がどうなっていて、こういうことが困るんですというのをもう少し具体的に、次回でも議論をさせていただければというふうに思います。

○東芝エネルギーシステムズ（加藤）　はい、わかりました。

○三菱重工（内海）　三菱重工、内海です。

一番大もとの前提の話なんですけども、ソフトウェアを使ったデジタル安全保護回路というものがあって、そこにCCFを想定するということなんですが、安全保護系の中で、全ての部分がデジタル化されているとは限らないわけなんですけれども、この文章の読み方なんですが、そういったソフトウェア共通要因故障によって、安全保護回路の機能が喪失すると想定するというと、喪失する想定をするのは、あくまでもソフトウェアで実現しているもの、あるいは、そこの故障で直接影響を受ける範囲というふうに限定して考えてよろしいですか。

○照井安全審査官　規制庁の照井です。

基本的に、その理解でよろしいと思います。通しの5ページで、一応、今ここで考えているデジタル安全保護系というのは、ソフトウェアを用いることに安全保護機能全部又は一部を作動させるものをデジタル安全保護系と言っていて、そのソフトウェアが共通要因故障により機能を喪失するということになりますので、逆に言うと、ソフトウェアじゃない部分というものは機能を喪失しないということになります。

○原子力エネルギー協議会（富岡）　ATENAの富岡です。

ありがとうございます。最後の13ページのところなんですけれども、事業者意見がある場合には次回の会合でと書いてありますので、ぜひお願いしたいと思いますが、ここにまさに書いてありますように、科学的・技術的な観点から議論すると、有意義な議論を行う

ため、理由とか文献とかデータとか、まさにおっしゃるとおりだと思いますが、今日、これを初めて見たばかりですので、ちょっと今日だけではなかなか、全てこれを理解しているかどうかちょっとわからないところがあります。次回の議論を有意義に行うためには、途中で質問とか、それは適宜させていただくということでよろしいでしょうか。

○西崎企画調整官　規制庁の西崎です。

今日、御説明して、御質問を受けたのですけれども、ちょっとさっきもありましたけれども、完全に我々も御質問の趣旨が理解できていないところもあるので、皆様も聞きたいところを全部聞けていないと思いますので、この資料について御質問があれば、またお受けしたいと思います。

○山中委員　そのほか、いかがでしょう。よろしいでしょうか。

どうぞ。

○山田総括審議官　規制庁の山田です。

先ほど独立性のことでお尋ねがあったと思うんですけれども、今回、我々がここで要求をしたいと思っていますのは、もうこれは趣旨は御承知いただけていると思いますけれども、ソフトウェア起因で安全機能を喪失するということへの対処を考えたいということですので、先ほど幾つか御指摘があったような、ケーブルをどうするんですかとかという話は、我々がそもそも想定している趣旨からすると、そこは共通要因故障の対象ではない話なので、今回、我々、こういう書き方をしていますけれども、こういう書き方だと、こういうところについて独立性を要求されると、そもそもの趣旨と違いますということであれば、その旨を明確にしていただいて、これは違うでしょうという確認をしていただければというふうに思いますが。

○山中委員　よろしいでしょうか。

それでは、次に原子力エネルギー協議会（ATENA）から、産業界の現状、今後の見解等についてお伺いしたいと思います。よろしくお願いします。

○原子力エネルギー協議会（富岡）　ATENAの富岡です。

デジタル安全保護回路のソフトウェアの共通要因故障ということですけども、ATENAが産業界で安全性の向上を検討するという中で、一つのテーマとして取り上げているものでありまして、ATENAのメンバーである事業者、それからプラントメーカーというようなところの意見を取りまとめて、今回、この会合に出席させていただいているということですので、これから説明する資料につきましても、ATENAとして御説明するものでございます。

よろしければ、中身の説明に入らせていただきたいと思います。

○原子力エネルギー協議会（谷川）　ATENA、谷川でございます。

それでは、資料の15ページから御説明しますけど、これは目次を示したものでございますので、割愛いたします。

16ページに行きまして、デジタル化する意味・目的ということでございますけども、御存じのように、1970年代に、アナログ制御装置で制御していたということでありまして、アナログ制御装置というのは、下にありますように、抵抗、コイル、コンデンサ、トランジスタででき上がった回路でございまして、やはりどうしてもドリフトがあったりとか、いろんなことがありまして、さらには生産が減ってくるとかということもありました。一方では、ICとかLSIのデジタル製品がどんどん世の中に広まってきまして、そこで原子力においてもデジタル製品を適用していこうということで、1980年代の中盤から、デジタル制御装置を段階的に原子力プラントに適用してきたということであります。ここで言うデジタル制御装置というのは、右の絵にありますように、マイクロプロセッサの上でソフトウェアが動作する装置というふうに定義しております。

決して、現在、アナログ装置がまだ安全保護系に使われているわけでありまして、その保守性が低下しているとか、そういうことを言いたいわけではありません。これはメーカーもきちっと予備品を確保したりして、保守もしっかりやっておりますので、安全保護系については、そういう問題は一切発生していないという状況でございます。

次のページに行きまして、原子炉施設に導入しているデジタル化、どんな技術を導入したのかということを簡単に御説明したいと思います。アナログ回路から単純にデジタルに置換をしたというのに加えまして、デジタルだからこそできる自己異常診断、あるいは保守ツールを導入して保守性を向上するとか、あとは、アナログ装置では非常に難しかった多重化というのをデジタルでは実現したということで、運転信頼性を向上したと。さらには監視・操作系に、VDU等がありますけれども、フラットディスプレイとかCRTを導入したということ。それから、それにタッチオペレーションもつけまして、監視操作盤を少し小さくしたりとか、ケーブルを少し本数を減らしたりとかということをやってきたと。

そういうことによりまして、一方ではプラント運転支援の拡大、これはまた自動化を導入したりとかして、プラント全体としては信頼性を上げる方向に持っていったということ。さらには、安全保護系にソフトウェアを適用する場合に、ソフトウェアの信頼性というのは、非常にやはり気になっていましたので、例えばここにありますようにシングルタスク

処理を行う、あるいは定周期処理を行う、シンプルな構造・機能を適用するということと、あわせて、そこでつくられたソフトウェアのV&Vをきちっと実施すると。その際には、可視化言語によって、第三者でも容易にチェックできるというシステムを取り入れまして、ソフトウェアの信頼性を大幅に向上してきたということをやってまいりました。そういういろんなデジタル化技術を安全保護系に対して適用したということでございます。

次の18ページにまいりまして、そういうデジタル安全保護回路がデジタル化されているプラントですけれども、当初からデジタル化されているプラント、すなわち新設プラントでは、PWRでは泊3号機、BWRでは柏崎6、7号機以降の新設プラントにおいて、デジタル安全保護回路が適用されているということであります。それから、既設プラントであれば、アナログをデジタル化更新したプラント、あるいは計画中のプラントは、高浜、大飯、美浜ということで、多くのプラント、PWRのプラントで、そういう更新もしくは計画がされているという状況であります。

次に、安全保護回路の範囲でございますけれども、デジタル化の範囲というのは、設定値比較回路及び論理演算回路ということになりますので、工認の範囲とは少し違いますけれども、我々、CCFの範囲というのは二つを含んだ範囲を考えているということであります。

それから、ソフトウェアの信頼性向上に対する取組を簡単に御説明したいと思います。

下に、ソフトウェアの向上が書いております。これはマイクロプロセッサでの動きといいますか、構造を示しております。オペレーティングシステムというのがありまして、これがいろんなタスクを動作させるのをつかさどっているということになります。それのキック信号によりまして、信号を入力処理するところ、その結果を用いて論理演算をするところ、そして、それを信号として出力するところと。大ざっぱに言いまして、こういう構造になっておりまして、これがシングルタスクといいまして、最初、キック信号が出れば、そのまま出力をして一つのタスクが終わると。同じタスクが何度も何度も続いていくという、それを定周期処理で処理していると。ウィンドウズのような割り込み処理というのは一切行っていないということであります。また、OSは、そういう処理を定周期で制御するという、非常にシンプルな機能を有しておりますので、決して複雑なものを適用しているわけではないということでございます。

21ページにまいりまして、そういうソフトウェアの信頼性を向上する取組として、産業界でやっていたのがJEAC4620/JEAG4609を自らつくりまして、ソフトウェアサイクル及び

管理手法を含めた品質保証活動、そしてV&Vを実施してきたということで、下の絵にありますように、システムの設計要求仕様から、ハード・ソフトウェアの要求仕様をつくる、そしてソフトウェアの実際に設計をする、ソフトウェアを装荷する、そして最後にハードと組み合わせて試験をすると。こういう一連のライフサイクルに対して、きちっと校正管理手法を適用しまして、上流側の要求がきちっと当初に反映されている、最後のものに反映されているということを各段階ごとに確認していくということで、検証とありますけれども、入力と出力をきちっと検証していくというのを入れると同時に、最後に、でき上がったものに対して妥当性確認試験を行うということで、こういうサイクルをきちっと回すことによって、信頼性の高いものをつくり上げてきたということで、当然ながら、CCFと思われる事象は一切発生していないということであります。

それから、次のページにまいりまして、そういう非常に信頼性を上げてきたわけではありますけれども、やはりソフトCCFが、じゃあ絶対起こらないかというと、そこはやっぱりゼロとは言えないということで、その部分に対しては、自主的にバックアップ設備を設けて信頼性を確保しましょうということで、デジタルの安全保護系は四重化されているわけでありますけれども、同じソフトが入っているということで、一つのソフトに、もしエラーがあると、それは四つのソフトとも不動作になる可能性があるということで、右側にありますようにバックアップ設備を、ハードワイヤードのものを設けました。センサは、そのソフトは用いておりませんので、センサの信号を用いて自動的に原子炉を停止させる機能とか、あるいは手動でポンプなどを立ち上げる機能を持たせるということと、もう一つは、デジタル安全保護回路のCCFでは、監視系も表示がおかしくなる可能性がありますので、ハードワイヤードの監視系を用いて操作を行えるようにしたということであります。

23ページに行きまして、じゃあ、どういう操作ができるのかということを示しております。これはABWRとPWRで若干違いますので、それを書いております。ABWRの場合は、自動作動系ということで、原子炉スクラム、それから再循環ポンプトリップが行われるようになっております。操作としては、やはり手動でスクラムを行える、あるいは主蒸気隔離弁を閉止する、あるいは主要な隔離弁を閉止するということと、高圧炉心注水系を起動できるようにしております。監視系は、そのような手動操作が確実に行われたことも監視できるようになっているという状況であります。

PWRも基本的には考えは同じでありまして、原子炉トリップ、それからタービントリップ、主給水隔離、補助給水起動というのは、反応度制御を行うためのものだということで

あります。操作もほぼ同じでありまして、原子炉トリップ、タービントリップ、あとは高圧注水系起動、それから補助給水と、格納容器隔離というところが手動で行われまして、その動作を確認するために必要な監視系がついているということであります。ここで、自動操作系というところが、先ほど話題になりました新規制以降の重大事故等対処設備というものを、ここでもバックアップ設備という形で定義をしているところであります。

24ページに行きまして、じゃあ、そのバックアップ設備の設計の考え方、あるいはスペックはどうなんだということで、これは新規制基準適用後の現状仕様を示しております。まず、バックアップ設備の中の操作系と監視系でありますけれども、これは常用系並みの設計としております。耐震要求も、そういった意味ではCクラス要求としていますが、実力としては、やはり安全系の機器を起動するというところもありますので、操作系についてはSs機能維持というのが実力です。そういうことによって誤動作防止を図っているということと、監視系につきましては、部分的にはSsかもしれませんけども、電路も含めて見ると、そうではない場合もありますので、部分的にSs機能維持になっているという言い方がいいのかもしれません。多重性は持たせておりませんので、シングルだということと、耐環境性というのは、事故時の条件下で機能維持という条件になると。操作監視場所は、基本的には中央制御室です。

それから、バックアップ設備につきましては、これは重大事故等対処設備の一機能をこれに割り当てているということでありまして、耐震性はSs機能維持ですし、多重性は回路の信号の部分を多重化していたり、回路を二重化しているという、若干、ABWRとPWRで異なりますけれども、単一の故障による誤動作を防止するというところを主眼に多重性を図ってきております。それから、耐環境性は事故時条件下で機能維持と。設置場所も中操ほかということになっております。

それから、25ページは安全保護回路でCCFが発生した場合の対処ですけれども、異常が発生しまして、装置の故障を示す警報が中央制御室に発報された場合には、警報の内容及び装置の状態を確認して、それで各事業者の社内規定に基づいて必要な措置を実施するということと、保安規定の制限に定める所要系統数を満足していないと判断した場合には、これは保安規定に定める措置を実施するということであります。

じゃあ、警報が発生しない場合はどうなのかということですけれども、これはバックアップ設備による原子炉トリップ、あるいは隔離弁閉鎖、高圧系の注入を行うという対応が可能なようになっております。

それから、安全保護回路のデジタル化の今後の見通しですけれども、ABWRは既にデジタル化されているという状況であります。BWR5は、現時点ではデジタル化されていないということで、現段階では、安全保護回路のデジタル化の計画はないという状況であります。PRWは、安全保護回路のデジタル化を進めているという状況であります。

それから、9番はPLD等の新しいデジタル機器を実機に適用する、どんなふうに考えているのかということですけれども、まずはFPGA等のPLDと書いてありますけども、FPGAはField-Programmable Gate Arrayということで、これはPLDの一種であります。PLDはProgrammable Logic Deviceということで、最近、制御を行うときに、こういうものが世の中でかなり使われてきているという状況であります。

このようなデバイスは、既にマイクロプロセッサや通信系コントローラのインターフェイス回路において、信号変換装置の一部と、デバイスということで、既に原子力発電所のデジタル装置にも適用されています。それはハード部品というような趣旨で取り扱っているという状況であります。そういう、例えばFPGAであれば、当然、単なる信号変換装置だけではなくて、大規模なロジックも組めるわけでありまして、その例が下に載っております。PLD構成（例）ということになります。これはI/Oがあったりとか、ロジックセルという中にANDとかOR回路がたくさん入っているということでありまして、それをつなぐことによって、それで安全保護回路のような大規模な装置もつくり上げることができると。

マイクロプロセッサとの大きな違いは、OSみたいなものがないということですね。あと、一旦、もう書き込んじゃうと、焼きつけちゃうとですね、簡単には変更はできないというところであります。

現時点で、事業者として、このPLD回路をデジタル安全保護系に適用する計画は、現時点ではないという状況であります。一方、PLDはマイクロプロセッサとは異なる構造でありますので、バックアップ設備に適用して、マイクロプロセッサと多様性を確保することが、これは十分可能だと思っておりますので、そういう使い方は今後もされていくのかなというふうに思っております。

次に、基本方針ということで、先ほど規制案を聞いたので、少ししゃべりにくい部分もあるんですけれども、簡単に御説明します。これまで事業者が自主的に備えてきたCCF対策の規制化に当たっては、効果的に安全性を高める観点から、以下のような配慮が必要だと考えているというところでありまして、ちょっといろいろ書いていますけども、実施方法については、仕様規定ではなく、性能規定にしてもらえないだろうかということで。今

回、規制案としては、性能規定に近い表現だったのかなというふうに今は感じております。

それは先ほど申し上げましたように、多様化設備としてはアナログも選択をしてもいいし、PLDというのも一つの多様化設備としては選択の余地がありますので、どちらでも選べる形にしてほしいというのが、この背景であります。

今度は、性能については、ちょっとこれもいろいろ書いてはいるんですけれども、やはり言いたいところは、発生確率が非常に低い事象に対しては、やはり判断基準も含めて少し発生確率に応じたような判断基準を適用したいというようなところを言いたかったわけでございます。それはいろいろ御質問させていただきましたので、次回会合に向けて、少し我々の考えをまとめていきたいというふうに思っております。

それから、設備追加等の対策が必要な場合には、適切な経過措置期間が設けられることということでございます。

2番に書いておりますように、産業界としましても、効果的に安全性を高めるために必要な検討はしていきたいというふうに思っておりますので、今後の会合を通じて意見交換を進めさせていただければというふうに考えております。

以上です。

○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。

○遠山課長　技術基盤課の遠山ですけれども、幾つか資料の確認をさせていただければと思います。

最初に19ページですが、先ほどの御説明ですと、デジタル化の範囲というのは、点線のところでやっているという趣旨とお聞きしましたが、それでよろしいですか。

○原子力エネルギー協議会（谷川）　ATENA、谷川です。

そのとおりでございます。

○遠山課長　続きまして、資料の20ページ、処理はシンプルなものとするというお話がありましたけれども、これは一つのマイクロプロセッサで行っているのでしょうか。それとも、複数で分担する場合もあるのでしょうか。

○原子力エネルギー協議会（谷川）　これはプラントによっても違いますけれども、複数の場合もあれば、1台で行う場合もございます。

○遠山課長　続きまして、23ページですけれども、下の※で、重大事故等対処設備として扱っていると、先ほどの議論の中でも出てきましたけれども、この部分は、バックアップ設備とは異なる設備になっているんでしょうか。

○原子力エネルギー協議会（谷川）　いや、同じでありまして、バックアップ設備としても位置づけていると。重大事故設備だけれども、バックアップ設備としても位置づけているということでございます。

○遠山課長　それから、その次の24ページで、幾つか細かいことが書かれているんですけれども、大きく分けると手動と自動の設備で、設計グレード、特に耐震性が異なるんですけれども、その意図というのは何かあるのでしょうか。

○原子力エネルギー協議会（谷川）　ATENA、谷川です。

これは、もともとは手動と自動も同じように常用系の設計としていましたが、自動のほうが、ATWS対策設備という形で、重要事故等対処設備になりましたので、それで、こちらが、ある意味、格上げになったということでございます。

○遠山課長　そうすると、先ほど位置づけているという御説明があったんですけれども、設備の耐震性を上げたということですか。

○原子力エネルギー協議会（谷川）　はい、そのとおりであります。

○遠山課長　それから、PWRのところで、自動と手動操作のところで誤作動防止と書いてあるんですけれども、これはどういう意味なんでしょう。

○三菱重工（内海）　三菱重工、内海でございます。

こういうバックアップ設備が作動することによって、例えばプラントに外乱を与える可能性があります。そういった事態をなるべく極力減らしたいということで、誤動作防止ということについては気を使っておりまして、多重化という考えもありますし、一つのポイントが多重化ですし、一つのポイントがこういった耐震性を持たせることによって誤動作をなるべく減らしてやろうということでございます。

○遠山課長　それから、設置場所でPWRが「中央制御室他」と書いてあるんですが、これは中央制御室ではないという意味ですか。

○関西電力（池田）　関西電力の池田でございます。

中央制御室以外でも、リレーラック室といったところでも操作するといったものがございますので、それを他で記載してございます。

○遠山課長　それから、先ほどの多重化の考えのところで、信号を多重化する場合と回路を多重化する場合とがあるようですけれども、何かこの考え方の違いというのはあるのでしょうか。あるいは、信号を多重化することで誤作動を防止しようとしているということなんでしょうか。

○原子力エネルギー協議会（谷川）　ATENA、谷川です。

BWRに関しましては、信号を多重化することによって誤作動を防止するという考えでございます。

○三菱重工（内海）　三菱重工、内海です。

PWRの場合、確かに回路という表現をさせていただいておりますけれども、実際は、センサも含めて、センサ、それから回路部分を含めて、2系統以上設けて、その一致で作動すると。そういうような回路にすることで、センサから作動回路まで含めて単一の故障では誤動作しないようにしています。

○遠山課長　それから、次の25ページですけれども、デジタル安全保護回路の装置の故障を示す警報というのがあるんですけれども、これは具体的にどんなものなんでしょう。特に待機系である安全保護系の故障というのは、どうやって示すのかなという質問です。

○三菱重工（内海）　三菱重工、内海でございます。

確かに安全保護系は、通常時は何も作動していない状態で待機しております。ただ、デジタル安全保護回路というのは、その間、ソフトウェアの実行をとめているわけではなくて、先ほどのスライドにありましたが、一定の周期で入力、演算出力というのを常に行っています。ただ、何も事態が起こらなければ出力は変化しないだけということになっておりますので、その実行のサイクルの中で、いろいろな方法がありますけども、自己診断機能と呼んでおりますけれども、自分自身の健全性をチェックする機能、あるいは動作状態をソフトウェアを実行しているプロセッサの外から監視する、ウォッチドッグタイマと呼んでおりますけれども、そういった監視回路をつけたり、そういうことで常に、何か異常が発生したら、それを検知できる機能を組み込んでおります。それが何かを検知した場合に、異常であるということで警報が出るということになっております。

○遠山課長　どうもありがとうございました。

○山中委員　そのほか、いかがでしょう。

○山田係長　技術基盤課の山田です。

資料の確認、書いてあることの確認をしたいと思っていまして、通しの21ページのところですね。これまで導入した実績では、CCFは起きていないということが書いてあって、そこに※で定義が書いてあるんですけども、この定義を超えると何かトラブル事象があったりするんですかね。※で限定して書いてある意味が何かあるのであれば教えてほしいです。

○原子力エネルギー協議会（谷川）　これはちょっと機能喪失が起こっていないよという意味ではなくて、複数のコントローラが同時におかしくなったという事例はないというふうに読み取っていただければと思います。
○山田係長　わかりました。ありがとうございます。
それから、もう一件は、通しの22ページなんですけども、ポンチ絵で描いてあるので簡略化されていると思うんですけど、実際、バックアップ施設でどういうふうにラインが分岐していて、デジタルの安全保護回路の多重化というのは、どこの場所で多重化されているのかというのは、もうちょっと補足的に教えていただいてもいいですか。
○原子力エネルギー協議会（谷川）　ATENA、谷川ですけども。
バックアップ設備、センサから分岐するところにはアイソレータが入っていまして、バックアップ設備の影響が、安全保護回路に影響に及ぼさないようになっているということと、検出器は四重化されておりまして、その四重化信号がそれぞれ4台のデジタル安全保護回路に4信号入っていきまして、そこで信号が設定値に達したかどうかをチェックして、そして2out4のロジックを組んで、2out4以上のロジックが成立すると、原子炉スクラムなどの動作を行うという構成になっています。ちょっとこの絵にはその部分の表現はしておりませんが、そういう構成になっております。
○山田係長　わかりました。ポンチ絵なので、そういうことなんだと思いますけれども、検出器も複数並べて描いてあって、それの検出器に対して同じように構成になっているということですか。
○原子力エネルギー協議会（谷川）　はい。例えば原子炉圧力であれば、原子炉圧力信号を、四つの信号がありますけども、四つの信号、それぞれデジタル安全保護系の四つに入れまして、その入れた信号で2out4を組んでいくという構成になっております。
○山田係長　バックアップ設備の設置の仕方も、それぞれの検出器で同じという。
○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。
バックアップ設備のほうは、自動のものは多重化してあるものもありますけども、手動のものはシングルであったり、その機能によって、そこはいろいろという形になっています。
○山田係長　わかりました。ありがとうございます。
○山中委員　そのほか。
どうぞ。

○成田課長補佐　規制庁、成田と申します。よろしくお願いします。

今のポンチのちょっと追加の質問なんですけども、バックアップ設備の手動操作系というのが青く四角で囲んでありますけども、一方、左側の黒いほうの検出器から流れてくるセンサの信号以外に、手動の操作系を働かせるために、この絵、何を見て判断するのかというのは、ちょっとポンチ絵ではわかりづらかったので、さっきの御説明で、右下にある青囲みの監視系と呼ばれるものとの関係があるのかどうかも含めて、すみません、ちょっと御説明いただけますでしょうか。

○原子力エネルギー協議会（谷川）　ATENAの谷川です。

ちょっとわかりづらかったのですけれども、次のページに、操作系と監視系が入っております。例えば高圧炉心注水系を起動するときは、原子炉水位とかドライウェル圧力の状態を見た上で高圧炉心注水系を起動すると。その起動をするためには、主要な隔離弁の状態、冷却材浄化系もしくは原子炉隔離時冷却系の内側隔離弁を閉めた状態で起動するというために隔離弁の状態を示しております。

起動したことを確認するためには、起動状態、それから系統流量を監視系に指示しておりますので、操作した結果が正常に動作したということの確認も、この監視系で行うということで、操作系に合わせて監視系を準備しているという趣旨でございます。

○成田課長補佐　規制庁、成田です。

ありがとうございました。

○山中委員　そのほか、いかがですか。

○今瀬専門職　規制庁の今瀬と申します。

25ページ、先ほど操作の故障を示す警報に関して御質問をさせていただいていたんですけども、ちょっとそれに関連して、ウォッチドッグタイマ等の自己診断機能に期待しているということなんですけども、一つは自己診断、ウォッチドッグタイマ等の自己診断にひっかからないような故障モードについて考慮されているかということと、もう一つ、ウォッチドッグタイマで、例えば、含む自己診断機能による検知が成功したとしても、例えば中央計算機、あるいは警報システムのような上位伝送ができなくなるようなプラットフォームに関するCCFが発生するようなケース、これを考慮しているかどうかについて、それぞれPWR、BWRについて教えていただきたいんですけれども。

○三菱重工（内海）　三菱重工、内海でございます。

自己診断機能、もちろん常に、即座に故障が生じれば見つかるということでいいんです

が、それだけで全ての故障が見つかるというふうには我々は考えておりませんで、そういう意味では、今御指摘いただいたようなケース、これはちょっと個々のケースによって違うと思いますが、何かそういうものはあり得るというふうには思っています。つまり、それはCCFという意味ではなくて、故障の発見という意味ですね。

当然、安全保護系は、先ほど申し上げましたように、通常時は動いておりませんので、保安規定に従って定期的に実作動させることによって、その機能を確認していくと。自己診断と定期的な実作動、これをあわせることによって、故障が放置される状態というのを極力減らすような設計にしています。

○今瀬専門職　BWRも同じような考え方でよろしいんでしょうか。

○東芝エネルギーシステムズ（加藤）　東芝、加藤です。

PWRと同じ考えです。

○今瀬専門職　ちょっとすみません、これにまた関連して追加の御質問なんですけども、先ほどのように、上位伝送ができないとか、自己診断に失敗するという、プラットフォームに関する故障というのは、故障頻度は非常に低いかと思うんですけども、諸外国の例では、アプリケーション部分の故障発生率と、プラットフォームの部分の故障の発生率とかをある程度区別して評価するとか、そういった評価もされていると聞いているんですけれども、国内では、そういった取り扱いはされているんでしょうか。

○三菱重工（内海）　三菱重工の内海でございます。

ちょっと答えが難しいんですけれども、要するにそういった差が出てくる可能性というのは、例えば諸外国において、そういった共通的なプラットフォームとしてのソフトウェアはどうか、あるいはアプリケーション、アプリケーションという意味は、例えばこれは原子炉停止系のソフトウェアで、これは工学的安全施設作動用のソフトウェアだと、そういう意味で、違う機能を持たせている場合に、アプリケーションが違うというふうに言うんですけれども、そのときにそれを分けて考えるというのは、多分、CCFの物の見方が多層的になっているからだと思うんですね。つまりアプリケーションの部分が、何らかの設計ミスが、例えばロジックのつなぎ忘れがあったとか、あるいは設定の、1桁間違えていたとか、よくある話なんですけど、そういう一般的な間違いをしていた場合には、同じ機能をつくり込んだ、例えば工学的安全施設だけが共通の影響を受ける、ただ、原子炉トリップのほうは影響を受けない、そういうような違いが出てくる可能性があります。

一方、プラットフォームの場合には、全設備が同じソフトウェアといいますか、のもと

で動いていますから、どの設備も同じように影響を受けてしまって、その違いをですね、当然、機能的な表れ方は違ってくるわけですが、一部の機能だけがCCFの影響を受ける場合、あるいはもっと広い、全部とは言いませんけど、もっと広いものが影響を受けるケース、それを分けて、例えばPRAのようなもので分けて考えるとか、それに何らかの発生の頻度という概念をうまく使って、そこの区別をしてやるとか、そういうような議論をするケースもあるので、それで分けているんだと思いますが、国内の場合は、ちょっと今正確なことは申し上げられませんけど、PRAの中でも似たような概念はある程度導入されていると思います。それはちょっと、現在、この場で詳細にちょっと御説明できませんけども、そういうことも一部は考えています。

○今瀬専門職　どうもお答えありがとうございます。

基本に関しては、ちょっとしつこく聞いていますのは、やっぱり異常が検知できるかどうかで、特に手動操作に対応されるような計画が多いので、その起点となる警報というのが的確に検知できるかどうかというのは非常に重要だと考えておりまして、また機会があれば、ちょっと正確なところ、あるいは詳細なところを御説明いただければと思います。

○西崎企画調整官　規制庁、西崎です。

24ページに関連して伺いたいんですけれども、バックアップ設備についてお伺いしますが、自主的にバックアップ設備を設けられているということなんですけども、当然、その設備を設計するときには、例えばある一定のこういった事象を考えたときに、この範囲で対応できるように設計しようということでされると思うんですね。今、自主設備というのは、どういった事象を考えて、それがどの辺でおさまるように設計されているのかというのを確認したいんです。

その趣旨はさっき、我々が言うところの判断基準はちょっと厳しいんじゃないかというふうに質問があったと思うんですけど、じゃあ、皆さんは今どういうふうな事態を想定して、どの辺で抑えるように設計しているのかというのをお知らせいただけますか。

○原子力エネルギー協議会（谷川）　ABWRで言えば、例えばバックアップ設備の操作系、監視系については、1系列しか設けていない。だけども、基本的にはLOCAが起こっても対応できるようにというふうに考えています。そのLOCAが起こってもという条件は、さらなる機械系の単一故障は想定しないとか、あるいは破断、ABWRの場合は、高圧注水系の配管の破断をLOCAと、中LOCAというふうに仮定しますので、当該の操作ができる配管ではLOCAは発生していないこととか、そういう、ある仮定のもとに選んでいるということで、その

仮定のもとであれば、例えば事故の基準は満足できないかもしれないけども、大きな破損には至らないとか、そういうようなクライテリアといいますか、で考えているという。つまり、全ての事象に対して対応できるようにということではないという、ちょっと答えになっていませんけども、そういう状況です。

○西崎企画調整官　規制庁、西崎です。

全ての事象、事故・過渡の全ての事象ではないという趣旨と理解しましたけれども、じゃあ、想定する状態はそうだとして、そのある想定している状態については、さっき対応できることという説明だったんですけれども、対応できるというのはどういう意味なんでしょうか。さっきはCV破損でいいんじゃないかという意見もありましたけど、CV破損ができるようにしているという理解なんですか。

○原子力エネルギー協議会（谷川）　やはり設計基準事故と重ね合わせて起こるというところが、やはり自主設備でありましたので、そこがやはりポイントでありまして、重ね合わせで起こる可能性は低いということを考えまして、事故の基準ではなくて、Beyond DBの基準で考えてもいいんじゃないだろうかということで、あまり事故の基準を満足できるかどうかという目で事象を見ていたわけではございません。

○西崎企画調整官　規制庁、西崎です。

わかりました。御説明はわかりましたけど、ということは、炉心損傷防止ができるようなバックアップ設備にはなっていないという理解でいいですか。

○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。

まず前提が、多分、今の立ち位置と、当時バックアップ設備をつくったときの立ち位置が違っていると思っていまして、当時、建設時のときは、やっぱり事故事象、設計基準に対しては安全保護系で基本的にはカバーすると。それは、そのために多重化なりV&Vをやって、きちんとソフトウェアの品質保証をして、それで確保するというのが大前提です。その上で、ただ、今議論になっているとおり、デジタルCCFというところは、やっぱり気になる部分というところがありまして、事業者としては自主という形で、先ほどありましたけど、何らか対応ができるようにということで、デジタルCCFにLOCAを踏まえた、LOCAを重畳させたケースというのを踏まえてそれに対応できる、基本、自動起動のところを何らか対応できるという意味では手動でちゃんと起動できる、運転員が気づけば手動で起動して注水ができるとか、そういうところをちゃんと確保しておきましょうというところで設置したというのがこの設備になります。

ですので、事故事象を全てカバーできるとか、炉心損傷防止を必ずカバーできるとか、そういうところまでは当時は議論をしていませんし、そこまでは、突き詰められると、確保できますということはちょっとこの場では言えないかなというところです。

○西崎企画調整官　規制庁、西崎です。

御説明はわかりました。

当時考えられていたのはそうだとして、今、現状の実力というんですか、実態として、今、LOCAとおっしゃいましたかね、LOCAとソフトウェアCCFを重畳させたと仮に仮定して、それで、どの範囲でおさまるという設計に現になっていると理解すればいいですか。

○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。

どの範囲というところが、どういうふうにイメージすればよろしいですか。

○西崎企画調整官　規制庁、西崎です。

さっきのお言葉をかりると、クライテリアというんですか、建設当時に設計上の、バックアップ設備に対する設計上のクライテリアって、特に設定されていないということですか。

○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。

クライテリアというところが、事故を確実に収束できるとか、そういうところのクライテリアであれば、それはそこまでの議論はされていないんですけども、そういったところを踏まえても、ある程度きちっと対応して、収束に持っていけるだろうというところで自主の設備をつけているということです。

○西崎企画調整官　規制庁、西崎です。

ちょっと同じ質問ばかりするとあれなので、やめておきますけど、きちっと対応されているというのが、どのレベルかを確認したいので質問しているんですけど。もう一回だけいいですか。そこをちょっと確認したいんですけど。

○原子力エネルギー協議会（谷川）　そうですね、この自主設備を決めたのが1990年の初めのころでありまして、米国でもそういう議論がいろいろなったときに、KK6，7（柏崎刈羽6、7号機）の建設最中だったのかな、そういう情報も加味しながら自主設備をつけるという判断をしたというときに、どこまで想定したのか、あるいはどんな結果をもとに判断したのか、どんな条件で考えたのかというのは、少し調べさせてください。

○西崎企画調整官　規制庁、西崎です。

承知しました。

あと、今、最後にしますが、米国の話が出たんですけれども、さっき、我々の判断基準が、炉心損傷防止が厳し過ぎるんじゃないかという意見がありましたね。そのときに、いや、諸外国の例から見ても厳しいんじゃないかということを言われていたと思うので、諸外国の例をよく調べられた上で言われているんだと思うんですが、例えば米国だと、NUREGの6303ですかね、だと、どういう要求になっているのか教えてもらえますか。クライテリアですね。クライテリアはどういうふうに設定されていると認識されていますか。

今日、時間がないので、ここではいいですけど、それについて御意見を出されるときに、さっき我々もパワーポイントで言いましたように、諸外国がそうだからと言われるのであれば、理由の一つにされるのであれば、諸外国の例をきちっと説明していただければと思うんですね。D3解析というのをやっていると思うんですが、じゃあ、CV破損防止でやっていますかということを説明していただければと思います。これはコメントなんですが。

私からは以上です。

○原子力エネルギー協議会（谷川）　すみません、ATENAの谷川です。

英国においては、やはり発生確率をベースにして議論をしていまして、LOCA＋CCFは、それは事故を超える事象だということで、事故の基準では少なくとも評価をしていないというのも一つの事実として申し上げた次第であります。

○川﨑安全管理調査官　規制庁、川﨑です。

ちょっと、先ほど私から申し上げればよかったんですけれども、参考でついている通ページ、65ページを見ていただくと、一応、ここで、我々が調べた範囲で各国がカバーしている事象というのは示しておりますので、これも参考です。

規制庁、川﨑です。

私から、次回ちょっとこうしたことを示していただきたいなというのがあって、先ほど山田からバックアップ設備がどのように接続されているのかというのをちょっと示してくださいというようなコメントを出していましたが、ATENAの資料でいうと通しページ19ページですね。これは今回、ちょっと我々デジタルが共通要因、CCFで使えないというふうに見るべきというふうに思っているのは、設定値比較部も含めて使えないときというふうに考えていまして、実際、安全保護系、機能によるんだとは思うんですけれども、この設定値比較部の前のほうからバックアップ系のほうに行っているのか、そうした情報も少しわかるように今後示していただいて、議論をさせていただきたいと思います。

○原子力エネルギー協議会（谷川）　わかりました。非常にポンチ絵過ぎて、信号の取り

出し場所もわからないような状況ですけども、その辺りは明確に取り出し場所もわかる形で、CCFではそこに影響がないということを御説明できる形でしたいと思います。

○川﨑安全管理調査官　規制庁、川﨑です。

ありがとうございます。

○山中委員　そのほか、いかがですか。

どうぞ。

○照井安全審査官　規制庁の照井です。

今の川﨑のやりとりと、あと、先ほどの1個前の議論で少しやりとりさせていただいており、やはり今の多様化設備、実設備でつけているものが一体どういう設計になっていて、ほかの安全保護系との関係で、どういう関係になっているのか。取り合いとか、実際の配置とか、いわゆる分離設計とかはどうなっているのかというのは、我々も非常に気にしているところでありまして、その点については、ぜひ次回、より詳細な議論ができればいいなと思っているので、その辺は示していただきたいなというふうに思います。

というのが1点と、あと、すみません、これは私の理解のために聞くんですけれども、23ページで、通しのですね。バックアップ設備の例で、すみません、私の理解は、もともとABWRとかというのを、自主設備としては、基本的に手動操作で期待をしていたんじゃないかなと思っていて、その後、SA設備の要求があって、あとはATWS設備ということで、自動ロジックも追加したというふうに理解をしたんですけど、そういうわけではない。もとから自主設備として持っていて、それをATWS緩和設備としてちょっと設計上強化して登録したという、そういうことになるんですか。

○原子力エネルギー協議会（谷川）　ATENA、谷川です。

もともとATWS設備を自主設備としてつけておりました。それが重大事故設備になって、さっきありましたように耐震性をアップしたりとかということをしたということでございます。

○照井安全審査官　規制庁、照井です。

理解をしました。

○山中委員　そのほか、いかがですか。

○山田総括審議官　規制庁の山田です。

先ほどちょっと川﨑からも指摘があった19ページのデジタル化の範囲のところで、設定値比較回路というのが、ソフトウェアの共通要因故障として考えるべき対象かどうかとい

うのが、多分、先ほどの、どこからどう信号をとっているかというのと絡むと思うんですけれども、この設定値比較回路というものは、多分、つくりようによっては、ロジック演算もして設定値比較もできれば、単純にA/D変換したものをAND/OR回路だけで、それで出力はYES/NOだけにするというのでもつくれると思うんですけども、多分、A/D変換した値をAND/OR回路だけで設定をして、あとは比較する数字だけは入るけどというものだとすると、多分、ソフトウェアの共通要因故障の対象にはならないような設計と言えるかと思うので、設定値比較回路というのはそもそもどんなものですかというのは、次回、ちょっと説明していただいたほうが、今後の議論、やりやすいかなというふうに思います。

それから、もう1点、実際に物がどうなっているのかというのと、これはまだ実際に導入する計画はないというふうに書いておられますけど、27ページのProgrammable Logic Device（PLD）というやつですけれども、これはProgrammableと書いているんですけど、プログラムをするわけですね。ロジックセルを多分つなぎ込むのをProgrammableと呼んでいるんだろうと思うんですけれども、つなぎ込みというやつは、恐らくソフトウェアでどういうふうにつなぎ込むのかというのをやっていくんだとするとすれば、高級言語をコンパイルしたmachine languageみたいな、そういうイメージと同じだと考えるとすると、ここはソフトウェア起因のCommon Cause Failure（CCF）って起き得るものだというふうに考え得ると思うので、今後の議論なのかもしれませんけれども、しそうだとすれば、そこのところは議論をさせていただく必要があるかなというふうに思います。

○原子力エネルギー協議会（谷川）　ATENA、谷川です。

まず、先ほどのデジタル化の範囲に関しましては、この絵はアナログの検出器の信号を取り込んでA/D変換をして、それで設定値を比較してという絵ですけども、おっしゃるとおり、接点で持ってくるものもございますし、そこは少しきちっとわかる形で次回御説明したいと思います。そうであっても、基本的には論理演算回路のところでCCFが発生すれば機能を喪失するというところは変わらないと思いますけれど、きちっと、その辺の違いがわかる形で表示したいと思います。

それと、PLDですけども、御指摘のとおり、まさに上流部分はソフトウェアそのものでありまして、そこに欠陥があるとCCFが発生するということなので、我々もPLDを安全保護回路に導入するときは、当然ながらCCFを想定するということだというふうに認識しております。

○山中委員　そのほか、いかがですか。よろしいでしょうか。

何か事業者のほうから、いかがですか。よろしいですか。

双方から質問、コメントが出たかと思いますけれども、第3回以降で、より明確化をして、お互いに明確化するということで、お答えあるいは要望を出していただくということでよろしいでしょうか。

それでは、本日予定していた議題は以上です。

本日、この後、17時から第2回会合を予定しております。第2回会合では、核物質防護に関する情報を取り扱いますので、セキュリティの観点から非公開で実施をいたします。

それでは、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第1回会合を閉会いたします。