資料２

機能安全を用いた機械等の取扱規制のあり方に関する検討会

第２回議事録

厚生労働省労働基準局安全衛生部安全課

第２回　機能安全を用いた機械等の取扱規制のあり方に関する検討会
議事次第

日　時：平成28年１月25日（月）15:25～17:21

場　所：中央合同庁舎５号館　専用第23会議室

１　開会

２　議題

（１）機能安全を用いた機械等の取扱規制のあり方について

（２）検討にあたっての論点について

（３）その他

３　閉会

○野澤安全課長　本日は、大変お忙しい中、御参集いただきまして、まことにありがとうございます。定刻より５分早いのですが、皆様お集まりですので、ただいまより第２回「機能安全を用いた機械等の取扱規制のあり方に関する検討会」を開催いたします。

初めに、本検討会では会議冒頭の頭撮りに限って写真撮影などすることを認めさせていただきますが、議事進行の妨げとならないよう指定の場所から撮影いただきますよう報道関係者の皆様へ事務局よりお願い申し上げます。

なお、本日は、平尾委員、梅崎委員が所用のため欠席されるとの御連絡をいただいております。

また、安全衛生部長は所用により途中で退席させていただきます。

そして､本日もオブザーバーとして経済産業省の堀補佐に御出席をいただいております。

それでは、本日も議事進行は向殿座長にお願いいたします。よろしくお願いします。

○向殿座長　それでは、今日、円滑な議論ができますように御協力のほどよろしくお願いしたいと思います。

機能安全と機械との関係、その中で規制の話、認証の話、機能安全とはそもそも何か、３つ論点があったはずです。この前は皆さんの御意見をいただきましたので、今日は議論ということになるとかと思います。

それではまず、議事に入る前に事務局から資料の確認をお願いいたします。

○安井副主任中央産業安全専門官　それでは、資料の確認をさせていただきます。

１枚目は次第でございます。

資料１　開催要綱・参集者名簿

資料２　第１回議事録

資料３　危険側故障確率の計算方法

資料４　検討に当たっての論点

資料としては以上でございます。

○向殿座長　資料の過不足はありませんでしょうか。

それでは、議事に入りたいと思います。

まず、事務局側で前回のコメントや論点をまとめてもらっています。論点について説明してもらう際に、前回質問が出た項目についてもその回答を一緒に出していただくという形で進めさせていただきたいと思います。項目数が多いため、幾つかに分けて議論したいと思います。

まず、資料４が論点のペーパーなのですが、項目１と関連した資料３について事務局から説明をお願いしたいと思います。安井さん、よろしくお願いします。

○安井副主任中央産業安全専門官　それでは、47ページの資料４につきまして御説明をさせていただきます。

検討に当たっての論点といたしましては、３つの論点がございます。

まず、第１点の「機械等のリスクに応じた機能安全の安全度水準の設定のあり方」でご

ざいます。

（2）のア、イ、ウとございますが、ウからの下線が引いてあるところが今回修正になったところでございますので、下線の部分だけ説明をさせていただきます。

「ウ　前回検討会での意見等」ということでございます。

機能安全一般につきましては、リスク分析（HAZOPやFMEAなど）を用いて危険な状態を定義し、それを回避できる状態、言ってみれば安全な状態を実現する機能を安全機能要求として定義する。さらにリスクグラフ等によってそれを実現するために要求される安全度水準やパフォーマンスレベルを危険故障確率として決定する。

IEC61508やISO13849では、電気・電子機器の安全関連システムを対象として安全度水準を決定するということでございますが、この安全関連システムは制御システムから独立していなければならないということでございます。

続きまして、危険側故障にはランダムハードウエア故障と系統的故障があって、安全度水準等というのは基本的にランダムハードウエア故障を対象にする。

機能安全の性質として、危険側故障の発生頻度を下げるための機能であり、故障による結果の重篤度を減少させるものではないということでございます。

IEC61508による安全度水準の設定の方法でございます。

まず、低頻度作動要求モードでは機能失敗平均確率というものが設定され、高頻度作業要求・連続モードでは危険側失敗の平均頻度によって定義されて、この２つのモードによって求められる確率が大きく異なり、10の４乗ぐらい違います。

安全度水準につきましては、計算する要素として平均危険側故障確率、これは検知できる故障と検知できない故障がございますが、それと検査インターバル、平均修理時間、共通故障原因、こういったものによって計算されるということでございます。これは後ほど別の資料で説明いたします。

検査インターバルを短くすれば安全度水準のレベルは上がるが、実際に検査できるかどうかについては検証が必要であるということでございます。これにつきましては、前回、福田先生から御説明いただいたISOとIECの比較の中で低頻度モードの計算の仕方がございませんでしたので、それを含めまして、若干復習も兼ねて御説明させていただきます。

資料３をご覧になっていただきたいと思います。43ページでございます。これは、定性的評価で要求安全度水準を決める方法でございます。IEC61508の方法でございますけれども、結果、事故が起きたときの重篤度、Ｆが頻度と繰露時間リスクパラメータ、Ｐが潜在危険回避失敗可能性リスクパラメータ、Ｗが望ましくない事象が発生するかどうかということでございます。こういった望ましくない事象が発生したときに安全機能が発揮されるわけですけれども、ISOの場合はＷというのがないということで、連続モード、常に非常に高い頻度で、あるいは連続で安全機能が求められるのを前提にしているということです。IECにつきましては、例えば機械式安全装置、安全弁のようなものがついているものがあれば求められる頻度が下がりますので、Ｗという概念が入っております。

次のページ、３枚目は、前回御説明したスライドでございますが、表２が低頻度作動要求モードで必要となる失敗尺度、表３が高頻度作動要求または連続モードで運用する失敗尺度ということでございます。見ていただくとわかりますように、同じ安全度水準でも10の４乗ぐらい求められる水準が違うということでございます。これがIECの特徴でございます。

低頻度作動要求モードと申しますのは、作動要求、つまり機械式の安全装置が壊れる確率が１年当たり１回以下の場合ということでございますので、そういった比較的安全性の高い機械について求められるものが低頻度作動要求モードで、高頻度作動要求モードというのはそれ以外のもの、連続モードはずっと連続しているということでございます。ISOの場合は高頻度作動要求モードを前提にしているということで、違いがございます。

それから、危険側故障確率ということで、ここに式が書いてございますけれども、これは御案内の方は御案内ですので、考え方だけ簡単に御説明いたしますと、作動要求当たりの機能失敗平均確率というのは、安全関連システムが機能していない時間を運転時間（機能している時間）で除したものということになっておりますので、時間当たりの平均になっているということでございます。

検知できない危険、例えばその機械が故障しているかどうかわからない場合は検査するまでわからないということでございますので、この検知できない危険側故障が発生していて機能していない時間をどう考えるかと申しますと、検査インターバルの半分の時間は機能しないと考えるということでございます。これが式の中に入っております２分のT_1という概念になっているということでございます。

一方で、検知できる故障が発生した場合は直ちに修理いたしますので、とまっている時間というのは修理時間だけになりますので、その場合は、MTTRと書いてありますけれども、平均修理時間だけがかかる、こういう形でございます。

続きまして、５ページのスライドで、これは一つの例でございますが、回路を多重化すると故障の確率は当然、下がるわけです。そこに複雑な式が書いてあります。PFDを下げる方法としてどれが一番重要か、見ていただくとわかるのですけれども、PFDに占める割合が大きいのは$2\alpha\lambda_{DU}(T_1/2+MTTR)$の部分でございますので、低減効果が大きいのは、設計上の工夫によって共通原因故障、つまり多重化していても同じ原因で故障してしまうと多重化の意味がなくなりますので、その共通原因故障の割合を減らす。あるいは自己診断というやり方を入れることによって検知できない故障確率を減らして、何でも検知できるようにするというやり方、あとは検査インターバルを短くする、この３つの方法をとることによってPFDが下がってくるということでございます。

これが設計上どうするかという議論になってくるわけですが、IECにつきましては、この手法を全面的に設計者に委ねておりまして、基本的に数値計算によって安全度水準を決定する。一方、ISOは、前回、福田先生に御説明いただきましたように、比較的、メニュー方式といいましょうか、あらかじめ定められた選択肢の中から対策を選んで、その組み合

わせでパフォーマンスレベルが決定する。複雑な数値計算はせずに済むという方式でございます。

６ページは別のところに出てきますけれども、機械式安全装置と安全関連システムの関係でございます。これは後ほど御説明いたします。

戻りまして48ページでございます。こういった形でやっておりますが、ISO13849によるパフォーマンスレベルにつきましては、機械設計を前提に、構造要件でありますアーキテクチャーのカテゴリーという概念を用いまして計算方法を簡易化しておりまして、出てきたパフォーマンスレベルは安全度水準の高頻度モデルと互換性があるということでございます。

パフォーマンスレベルにつきましては、平均危険側故障確率（MTTF）、診断範囲（DC）、カテゴリー（アーキテクチャー）、共通原因故障（CCF）、こういった要素の組み合わせで決定されるということでございます。ここまでは勉強したところでございます。

あと、議論になった部分は、機能安全の適用範囲というところでございます。

制御装置の安全性の向上が作業の安全の向上に直接つながる場合とそうでない場合があるので、法令に盛り込む場合には作業の安全の担保を確実に行うべきである。

機械の安全の確保では、機能安全が独立してあるわけではなく、今までずっと培ってきたインターロック、フェールセーフ、ヒューマンファクター、こういったものを含めた総合的な技術としてどう考えるかということが必要です。

既存の設備に対して、信頼性の改善、機能安全というものをどのように活用できるかという検討も必要であるという御指摘があったところでございます。

検討のポイントというところでございます。これにつきましても、前回の御議論を踏まえまして若干直しておりますが、直した部分が下線でございます。

まず、「ア　労働災害防止のための機能安全の適用」というところでございます。機能安全の発現、機能安全が機能することを求められる作動要求状態がどういうものかということでございますが、先ほど御説明いたしました低頻度モード、これは例えばですけれども、機械式安全装置が設置されていて、基本的にそんな高い頻度で安全機能が求められない。高頻度モードにつきましては、機械式安全装置が設置されていないものとか、あるいは構造的になかなか機械式安全装置が設置できないようなものというような形に整理しております。

それから、機能安全が必要とされる安全関連システムでございますけれども、IECなどの考え方では、単純なフェールセーフやインターロックでは対応困難な危険状態というふうに書かれておりますので、そういう意味では、従来のものと連続性があるような形で考えられるということでございます。

そこでどういったものがあるかというのは、ここに書いてございますが、例えば安全関連システムというのはセンサーと論理処理装置と最終出力装置がございますので、それぞれに複雑性がある場合があることを想定しているということでございます。

それから、労働災害防止の観点から、機能安全の対象となる安全関連システムが制御装置に組み込まれる必要がある機械というのは何が考えられるかということでございます。

低頻度モードの適用例といたしましては、爆発等の結果の重篤度が高いような機械は、法令上、機械式の安全装置が義務づけられておりますので、そういったものが考えられ、例としてはボイラーとか圧力容器ということでございます。

高頻度モードの適用例ということでございますが、一定の重篤な結果をもたらすけれども、何十人も一遍に亡くなるようなことはないという機械で、機械式安全装置の装備が比較的難しいようなもの、例えば人間と協働作業中の産業用ロボットみたいなものが適用例として考えられるということでございます。

どちらのモードに分類すべきか不明なものもございまして、これは御議論をいただきたいのですけれども、例えばプレス機械の光線式安全装置のような保護停止のための安全装置、こういったものが低頻度なのか高頻度なのかという議論がございます。

緊急停止のための安全装置もございまして、これも使われるケースは余りない機械ですけれども、どのレベルの信頼性が求められるのかということがございます。

機械等の事故の重篤度をレベル分けする指標、例えばボイラーでありますと圧力によって構造規格の適用条件が厳しくなってきますけれども、そういったレベル分けをするような指標（温度、圧力、積載荷重、速度等）を制御するような機械はどういう分類になるのかということでございます。

「イ　労働災害防止の観点から要求される安全度水準の設定のあり方」でございます。

前回、梅崎さんからも御指摘ございましたけれども、労働災害の許容可能リスクは10のマイナス何乗とか決められるのですかということですけれども、かなり難しいと思いますが、そういった可能性があるかどうか。

定性的評価を行うのであれば、どういった点で行っていくのか。現在のHAZOPのようなやり方がいいのかどうかということでございます。

製造者とユーザーの協働ということでございますが、リスクの分析をするためには、機械が一体どの場所に置かれるのか、例えばボイラーであれば人里離れたところに置かれるのか、病院の中に設置するのかによって事故が起きたときの重篤度が全然違いますので、そういった情報が適切にメーカーに伝わらないといけないということがございます。その辺の協働をどうするのか。あるいは要求される安全度水準の設定について製造者とユーザーのどちらが責任を負うのか。要求水準の設定が適切かどうかについてどこまで専門的な第三者機関の認証が必要なのかという議論がございます。

「ウ　安全関連システムの安全度水準の算定における留意点」ということでございます。

これは先ほど御説明しましたが、検査インターバルに大きく依存しますけれども、例えば連続運転を行っている機械というのはなかなかとめられませんので、１年間連続運転していると１年間検査できない、そういった機械もございます。そういったことも考えないといけないということでございます。

論点の説明は以上でございます。
○向殿座長　どうもありがとうございました。
論点１「機械等のリスクに応じた機能安全の安全度水準の設定のあり方」ということで、この前の御質問に対しても幾つかお答えしているということです。何か御意見、御質問等ありましたら。
低頻度と高頻度というのは単位が違うわけですね。単位時間当たり何回か、どのくらいの確率かというのと、１回押そうと思ったとき動くか動かないかという確率、低頻度と高頻度では単位が違うので比較というのは意外に難しい、状況で違うかもしれないということですね。
○福田委員　そういう意味では、先ほど44ページで10の４乗ぐらい違うという御説明がありましたけれども、上は無次元量、下は時間当たりなので、10の４乗というのは見かけ上そうかもしれませんが、下のほうは単位があるので１年当たりにするとちょうど４乗ずれますから、ぴったり数字は同じになってしまいますね。だから、４乗というのは偶然の話であって、ここでは意味がないことなので、さっきの言い方はもしかすると誤解を招くかもしれないと思います。
では、せっかくマイクがとれたのでちょっとしゃべらせていただきます。これも細かいことなのですけれども、誤解を招くといけないという意味で発言させていただきます。
48ページの上から３行目の「機能安全は、危険側故障の発生頻度を下げるための機能であり」というのは、多分言っていることは機械全体の危険側故障ということを言っているのだろうと思いますが、安全装置が必要ないとき働いたのを安全側故障、安全装置が働かなければいけないのに働かなかったのを危険側故障という言葉遣いのほうが一般的と思います。その２つの比をSFFとかいろいろ言っているわけですけれども、これを書かれたときは、機能安全は機械の危険事象の発生と本当は言いたかったのではないかと私は思って読んでまいりました。ちょっとこれは細かいことかもしれませんけれども、そこら辺、言葉をとり違えて走っていくとおかしなことになるかなと思います。
それから、もう一つ、これはどう定義されているか、いろんな物の本があるから何とも言えないのですけれども、48ページの(３)のアの丸１、次のページの丸２と行くわけですが、「機能安全が必要とされる、安全関連システムの『相反する故障・失敗の潜在危険』」が「ある場面では安全側故障、ある場面では危険側故障となる潜在危険」とあります。これが機能安全を必要とされるところと定義されるというか、機能安全をこう定義されると、例えばライトカーテンという、単純に手が入ったとき、とめるというのは機能安全ではないということになってしまうのかなと思います。実は世の中は混沌としていまして、ISO13849は機能安全ではなくて機械安全というのだとか、あるいは機能安全でないとか、機能安全の単純なものだという方もいれば、いろいろ言葉がごちゃごちゃになっています。例えば化学プラントで、とめたほうがいいときと、とめてはいけないときとある場合、そういうときに出てくるのが機能安全と定義すると、機械というのはとめればいいというふ

うにつくれというのがISO12100の要請ですから、ロジックの話とすれば機能安全ではなくなってしまうので、言葉をきちんとしておいたほうが後々議論がおかしくならないという気がしました。
○向殿座長　いかがですか。今の最後の話は、機能安全はいろんな適用範囲があるから、その中の一つとして、故障すると安全側か危険側かわからない、そういうような場合にも機能安全は使われる、これはそういう読み方でしょう。機能安全が必要とされる云々というのは、それ以外にも当然、機能安全というのは必要なわけです。たくさんあるけれども、特にこの場合、どっち側に壊れるかわからない。どっち側に壊れても安全かわからないというような場合には、それこそ壊れたらいけないから機能安全かという解釈ならば、意味が通る。
○福田委員　そういうことだと思います。
○向殿座長　わかりました。
　ほかに。
○須藤委員　例えばボイラーでいうと低頻度モード、書いてあるのが、例えば安全弁のように普通はめったに働かないという安全装置、もう一つのほうは、先ほどおっしゃられたように、火炎検出器のように、ある場面では火がなくてはいけない、ある場面ではあってはいけない。同じ一つの火炎検出器、センサーは同じなのですけれども、そういう場面が生じる。ボイラーはそういうことになるのです。そういうことと考えてよろしいのですか。
　燃焼中というのは火がなくてはいけないから、例えば失火して火が消えた、それを見張っているのも火炎検出器ですし、着火前のパージ工程のときはここに火があってはいけないわけで、火がないというほうが安全なわけです。そういうことを一つのセンサーでやる。そこのところが今の高頻度モードという意味になるのでしょうか。
○向殿座長　ボイラーの例でいうと、低頻度か高頻度か、多分ずっと見続けていて、故障することによって危険側になってしまう事象が起きるのなら、これは高頻度モードですね。低頻度モードというのは、ふだんはめったに働かないから、働かなくてはいけないときにちゃんと働くかどうか、そういう概念ですね。非常停止ボタンみたいなものでしょうね。今のお話は多分、高頻度だと思いますね。常に見ていなくてはいけない。多分、解釈はいろいろある。
○安井副主任中央産業安全専門官　実は後ろのほうでも出てくるのですけれども、いろいろ御議論いただきたいポイントの一つではございます。例えば49ページから50ページにかけてのところですけれども、プレス機械の光線式安全装置というのは高頻度なのか、低頻度なのかとか、あるいは緊急停止スイッチはどうなのかとか、その辺は決まりがあるわけではないと思いますが、何か考え方みたいなのがある程度あると規制をつくる側としては楽なのですけれどもというのはございます。
○向殿座長　緊急停止ボタンというのはふだん使わないとすると、いざというとき、押したとき動くか動かないかというと低頻度のように見えるけれども、実は常にオンラインで

チェックしているということになっていて、動くか動かないか自己チェックしているということになると、ある意味では高頻度というふうに解釈もできるわけですね。今の話は意外に難しいのかな。福田先生は何か。

○福田委員　ただ、IEC 61508はたしか定義が書いてあって、先ほども安井さんがおっしゃっていた１年間以内か、またはプルーフテストの半分よりも長い間隔でしかデマンドが出ない、作動要求が出ないのをたしか低頻度と定義していた。多分、記憶間違いしていないと思いますが、そうやって定義しているので、このときのテストはプルーフテストだったと思います。例えばプレスのライトカーテンというのはプルーフテストをやるわけではないですね。そうすると、このときはどう考えればいいのですかね。

それともう一つ、結論的に言えば、IEC61508ではなくてISO13849は、自分たちは高頻度だと言い切っていますね。どこかに書いてあった。故障率で考えて、機械の安全装置はISO13849は高頻度と考えるとどこかに書いてあったと思います。そういう意味では、世の中的には高頻度と考えられている。杉田委員、合っていますね。

○杉田委員　今、明確な記憶がないのですが、恐らくそうだったと私も認識しています。

○福田委員　私もそうで､絶対に自信があってしゃべっているわけではないですけれども、たしかそういうことだったと思います。

○向殿座長　要するに、ライトカーテンは、常に見ているから、明らかに高頻度と考えていいのですね。

○杉田委員　マニュアルアクセスするところで出しているのは常に人が介在するので、高頻度ですね。

○向殿座長　介在する。高頻度ですね。いいですか。今のは解釈が合っている。

○安井副主任中央産業安全専門官　保護装置は恐らくそうだと思いますが、人間が積極的にとめる、はっきり言って全ライフサイクルに１回押すかどうかというものもあって、それを例えば高頻度モードのレベルでやれと言われると非常にきついのですけれども。

○向殿座長　非常停止ボタンは低頻度でしょう。回数にもよるのでしょうが、これは直感的に何となくわかるけれども、厳密に細かいところで考えてみるとどっちなのだというのが出てくる。

ほかに、一番詳しそうな池田さん、今の話はどうですか。

○池田委員　確かに使わないですものね。

○向殿座長　使っていないからね。

○池田委員　確かに非常停止ボタンはほとんど使いませんから、押したときに初めて動くか動かないかが証明されますけれども、ただ、非常停止ボタンのシステムによっては常時監視しているのもありますので。

○向殿座長　物による。

○池田委員　そこの定義次第ですね。

○杉田委員　これも設計者の定義でそれをどう持っていくかによりけりではないでしょう

か。それでするしかないと思います。
○向殿座長　ほかに御質問はございませんでしょうか。
○安井副主任中央産業安全専門官　強いて１つだけ確認させていただくと、例えばボイラーの安全弁のように、もともと安全弁が機能すること自体が全ライフサイクルに何回あるかということで、しかも安全弁が故障していることを前提にしますので、ああいう機械式の安全装置がついていれば低頻度というのは大丈夫ということですか。
○向殿座長　どうぞ、石田委員。
○石田委員　安全弁も考え方によって変わってくるのです。通常使用状態で安全弁が働くということは、安全要求、デマンドのときかどうかはわからないのです。設計上、通常使用状態の範疇に入れてもいい場合があります。本当に安全弁が働かないといけないのに働いていないというのを監視する場合に機能安全という考え方が必要になってくるのではないかという気はしています。これは結構、議論しているところなのですが、そこはメーカーさんあるいはユーザーさんというか、事業者さんの考え方だと思っています。
○安井副主任中央産業安全専門官　逆に言えば、ボイラーの安全装置というのは事故があったときしか使わない機械なので、ふだん吹いたら困りますから、そういう機械については低頻度と言えるということですね。わかりました。
○向殿座長　普通の意味では確かに低頻度。
○須藤委員　ボイラーの場合は、安全弁が吹く前に圧力過昇にならないように、圧力スイッチですとか電気的に燃焼を遮断する装置はどんなボイラーでもついているわけで、それも効かなくなったときに初めて機能するのが安全弁となると、安全弁が働くようなことが年中あってはいけないということなのです。そういう意味では、制御装置のほうが安全装置の機能の一部を兼ねているのが現在のボイラーの制御装置であると思います。
　先ほどの緊急停止ボタンというのも、例えばプログラマブルコントローラーを介してそのボタンを押したことによる機能を動かそうとすれば、プログラマブルコントローラーから見ていれば､常にそのポートに緊急ボタンの信号が入ってくるか見張っているわけです。そういうふうに捉えると低頻度なのか､制御側から見るとどうなのかなと思ったりします。
○池田委員　安全弁にしろ、非常停止ボタンにしろ、それが安全関連システムの制御要素の一部なのか外なのかというところでまた変わってきますので、悩ましい話です。
○向殿座長　これは考えると相当悩ましい話になりますね。
○池田委員　今、須藤さんがおっしゃったように、非常停止ボタンを二重系にして、一方は強制的に溶着しないような構造にする。もう一方の回路はプログラマブルの装置に入れてチェックする。この場合、このデバイスは安全関連システムとみなすのかというのはよく議論があります。
○向殿座長　これは設計側の考え方というのもあるし、今の安全弁でも、よく考えてみるとめったに吹かないから低頻度だというけれども、それをコンピューターで常にコントロールして上がりそうなところを下げている、この機能は連続ですね。連続のところと低頻

度が一緒になっている。今度は安全弁も電子装置を入れておいて、いざというときに吹くか吹かないかをオンラインで常にチェックしている、常に監視しているということになると、その監視機構は実は連続モードになるという話、そういうことですね。
○安井副主任中央産業安全専門官　そうです。池田委員の御指摘があったように、安全関連システムかどうかというところが非常に大きいとは思いますけれども、機械式の安全弁というのは、完全に機械式、例えばばねが入っているようなものについて安全関連システムと普通言わないと思いますので、いわゆる電子制御ではありませんので、そういったものが前置されていれば電子制御の機能安全に係る負担が軽くなるということだろうと思います。そこは機械式かどうかというのが非常に大きな部分であろうと思います。
○向殿座長　ありがとうございました。いろいろ議論があります。
　ほかに御質問、御意見、どうぞ、お願いします。
○杉田委員　さっきの続きですけれども、ここで機械とボイラーをどう分けるかなのですね。ボイラーは今まで安全弁が第一の安全デバイスとして入っていますので、温度リミッターや圧力リミッターというのも入っているのですけれども、機能的に違うものがあるので、基本的にボイラーでは機械式の安全弁しか最終の安全装置と認めていないということです。例えば機能安全云々の何かの規定を割り当てれば安全弁に電子制御を入れることができるのか、そういうことを今まで誰もされていませんけれども、世の中で誰にも認められていませんけれども、そういうことは可能になるのか、そういうことを考えるメーカーもなきにしもあらずと思います。
　須藤さんが考えているような大きな発電用ボイラーだったり温水用ボイラーと違って、小さい煮沸器のようなもの､ボイラーではないけれども､小さいオートクレーブがあって、それは今、安全弁がついています。小さいものになると反対に安全弁がなくて、通常は圧力リミッターとか温度リミッターでモニターしているのですけれども、結局それがなかなか安全を担保できないという問題があると思います。小さいものになればなるほど安全弁が大き過ぎて使えないというのがあります。ここで言っているボイラーというのはかなり大きなものですけれども、小さい圧力容器を考えると割と小さくても高圧になるものがあって、なかなかそれに見合う安全弁がない。
○向殿座長　安全弁が大き過ぎて。
○杉田委員　大き過ぎてないのです。発電用ボイラーの安全弁を使わないとだめで、そうするとその安全弁のほうが製品より高くなってしまうというのでなかなかつくれないということもあります。ここでもしこういうことを考えたらそういうことは可能になるのでしょうかということです。
○向殿座長　今のはある意味ではおもしろい。コンピューターでコントロールしながら安全弁を。
○安井副主任中央産業安全専門官　御指摘につきましては、次の論点で出てくると思いますので、そこで御議論させていただきたいと思います。

○向殿座長　よろしいですか。
○安井副主任中央産業安全専門官　安全度水準の設定のあり方で、製造者とユーザーの協働というところがありまして、例えばユーザーから十分に情報が来ないとHAZOPとかFMEAできないのですけれども、こういう仕組みというのは日本では余りないと思います。こういうところについて何か御意見があればいただきたいのです。
○向殿座長　お願いします。
○石田委員　我々は、厚労省さんから出していただいている機械の包括安全基準を事業者さんと製造者さんに適用してもらって、コミュニケーションを密にしてもらおうということでアドバイスさせてもらっています。あの機械の包括安全基準というのはすごくいい指針だと思いますので、それを我々は使わせていただいているということです。
○向殿座長　あれはユーザーとメーカーと両方にリスクアセスメントを要求しています。あるメーカーに言わせると、ユーザーに情報をくれというと、いや、これはノウハウだから出さないとかいうのがあって、実は協調できないというようなことを言われたことがあります。でも、基本的にやはり両方で協調してやるべき問題ですね。
○石田委員　そうですね。
○向殿座長　ほかにございませんでしょうか。
○安井副主任中央産業安全専門官　現実問題として、製品を設計する段階でユーザーがどこに設置するかというのを決めてもらわないと困るのですが、そういうのは日本の製造現場では余りないような気がするのですけれども、そういった点はどうですか。
○石田委員　ほとんどないと言っていいと思います。それで製造者さん側がすごく困っていて、ありとあらゆるパターンを考えて、例えばSILの幾つというのを決めていかないといけない、今そういう状況に陥っているので、製造者さん側にすごく負荷がかかっていて、開発期間が長くなったり費用がかかったり、そういう状況はあります。
　労働安全衛生法の基本は、事業者さんに対して責任がありますよとうたっていますので、我々としては、やはり事業者さんに音頭をとってもらって製造者さんにどんどん情報を出していただければありがたいという気はしています。
○向殿座長　この問題はかなり難しい問題で、メーカー側はどう使われるかわからないからリスクアセスメントをある限った条件しかできないということになる。使い方によってはいろんなリスクが出てくる。ユーザー側と一緒にならない限りメーカー側は指摘もできないし、SILも計算できないことになるという話ですね。
○石田委員　プルーフテストも、20年に１回という事業者さんもいるし、朝と昼に２回やるというような事業者さんもいるので、製造者として設計する負荷が全然変わってきます。やはり事業者さんが情報を出していただくというのはすごくありがたいという気はしています。
○須藤委員　ボイラーの場合は、ボイラー及び圧力容器安全規則ということで、唯一、低水位検出器の作動確認というのがボイラー技士に課せられまして、実際に動かして、働く

かどうかというのを１日１回やれ、それは書いてあるのですけれども、ほかは細かくは余りないですね。
○向殿座長　どうもありがとうございました。今、言ったような課題はあるということですね。ほかに。
○福田委員　理屈だけで言えば、大学にいるので現実がわかっていないと言われればそれまでですけれども、例えば量産品だったら一個一個お客さんに聞いてつくれないから、この機械は屋内の平らなところに置いてとかと始まって、いろいろやっていって、その条件で多分リスクアセスメントをやって、その結果として、１年に１回、半年に１回、１カ月に１回調べてくださいとか書いてあるわけですね。一品物であれば、多分、お客さんとやりとりができて、そこで仕様を決めていくのではないのかなと思います。
　私の家はガスファンヒーターを今、使っているのですが、２週間に１回、後ろのフィルターを掃除してくださいと書いてあります。私が買ったガスファンヒーターを設計した会社は、普通の家の使用状況を想定してやっている。その結果として出てくる。直接やりとりできなくても、制限仕様とか機械の仕様とか決めて、その前提でやる。だからこそ逆に、それをきちんと伝えなければいけないというところでISO12100は考えているのではないか、私はそう理解していますけれども、いかがでしょう。
○向殿座長　今の話は量産品と一品物では当然違うということで、ISO12100はどっちかというと量産品のことも相当考えて書いてあることは事実ですね。どうですか。
○石田委員　おっしゃるとおりです。ただ、製造者側のほうは常に競争しているのです。例えばユーザーさんがある一点を捉えて「Ａ社さんはこうですよ。御社はどうなのですか」と聞かれたときに、すごく製造者側は無理するのです。そこは、私、見ていてすごく苦しいところです。一点だけ捉えて、ここを何とかしなさいというユーザーさん側の指示というのはすごくつらいと思います。
○福田委員　だからこそ厚生労働省さんも、生産技術者も15時間ぐらい勉強してきちんとそれを知りなさい、こう言っているわけかなと思います。結局、どこまで議論するかというのは、これを考えると話が発散してしまう。ただ、理屈から言うと、私が言ったことは間違っていなかったはずです。どこまで現実的な議論をするかというのは、むしろ安全課さんに聞いてみないとよくわからない。ただ、私たちは、理屈は理屈でどうだと、それは現実とどうずれているかという形で議論しておかないと、現実と教科書的な話とごちゃごちゃにして議論すると、話はごちゃごちゃのまま終わってしまうような気もします。
○向殿座長　ありがとうございました。
　今の話の中で、やはりインテグレーターというか、両方を知っていて、中間に入ってやる安全技術者がかなり必要だというところにつながる。
　ほかにございませんでしょうか。
　よろしいですか。いろいろ論点があって御質問が出ましたが、安井さん、いいですか。いろいろ意見があって、また参考にしていただければと思います。

さて、論点１は終わって、論点２のほうに行きましょう。論点２は「機能安全の安全度水準を満たす機械等の取扱いに関する規制のあり方」ということです。これも安井さんのほうで御説明ください。

○安井副主任中央産業安全専門官　それでは、51ページから御説明いたします。「機能安全の安全度水準を満たす機械等の取扱いに関する規制のあり方」ということでございます。

概要と国際規格・法令等は変わっておりませんので、省略いたします。

前回の議論ということでございます。ボイラーと産業用ロボットについて議論がありました。

まず、ボイラーにつきましては、欧州では、EU指令（圧力容器指令、機械指令等）に整合する規格（ISO、IEC、あるいは欧州独自の規格であるEN）に適合しない機械等は市場に流通できないという制度になっております。また、その適合性の評価は、機械等の危険性に応じて自己宣言から第三者認証まで分かれているということでございます。

ボイラーの安全関連システムについてはEN50156という規格がございまして、これに適合するわけですけれども、この中にはIEC61508で定める要求安全度水準を満たすのか、あるいは個別製品規格(Ｃ規格)に適合することが求められているということでございます。

安全関連システムにつきましては、制御システムから独立するとともに、機械式の安全装置に加えて設置する必要がございます。

これにつきましては、資料３に戻っていただきますが、45ページの「機械式安全装置と安全関連システムの関係」でございます。これはEN12953というボイラーの規格でございます。これを見ていただくとわかりますように、セーフティー・アクセサリーの中に、セーフティーバルブ、これは機械式の安全弁、バースティングディスクというのは破裂板、これとリミッティングデバイスという、リミッターということになっていますけれども、これがセンサーとロジックとアクチュエーターという、まさに安全関連システムがあるということです。こういった安全関連システムをつけたからセーフティーバルブをつけなくていいという形になっていなくて、並列の関係にあるということでございます。

51ページに戻っていただき、③でございます。英国の例では合理的に実施可能な措置の判断基準としてのガイドラインが定められていて、ボイラーの安全関連システムの安全度水準が高くなるにつれて点検の頻度や資格者の配置が緩和される仕組みをとっているということでございます。

産業用ロボットでございますが、これは製品規格としてISO10218、上位規格としてISO12100、ISO13849-1というものに準拠しているわけでございます。

制御システムの安全関連部というのは主に停止するための回路であって、安全性能を維持できなくなったときに機能する保護装置、これはインターロックのようなもの、それから人間が危険を察知したときにスイッチを押す非常停止の２種類があります。

位置の監視については、従来は機械式のストッパーのみであったけれども、電気・電子制御による監視と保護停止が認められつつあります。

安全関連システムについてはISO13849-1というのがございますが、ここではカテゴリー３という構造要件が定められた上で、パフォーマンスレベルであるｄを満たすか、IEC61508で規定する検査インターバルが20年以上という条件のもとで、ハードウエアフォールトトレランス、これは冗長性ですけれども、冗長性が１の安全度水準２に適合するように設計するということで、安全度水準のみならず構造要件を規定しております。

安全度水準を満たす安全関連システムを安全適合といいますけれども、これは産業用ロボットについては基本的に自己認証であります。

人間とロボットの協働作業の条件として、位置、速度、力の３要素の監視と、異常時の保護停止に関する安全関連システムが求められているということでございます。こういったものを満たせば、逆に言うと協働ができるということでございます。

その後は御意見でございますけれども、機能安全の労働災害防止対策への活用方策ということでございます。

労働災害防止について、我が国として災害の許容リスクを定量的に定める、つまり死亡災害リスクが10のマイナス何乗でなければいけないと定めるのは難しいということなので、定性的な方法で、結果の重篤度と発生頻度の組み合わせでリスクを定めるというやり方が行われています。

機能安全は、故障確率を低減させるもので、先ほど御指摘がございましたけれども、事故の確率を低減させるものであって、重篤度を低減できないので、対象とする機械によっては安全関連システムの故障確率を減少させてもリスクは下がらないかもしれない。そういう意味では、機能安全によるリスク低減効果は総合的な判断が必要です。

リスクを下げるためには、本質安全化や、重篤度を下げる方策を含む機械式の安全装置などを優先すべきであって、制御機能によるリスク低減措置は最後の手段とすべきである。

一方で、ロボットと人の協働のように、本質安全化や機械式の安全装置ではリスクを低減しにくいものについては機能安全によらざるを得ないという議論もございました。

機能安全は設計段階から導入すべきであって、ユーザーが後からつけるようなものではないという御指摘もありました。

安全装置の信頼性が上がったから安全装置の点検間隔を広げるためには、設計段階での点検間隔、これはプルーフテスト間隔ですが、それを指定して安全度水準が定められるので、それと矛盾しないようにしなければいけない。

よい安全装置がついたから機械の故障を容認できる、つまりブレーキが高性能になったからアクセルペダルの戻りが多少悪くなってもいいということではありません。

点検頻度の緩和は、代替機能、例えば遠隔操作が入ったから、従来、人が担っていた関与を減らせるということではないかという御指摘も寄せられております。

検討のポイントにつきましては、前回のものからは全面的に書き直しております。いろんなケースごとに御議論いただきたいということで、アからカまでケース分けしております。

まず、アでございます。事故の結果の重篤度の大きな機械、これはボイラーなどですけれども、爆発してしまえば周りの人を全部巻き込んでしまうような危険な機械につきましては、従来から機械式の安全装置、まさに安全弁などが義務づけられておりまして、先ほどちょっと議論がございましたが、基本的には低頻度モードでの安全関連システムというところで仮に要求安全度水準を満たしたとしても、機械式安全装置の省略は認められておりません。

これの考え方としては、重篤度が大きいということになりますと、故障確率が下がっても、いわゆるリスクが下がらないというような考え方なのか、あるいは重篤度が非常に高いので、機械式の安全装置と電子的な安全関連システムの多重化により頻度を徹底して低減するという趣旨なのか、どちらなのかという議論がございます。

あるいは、安全関連システムが、機械式安全装置がないと仮定した上で非常に高い高頻度モードの要求安全度水準を満たせば、機械式安全装置の省略を認めることができるのかという議論もございます。

ただ、こういったものにつきましては、事故の重篤度が大きい機械は内包エネルギーが大きいため、基本的に連続運転ということもありますので、検査インターバルを小さくすることが難しいことはございます。ただし、自己診断の機能などを入れることによって危険側故障確率を下げることは可能かもしれないということでございます。これは、原子力発電所に機械式安全弁は要らないのかという議論にもつながる話ですけれども、どこまでできるのかというところは議論があるところでございます。

イでございますが、事故の結果の重篤度が相対的に低い機械、もちろん事故が起きれば挟まれ巻き込まれて、けがをしたりする可能性はありますけれども、少なくとも何十人が一遍に亡くなるようなことはないような機械、例えば産業用ロボットというものにつきましては、従来の機械式の安全装置、例えば囲いやストッパーというものを電気・電子制御の安全関連システム、監視であるとか保護停止によって代替することが規格上、徐々に認められつつあります。ただ、この場合であっても、単なる要求安全度水準、つまり確率だけではなくて、構造要件（自己診断（アーキテクチャー））や冗長性の指定、そういったものを要件として課すべきなのかどうかという議論がございます。

機械式の安全装置を電気・電子式には徐々に代替していくような流れにありますけれども、そういうことが認められる基準として、事故の結果の重篤度が低いかどうか以外に何か考えられるものがあるかどうかというところでございます。

ウですが、低頻度モードの機械、言ってみればボイラーのような安全弁がついているようなものについても、電気・電子式の安全関連システムの安全度水準の高さに応じて、点検頻度や監視体制の緩和がイギリスなどでは認められておりますので、そういったものを考えることは可能なのかどうかということでございます。この場合は、PFDの計算の前提としての検査インターバルの関係が出てくるということがございます。また、ここでも単に確率だけではなくて構造要件を課すのかどうかという議論がございます。

エの保護停止装置や緊急停止装置につきましては、一定の頻度で点検が義務づけられているものがございます。この点検頻度について、要求安全度水準を満たした場合、最適化する余地があるかということでございますが、具体的には、例えば動力プレス、コンベヤーといった事故によって一定の後遺障害をもたらすような機械につきましては、安全装置や非常停止装置が義務づけられた上で、作業開始前点検や１年に１回の自主検査が義務づけられております。一方、産業用ロボットあるいは人力車といったものにつきましては、非常停止装置の設置が義務づけられていますが、点検の意味がないような機械もございます。こういったものについてどういった形で点検頻度を考えていくのかという議論がございます。

オは、機械等の規制のレベル分けや適用除外を行う指標ということでございます。例えばボイラーであれば、伝熱面積が大きくなればなるほど構造規格上の要件が厳しくなっていきます。簡易ボイラーから小型ボイラー、正式なボイラー、そういったものがございます。あるいはクレーンとかゴンドラなども同じなのですけれども、こういった適用除外を行う指標ということで、温度、圧力、速度、積載荷重等の制限については、従来、機械的に担保しているケースが多い。例えばボイラーは伝熱面積ですから、これは発熱するエネルギーと熱媒の伝わる面積を規定しておりますので、かなり物理学的に制限があります。それから、無圧ボイラーの場合は大気に開放していますので、絶対に１気圧以上は上がらない。そういった形をやっている一方、一部、電子制御によるものを認めるケースもございまして、例えば第一種圧力容器の適用除外に加熱蒸気遮断機を設ければ圧力容器ではないとか、そういったものがあったり、ボイラー技士資格のレベル分けをするときに、自動制御ボイラーのときの伝熱面積の算入の特例を認めるとか、そういった一部、制御の考え方が入っているものもございます。

こういったことで、事故の重篤度が高い機械でも、規制のレベル分けや適用除外の指標に関しては、事故との関連性が低い場合には機能安全を前提とした電気・電子制御を入れる余地があるのではないかということでございます。

最後は、カの遠隔操作でございます。一定の自動制御の機能を有する場合には遠隔操作を認めているものがございます。例えば自動制御ボイラーの事業場内監視装置、そういったものがあるのですけれども、これで点検の頻度の緩和を認めていないということでございます。遠隔操作につきましては、操作される側の信頼性に加えて、通信の機能安全という議論が出てきますので、これについては機器本体の機能安全とは切り離して議論すべきではないかということでございます。

論点の説明は以上でございます。

○向殿座長　どうもありがとうございました。

では、論点２の件で何か御質問、御意見ございましたら、お願いします。

○福田委員　例によって細かいことで申しわけありませんが、やはり言葉をちょっと丁寧にということもあって、52ページの下のほうの②の「機能安全は、故障確率を低減させる

もので、重篤度を低減できないため」というのは私が例を出して話をしたところですけれども、次の行に「リスクは下がらないかもしれない」とあります。これはちょっと違って、危害の大きさは下がらないかもしれないですけれども、確率が下がりますから、リスクはやはり下がります。リスクは発生確率掛ける危害の大きさですから。これは多分「減少しても危害の大きさは下がらないかもしれない」というのが正しい文章だと思います。リスクは下がらないと言ったら、これは定義からして違っていると思います。

それから、これは私の意見なのですが、53ページの(３)のアの①の「重篤度」云々、機械式とか電子式とか、両方求めているのは化学プラントでもIEC61511でもそうですし、そもそも化学プラントは多重防護しなさいとか、いろいろ書いてあって、要は内側と外側、さらにその外があって、みんな違うことを考えて防護してくださいと言っているのです。

機械式安全弁は、ばねで押さえているから、力が加わればばねの力が勝つということです。ねばねばしたようなものが入っているタンクの安全弁だと規定圧よりもちょっと先にいかないと開かないことも現実的にはあると聞いています。でも、とにかく、あるところまでいけば絶対開く。それよりはタンクが丈夫であればいい。ところが、機能安全は、センサーが壊れたら幾ら温度が上がっていっても圧力が上がっていっても絶対に開かないのです。弁を開放しない。その違いがあります。

そういう仕組みの違うものを、冗長なのだけれども、異種のものでやっているところに深層防護や多重防護の考え方があるので、化学プラントにしろ、ボイラーにしろ、信頼性が片一方上がったからという、将来は究極に信頼性の高い安全装置ができるかもしれませんけれども、少なくとも今は違う種類のというところが一つの力点ではないか、そういうふうに私は理解しています。

○向殿座長　ありがとうございます。多重というのはダイバーシティーですね。違った機能による多重系、二重系、三重系ということも重要だという話ですね。

さっきのリスクは下がらないというのは、確かにリスクというのはひどさと頻度の組み合わせだから、頻度が下がればリスクも下がると考える。ひどさは下がらない。

○安井副主任中央産業安全専門官　53ページのアの①に書いてありますように、おっしゃるように「十分に下がらない」というところだろうと思います。

○福田委員　「十分に」というのが抜けていたのですね。了解しました。

○向殿座長　ほかにございませんでしょうか。

○池田委員　福田先生の話の続きになりますが、53ページのアのところです。機械式の安全装置というものが電気・電子機器に置きかわってきているという話は、もともとは機械的なストッパーとか、あらかじめ設計で決めたら後から動かせない、融通がきかなくて実際に使いづらい、でも最後はがっちりとめてくれるので安心して使っていたのだけれども、最近、制御のほうがプログラマブルでいろいろできるようになってくると、機械的な安全弁もそうですが、ある一定のところでしか機能しないのだとちょっと使いづらいというところで、ではそこを電気・電子ソフトウエアで置きかえられないかとなってきたというの

がそもそもの経緯です。出てきた目的がちょっと違っています。
○向殿座長　わかりました。必ず古いものを残してと言っているわけではないということですね。
○安井副主任中央産業安全専門官　池田さんのお話ですが、産業用ロボットなどの場合、そういうのが認められているのは、逆に言うと、制御装置がうまくいかなくてもそれほど大きな災害にならないという前提はあるのでしょうか。
○池田委員　いや、誰もそんなことを言っていないと思います。さっきの話もちょっと関連しますが、産ロボの場合はロボットのキャパシティーというか、能力によって安全の機能を変えるというのがないのです。基本的に小さいロボットでも大きなロボットでも、製品規格のほうは安全機能は同じというのが原則になっています。
○向殿座長　エネルギーの大きさは余り関係ないのですか。
○池田委員　評価はしますけれども、規格のデフォルトというか、標準は同じです。
○向殿座長　ほかに御質問、御意見ございましたら、どうぞ。
○池田委員　一番最後の遠隔操作の話ですが、ロボットやクレーンとかも遠隔で操縦したり遠隔のモニタリングというのが出てきているのですが、そこの無線のコントロールを安全関連システムと呼ぶかどうかで議論が大きく変わってきます。単にボイラーの状態をただ見ているだけで何もしないというのと、その情報を飛ばして処理して、また制御に戻すというのと、そこにまた人が介在して制御に入るとか、いろいろモードが違うと思うので、遠隔というのを一くくりに議論はできないと思います。
○向殿座長　遠隔だけでは簡単に片がつかない。
○須藤委員　昔はボイラーの遠隔制御とか遠隔監視といいますと、例えば水面計でボイラーの水位を見ているときに、工業用テレビを使いまして、テレビカメラで水面計を写しているわけです。その信号をそのまま中央監視室へ持ってきてブラウン管で見ているというのから始まって、差圧発信器という、圧力を発信する、アナログ信号を出す機械があって、そのアナログ信号の電流値をそのまま電線で引っ張ってきて、制御用の電線ですが、それを表示器の、例えば指示器というのがありまして、針がついているわけですが、そういう時代がありました。
　最近は、そこのところが電線ではなくなりまして、イーサネットや、そういった通信回線を使うようになりました。ボイラーのところにはいろんなセンサーがついているわけですが、それを一旦、プログラマブルコントローラーへデータとして取り込みます。そこと中央監視室というのは、いわゆるバスという通信回線だけで結ばれています。その通信回線の信頼性というのは余り問われていないのです。すごく重要なスペースシャトルか何か、ああいうものは専用のバスを使うのでしょうが、場合によっては今のインターネットのような考え方で、しかもモニタリングだけでなくて緊急停止ボタンを遠隔監視室で押すわけです。それも実は通信で向こうに飛んでいく。制御器メーカーはそこのところも含めて、我が社は安全ですと。それぞれのメーカーがそれぞれ固有のバスを使ってそういうものを

構築しているのですが、確かにそこのところの信頼性というのはメーカー任せで、例えば遠隔監視の基準というのがボイラーの安全規則にもありますけれども、そんなことは全然書いていないですね。とまればいいというか、あるいは見られればいいまでですね。

○向殿座長　ある意味、通信の信頼性は意外に難しくて、とめろといったってとまらないことがいっぱいあるし、オンラインで見ていると途中、雑音が入って聞こえないとか、もっとひどいのは、セキュリティーの問題があって、変なやつが入ってきて爆発させたとか、あり得るわけです。そうするとセーフティーだけでなく、セキュリティーの問題も実は入ってくるという感じはしますね。遠隔だから、そこに人がいないから、少しぐらい危なくてもいいというのはないのですか。人がいなければ誰もけがをしないからという、隔離と同じだというのはないですか。それもあり得るのではないかな。

○安井副主任中央産業安全専門官　まさに池田さんが御指摘いただいて、須藤さんも指摘されていますけれども、単なるモニタリングなのか、それをPLCに戻して制御として使っているのかというところで求められる信頼性は多分違うのだろうと思います。

現在の遠隔操作についてはモニタリング以上のことは想定してつくっていませんので、そういう意味では、今後の課題ではあろうと思います。現時点ではいろんな通達とかございますけれども、遠隔監視で制御するところまで踏み込んでいるものは今のところないので、遠隔制御を認めるということであれば、先ほどのまさに通信の問題は出てくるのではないかと思います。

○向殿座長　製品安全で空調を遠隔で操作するというのがあって、その場合、オフにするのは認める。オンにするのは認めないというのがあります。

○須藤委員　ボイラーの遠隔監視基準は、起動停止は、今の通達ですと遠隔監視場所でやっていいことになっています。実際に遠隔監視ボイラーの設計をやるときに、水位、圧力、温度というデータは通信で持っていくけれども、起動停止だけは実配線で持っていくとか、いろいろ考え方によってユーザーさんもメーカーもその辺ちょっと難しいところなのです。

○向殿座長　当然、起動オーケーは遠隔で認めないわけね。

○須藤委員　今は遠隔で起動は認めています。こちらの平成15年に出ているのを見ていますと、起動装置はボイラーの設置場所または遠隔監視場所、緊急停止装置は遠隔監視場所に必ずつけるということがこちらの通達には載っています。そういう意味では、普通、全部、通信回線に返していいのというのは議論になるところです。

○安井副主任中央産業安全専門官　ボイラーの場合、２種類ございまして、一つの事業場の中に遠隔装置室がある。言ってみれば原子炉の中央操作室みたいなイメージなものと、事業場外から遠隔監視するもの、２種類に分かれております。遠隔監視についてはそういう操作は一切認めておりませんで、認めているのは、いわゆる事業場内の中央操作室みたいなものですね。例えば原子炉など運転できませんので、そういったものはもちろん認めてはいます。そこはちょっとまた違う議論ではございます。

○向殿座長　ありがとうございました。

ほかに御質問、御意見等ありましたら、どうぞ。
○須藤委員　あともう一つ、ボイラーの場合、今、議論されているのは、安全弁がばね式の機械式ということで考えて、機械式の安全装置となっているのですが、例えば低水位遮断機は、ポンプの調子が悪くなってどんどん水位が下がっていくときに燃焼をとめなければいけないわけですね。燃焼をとめるにはどういう回路になっているかというと、簡単にいうと、フロートという浮いているものがあって、それがだんだん下がっていくとスイッチが切れるわけです。スイッチの切れた電気信号でそれをコントローラーのほうに渡して、燃焼するためには燃料の遮断弁をあけているわけですが、遮断弁はあけた状態で、燃料の調節するのは調節弁というのがあって、かげんしているのですが、その遮断弁を閉めるという動作でもって緊急停止ができるわけですが、既にその中にそういった制御機能が入っています。
もう一つは、運転しているボイラーが何かのことで失火した、消えたというときに、火炎検出器がそれを検出して、火が消えたという信号をやはりコントローラーへ持っていって、そこからアクチュエーター、通常、遮断弁というのは電気空気式だったりするのですが、結局、電気信号に変えてバルブを閉めて燃料が生で吹き出すのをとめるということでいうと、ボイラーというのは、安全弁以外はそういうものが既に介在しているわけです。
○向殿座長　かなり入っていますね。機械安全のポジティブモードでいうと、下がったらひもが出て、ひもで引っ張らないといけないとか、そういう話に多分なるのでしょうが、電気信号に変えて制御している。現実はそうでしょうね。ほかに。
○安井副主任中央産業安全専門官　ボイラーの話になりましたので、欧州の考え方などを御説明しますと、欧州の場合は、通常の制御装置と安全関連システムを分け、独立されていて、その場合は、先ほど言ったような安全要求を満たす機能があるかどうかについて十分に設計上検討した上で、安全度水準を満たすことを担保するということが規格上求められていますが、日本の場合は、恐らく独立していなくて、通常の制御装置でやっているケースがほとんどだろうと思いますので、そういう意味では、今回議論しているような機能安全の定義には当たらないものが多いのではないかと思います。
○向殿座長　ほかに、どうぞ、石田委員。
○石田委員　54ページの「オ　機械等の規制のレベル分けや適用除外を行う指標」というところで、例えば温度ということが書かれています。我々が製品を評価する場合、必ず温度上昇試験が入ってきます。最近、欧州の認証機関の試験の例を見ると、温度のところで例えば100度というのが要求事項であるとすると、例えばSIL2の温度制御器でコントロールするということを条件にして温度試験はしないというのが結構あります。製品の評価をする中で、一つの試験も、ある意味、規制緩和されているという状況が散見されるわけです。
もしこれが入ってくると設計のほうもすごく楽になります。今は構造要件で温度を上げないという構造にする設計なのですが、設計者のほうもSIL2の温度制御ですればそれでいいのだということで、ある程度トライ・アンド・エラーの実験をしながら製品をつくり込

んでいくという作業をしなくてもよくなってくる。それをやり始めると製品開発の期間も短くなる。評価の期間も短くなるということで、例えば商品そのものを規制緩和するというのではなくて、試験の中でも緩和してもらえると、メーカー側、評価する側もすごく楽になるのではないかと思っています。
○向殿座長　SILの高いのを使うと規制から見るとテストをやらなくていいということになる、そういうことで非常にありがたいという議論と、それで大丈夫なのかというのがもう一方であるわけです。どうぞ。
○杉田委員　要は、ボイラーでも圧力容器でも構造要件が非常に厳しい。SIL2、SIL3の制御装置がつけば今までの構造要件を緩和できるとか、厚み等があったり、溶接条件だったりができるのか。そうすると製造者に対しては非常にメリットがありますね。そうではなくて今の構造要件にSIL3の制御装置をつけなさいとなると、さらに安全になっていいのですが、メーカーさんはしんどいのかなという気がします。
○向殿座長　どうもありがとうございます。
　ほかにございませんでしょうか。
○安井副主任中央産業安全専門官　今の議論ですけれども、先ほど福田先生がおっしゃったように、事故が起きたときの多重化という議論がありますので、制御だけでかわせるかどうかという議論があると思います。先ほど温度制御もありましたが、温度制御がクリティカルに事故に直結するということであると機能安全だけでは認められないのでしょうが、必ずしもそうでもないような場合だったら認められるとか、そういったものがある可能性はあるのではないかと思っていまして、そういう観点で何か助言などがあればいただければと思います。
○向殿座長　機能安全というのは、確かに確率、信頼性でやっているけれども、ある想定があって、想定内での確率であって、想定外のことが起きるとやはり物理的な構造で安全を担保するというのはあり得ます。エレベーターなどはまさしくそうでして、どうしようもないときは物理的にくさび型でとめるとか、ああいうのが最後に入っています。機能安全、ハザードは何かとずっとリストアップして、その中でちゃんと考えているけれども、それ以外のことが起こり得るとすると最後の最後は機械を物理的にとめるのだというのを置くべきだという意見は安全屋さんは持っていますね。
○安井副主任中央産業安全専門官　例えばですけれども、温度と圧力というのは一定の関係があるわけで、例えば圧力について機械式安全装置が入っていれば温度については機能安全でいいですとか、どこかに何がしか多重系があれば、冗長的なセンサーについては例えば電子式のものも入れていいとか、まさに安全設計だと思いますが、そういうのはいかがでしょうか。
○須藤委員　今の安全規則はそういう意味ではすごく厳しくて、先ほどの温度制御という話ですが、例えば真空式の温水機というのがありまして、これは大気圧以上にならないということでつくられています。いつもは温度センサーでバーナーのコントロールをしてい

て、真空の状態で90度ぐらいのお湯をつくる機械です。真空といっても大気圧にかなり近いところの負圧で運転しているのですが、本当に制御装置が壊れたら圧力が上がってしまうわけです。そのときにどうやって担保するかというと、真空式のボイラーというのは、溶解栓といって、はんだのような金属で、これが95度ぐらいでうまいこと溶けてぽんと大気に開放されるわけです。それがなければだめですというのが今の規格なものですから、温度制御器だけでいいですよというのは、私どもは工作責任者大会というのを毎年やっていますが、その中でやはりそういう質問が出るわけです。今の場合、いわゆる電気式のものは基本的に信用できないということになってしまいます。温水ボイラーであれば、例えば電気系が暴走しても、安全弁がついているからそれ以上の圧力にはならないということでオーケーなのです。

○向殿座長　極端なことを言うと、自動車屋さんなんかがやっているISO26262を見ると、機能安全は確率だけでちゃんとやって、危険側故障率がどんどん下がれば二重系とか要らないと主張する人がかなりいますね。ここですね。

○池田委員　自動車とエレベーターは比較できないですけれども、先ほど向殿先生がおっしゃったように、エレベーターはもし大きな事故でとまらなかったら大変なことになるので、いろいろ機能安全で制御をがっちりつくるけれども、最後の最後はエネルギー的に受けましょうというところは規格として残していますね。ロボットはそういう差はつけないといったけれども、エレベーターはそういう機械だということで、機能安全はちゃんとやるけれども、そこまでは完全に信用していないという思想ではないでしょうか。

○安井副主任中央産業安全専門官　やはり事故が起きたときの重篤度で違うということですかね。

○池田委員　エレベーターのISOを決める委員会にちょっと私もかんでいたことがあったので、どうやって決めていたか興味深く見ていたのですが、全世界で稼働しているエレベーターの台数や稼働時間や今までの事故の統計、そういうデータを一応ちゃんと集めて、それぞれの安全関連部のSILを決め打ちしていったという過程を見ていまして、かなりよくやってはいるのだけれども、どうしても最後のどかんというところは、それは決してないという経緯がありました。

　機械的な最後のとりでとなるような安全弁であっても、機種によって、分野によって違うのでしょうけれども、そのままつけて捨てられるまで何も見ないでほっておくのもあれば、１年、２年で取り外して性能をチェックしろといっている機械設備もありますので、では、その違いはどこから来ているのかというところがこの問題のヒントかもしれません。

○安井副主任中央産業安全専門官　まさに御指摘いただいたところは54ページのエのところでございますけれども、保護停止装置や緊急停止装置について、御指摘のとおり、作業前点検を義務づけているものとそうでないものがあります。これは重篤度なのか、あるいはどういう哲学に基づいて分けるのかということで、機能安全を使えるかどうかについて大きく違うと思いますが、何か御意見があればお聞かせいただきたいと思います。

○向殿座長　どなたか。
○池田委員　一つは、重篤度で考えている場合もあるでしょうし、もう一つの側面は、機械的な安全装置のそもそもの信頼性が、今、電気・電子のほうが数字としては高いでしょうから、機械的なほうも確実に働いてはくれるけれども、実は何もしないと動かないというところで、ばらしてチェックというところが入ってきていると思います。
○向殿座長　ありがとうございます。
　この辺は、ある意味で機能安全の本質的なところですね。電子装置に対して全部任せていていいか、ボイラーだと最後は安全弁があるという安心感はあって、後は制御で安全を任せているというところがあるのではないかという気がしますね。しかし、そんなことを言ったら、機能安全で規制を少し緩めようとか、つながらなくなってしまうのかな。
○杉田委員　機能安全でやると、結局、入力のセンサーの部分が非常に重要になってくるので、温度制御の話が出ていますが、では温度センサーでこのSIL2、SIL3に至るのがあるのかというと、まだないはずです。さっき言った温度で溶けるようなものが、機械安全でも最終的にはバイメタルでやらないと実は安全を担保できないので、幾ら高性能とうたわれている温度センサーを持ってきても､それにいい制御回路をつけてもSILはできなくなってくる。圧力センサーは物によってあるものもありますが、規格ができているというのがあって、ありますが、温度センサーに限っては何も安全度に関する要求がないので、一般に温度センサーはどんな製品にもついていますけれども、それで自動制御して、機械であっても家電品でもそれでとめているのですが、ある意味、安全は担保されていないというか、最終的に担保しているのはバイメタルのようなハード的な部品的なものになっています。
○安井副主任中央産業安全専門官　今の御議論、ちょっと確認ですが、例えば温度センサーそのものは、データを入力してテストすることはできなくて、実際に熱を当ててやるしかないということで、検査インターバルが短くできないという意味でしょうか。
○杉田委員　検査インターバルというか、温度センサーに関しては、評価して、その信頼性を上げるということに対しての決め事がないと言うべきなのでしょうか。
○安井副主任中央産業安全専門官　論理的には、例えば物理的に熱を当てて、まさに火災報知器のような検査を毎日やれば計算上の確率は劇的に上がるのですが、そういうことを組み込まれているセンサーにやれるわけはない、そういうことですかね。
○向殿座長　ありがとうございます。
　どうぞ。
○池田委員　本質の話で、プラントとか発電所のような大きな設備の場合の設計は、安全性関連部だけではなくて、通常の制御から、人がかかわるところから、避難退避とか、深層防護というか、あれで大きな設計方針を立てて全体の安全側の目標を決めて、わかるところは潰していって、最後の機能安全にどのくらい性能を持たせようかというところに落とし込んで性能を決めていっていますので、プラントならプラント、機械なら機械という

ものの全体の安全の目標を決めないと、どう割り振っていいのか、目標をどこに置いたらいいのかというのは結局わからないと思います。では、それを誰が決めるのかというところは、今そこはメーカーさんが自分で決めろとアセスメントで言っているだけですから、そのあたりをどう考えたらいいかというところがこの検討会の大きな課題でしょうか。
○安井副主任中央産業安全専門官　今、池田委員が御指摘いただいたのが適合のところでありましたユーザーとの関係ですが､プラント全体のHAZOPをするのは誰なのかというところにつながっているという議論だとは思います。
○向殿座長　プラントが爆発したと想定して、どのくらいのエネルギーを持ってどこまで迷惑かかるかと考えてひどさを決めてという形で押さえていって、最後に確率と制御の部分でSIL幾つという､そういう外側の事故が起きたと仮定して､どこまでが許せるかという範囲内から持っていくというやり方が確かにあるのでしょうね。
○池田委員　昔のドイツの原発がそういう設計方針で、数字で具体的に、規格で出していました。今はないです。
○向殿座長　ほかにいかがでしょうか。
SILが高くなると規制を何とか緩めるところはないのかという議論で来ているところでありますが、いろいろ御意見ありがとうございました。
それでは、次に行きましょうか。３番目、これは認証の話ですね。論点３番目ということで、56ページ、お願いをいたします。
○安井副主任中央産業安全専門官　「機能安全の安全度水準の第三者認証のあり方」でございますけれども、下のほうに前回御説明いただいた内容を簡単にまとめております。
まず、機能安全の第三者認証は、導入フェーズ、コンセプトフェーズ、メインインスペクションフェーズ、認証フェーズの４段階で実施する。
導入フェーズでは、エンジニアのトレーニング、資格制度を活用する。
コンセプトフェーズでは、製造者から安全要求仕様、安全コンセプトなどの提出を受けて、危険な状態を回避するための安全方策（安全な状態）を特定するため、故障モード影響分析（FMEA）などが適切に実施されているかどうかの評価を実施する。
メインインスペクションフェーズでは、実機を用いた試験を行いまして、最終報告書を作成するわけですが、ここでハードウエア故障挿入試験や、ソフトウエア検査、電気安全試験、環境試験などのほか、機能安全マネジメント監査も実施する。ここでユーザー向けのマニュアル審査も行われるということでございます。
認証フェーズでは、最終報告書と安全コンセプト等の整合性確認、テスト結果の検証などの総合レビューを行って、証明書を発行するということでございます。
審査の対象となる故障の種類ということでございますが、審査は基本的にランダム故障を行うわけですが、特にソフトウエアにつきましては、決定論的故障についても対象とします。ランダム故障は確率的な評価を行うわけですが、決定論的故障は主にヒューマンエラーの防止という観点から、チェックリスト方式（TOE）というやり方で審査するというこ

とでございます。

認証の対象単位でございますが、制御装置や安全コントローラーのようなデバイスに対して認証を与えるケースが多い。あるいは制御装置など組み込んだ状態で機器全体の認証を行う場合もあるということでございます。認証を受けたデバイスを組み込んだ機械等全体に機能安全の認証が必要な場合は、組み込んだ状態で再評価を行う必要がある。認証に要する費用や時間は、認証対象の安全関連システムの用途の広さに依存する。多用途になればなるほど審査に費用と時間を要する。

ISO/IECによる機能安全の認証機関となるための要件でございますが、各国の認定機関、日本では日本適合性認定協会（JAB）から認証機関として認められる必要があるということでございます。認証機関になるための要求事項というのは、ISO/IECガイド65に定められておりまして、組織運営機構、人的資源、プロセス、マネジメントシステムに関する要求事項が定められています。現在、JABに認定された機能安全の認証機関はなくて、欧米の認定機関で認定された認証機関の日本法人が機能安全の認証を実施している状況でございます。

検討のポイントでございます。

まず、「ア　専門的な第三者機関による認証の必要性」でございますが、今までいろいろ議論いただきましたけれども、仮に機能安全の要求水準を適切に満たしているかどうかによって規制を分けるということであれば、それを専門的な第三者機関が認証する必要があるのではないかということでございます。

「イ　専門的な第三者機関の要件」としては、ISO/IECガイド62というのがもともとございますけれども、そこで書いてあるのは比較的、抽象的な内容でございまして、個別具体的にどういう認証をするのか、認証ノウハウを書いているわけではありませんので、どこまでそういう能力があるのか審査するのはかなり難しいところがあろうと思います。

「ウ　機能安全の認証」につきましては、前回御説明いただいたとおり、導入、コンセプト評価、各種試験、認証のフェーズがあるということで一応入れさせていただいております。こういったことができる機関でないとだめだということになろうかと思います。

「エ　認証機関の認定」としては、ISO、IECのスキームによればJABで認定するわけですけれども、そこに至らないような状況においてどのような形で第三者機関が認定していくのかという議論がございます。特にJABなどの場合は、認定するときに経験を要求され、鶏が先か卵が先かという議論になりますので、現時点で認定機関がない、認証機関がないこの状況からどのような形でそういったものを育てていくのかというところも御議論いただければと思います。

説明は以上でございます。

○向殿座長　どうもありがとうございました。

認証機関、認定機関も含めて御説明がありましたけれども、認定機関になるためには、日本ではない、経験がないからできないということになって、では、一つの道は何かというと、国際規格に合わないけれども、認証、認定の小さな形でやっていって経験を積んで、

だんだん近づけていくという話になるのか、ほっておくと常に外国の認定機関、認証機関という話になってしまうのだと思います。いかがですか。石田委員が一番悩んでいるところです。
○石田委員　率直に言うと、立ち上げのときは行政のほうからアポイントしていただくのが。
○向殿座長　サポートがあって。
○石田委員　はい。非常に助かります。それで何年間か経験した上で、認定する機関、例えばここで言うJABさんなんかも一緒にトレーニングを受けながらみんなで底上げしていくという方法をとらないと、本当に卵が先か鶏が先かという議論になってしまって、どこかで腹をくくってやらざるを得ないのかなという思いはあります。
○向殿座長　ほかに。
○福田委員　石田さんや杉田さんがいる前なのですが、まず、ISO/IECガイド65は、今、ISO/IEC17065になっているので、これは直されたほうがいいと思います。それから、57ページのISO/IECガイド62は65の書き間違いだと思います。全部、ISO/IEC17065です。
　それはともかくとして、ISO/IEC17000というのが用語とか概念の規格なので、そこに認定機関は最後は政府の権威によると注がついていまして、やはりそうやって育てろということではないのですかね。杉田委員がいらっしゃるので、ドイツの認定機関はどうやってできてきたか、先輩方は何をやっているか、イギリスでも何でもいいのですが、卵が先かというのがやはりイギリスだってドイツだってあったのではないかと思います。
○杉田委員　済みません。認定機関のスタートまで把握していないのですが、各国に認定機関があるのは事実ですね。恐らく最初は国家レベルで何らかの、俗に言う言葉でお墨つきを与えたところが認定機関のように独立してきたと思います。それがどういう背景かというのは、ドイツではDAkkS、イギリスはUKASがあって、当然、今は内容、スキームは同じ活動をしていますが、その出発点がどうだったかというと、私、勉強していないのでわかりません。
○向殿座長　どうぞ。
○石田委員　なぜこれを言うかというと、産業安全技術協会はISO/IEC 17065の認証をとっているわけでもなし、JABの認定をとっているわけでもなし、でも厚生労働省の登録検定機関ということで、それだけで国際的にある意味、通用するのです。ISO/IEC 17065やISO/IEC 17025、そこにこだわらずに、日本は世界的に見ても信頼が置かれている国ですし、そこは行政の力を期待したいと思っています。
○向殿座長　いかがですか。どうぞ。
○杉田委員　その前に、最初にちょっと文言の話なのですが、56ページのウのところで「機能安全の第三者認証は、導入フェーズ（教育訓練・構想）」とあって、その後、丸２で「導入フェーズでは、エンジニアのトレーニングを実施する」とあります。これは前回私が説明したと思いますが、必ずしもトレーニングが必要というわけではないので、導入フェー

ズイコールトレーニングというわけでもないし、当然、経験のあるお客さんであればする必要もないし、どっちかというと、これから何をやろう、つくろうとしているのかというその辺の構想の確認のほうが強いと思います。要するに、必ずしもトレーニングというわけではないので、そこだけちょっと訂正していただければと思います。

○向殿座長　ありがとうございました。

○杉田委員　続けて、認証機関の認定の話ですが、要は、日本で認証機関をつくった場合、どういうスキームで運用するかということなのです。今、特定機械の認証というのは労働安全衛生法のもとの特定機械で、それぞれの安全衛生規則、構造規格でボイラー、圧力容器、クレーン、エレベーター等がありますが、それだけが認証のスキームです。その他の機械はないのです。あと、高圧ガス保安法に基づく高圧ガス設備がありますけれども、一般的にそれ以外の機械もないし、機能安全も何もない。

そこで認証機関をどうつくるかという話で、例えばどこかの機関がISO17065の認証機関になって、機能安全の認証機関になって、何がしかの認証を出した、それを労働安全衛生法で受け入れていただけるのかどうか。つくっても、結局、独立していれば意味がない。反対に、石田さんが言われたように、日本の法律はISOよりもさらに厳しいので、日本の労働安全衛生法に適合したものは61508に自動的に適合するという交渉を行政機関にしていただけると非常にいいのではないかと思います。相互認証という形にするのも日本国としてはいいことだと思います。今、明らかにISO/IECのスキームに入っていくところでそこだけつくったとしても、国の法律と乖離していれば全く意味を持たない。国の法律に入れるのだったら、それが国際スキームのさらに上位にあるので相互認証しましょうという交渉をしていただければと思います。

○向殿座長　ありがとうございます。

私も経済産業省とかいろんなところでやってきたけれども、結局、認証をするのに安全基準とか何かはISO/IECにのっとってやろうとしても、日本は日本で省令とか何かがあって、またちゃんとスペックに合わないといけないという、ある意味、二重になっているわけです。輸出する場合はちゃんとISO/IECにのっとるけれども、国内では日本の省令だけでいいというダブルスタンダードになっていて、メーカーは相当苦しい話になっています。日本の中で認証をちゃんとやろうと思ったって、いや、日本では省令に従ってやればいいので要りませんと言われて、ビジネスにならないというのが現状です。

10年、20年ぐらいこういう話をして、ちっとも日本では立ち上がらないというのが現実で、ダブルスタンダードというのは実は消えていなくて、今でも歴然としてあるのです。これを解消するのは、今、杉田さん言われたみたいに、国が認めたもの、今、特定機械だけしか縛っていないけれども、包括的に決めて、国がこの基準、ISO/IECもいいですが、日本のJISでも構わないけれども、これにのっとっていれば国としては認証したと一緒という形で一本化すれば、そのお墨つきに相当する今の大臣認定とか、そういう話で国がバックアップしていますよということになれば世界に通用することになるというのが石田さんの

お話だと思います。

日本がなぜ認定・認証でちっとも立ち上がらないかというのは、日本の国の法律とか規制の考え方、概念というのがかなり独特で、しかも非常に厳密で厳しいというのも事実で、これが日本の製品の安全を高めているのも事実であるけれども、世界の流れから見るとどうも独特の構造になっているというところに問題があるような気がします。どうですか。言い過ぎですか。

○安井副主任中央産業安全専門官　今回議論させていただいているのは法令に盛り込むことを前提にしていますので、盛り込まないのであれば、そもそもこういう検討会を開く意味はありませんが、ただ、盛り込み方については非常に検討を要するとは思っています。

一定の認証を受けた機能安全の機能であれば、例えばボイラーであれ、そういう制御機械であれば点検頻度を緩和するとか、そういう形を個々の省令に仕組むのは可能だと思います。ただ、それは前提として、先ほどの鶏、卵ではないですが、認証できる機関が要るので、そういったものがパッケージできるようにしたいとは思いますけれども、向殿先生が言われたように、包括的にどうこうというのではなくて、法令の取り入れというのは多分こつこつと個別具体的にという形になっていこうと思います。

○向殿座長　わかりました。

これがうまくいくと日本では画期的ではないですか。安井さんのやっていることはすばらしい。どうぞ。

○杉田委員　認証という話で、圧力容器のようなものと機能安全の認証を一緒にしてしまうと、恐らくメーカーさんが困るのです。圧力容器をつくっているメーカーさんは機能安全に対して経験がないので、その部分というのは、そういうユニットを買ってきてつけるしかないはずです。インプットになるようなセンサーとか、普通、圧力容器だったら安全弁をつけるのと一緒にリミッターをつけたりとかして、そこから先は制御なので知りませんよという話になるのです。そういう考え方で法令のほうも考えてやらないと、そうなると、そこにつけるべき何らかのセンサーのようなものも、認証されたものであるならば、そこにつけていいですよと。最終的には、エンドユーザーさんで組み込んだ後、圧力容器、ボイラーだけをつくっているメーカーさんからしてみれば、電気制御のことを言われても全くわからないはずです。材料と溶接とかやっているところに機能安全のものをつけてくださいと言ってもなかなかできないはずなので、そこも含めて考えていかないと、今の構造規格だと基本的には構造容器寄りであって制御は入っていない。そういうところへ入れてくると、今まで読んでいた人が理解できなくなってくるというのが出てくると思うので、そこを考えてやるべきかなと思います。その意味では、認証された制御装置であったり、制御のためのインプットとしては、それさえつければ、つけ方も問題ですが、それがあればいいとなっているほうがいいのではないかと思います。

○向殿座長　どうもありがとうございました。

ほかにこの件。

○安井副主任中央産業安全専門官　今の御発言に関連して、例えばボイラーであると構造規格というものでハードウエア要件を決めた上で、後はボイラー等安全規則という規則、これは省令ですけれども､それで取り扱いの要件を決めています｡今日議論しているのは、例えば点検とかいうことになると実は取り扱いのほうで、省令のほうです。省令のほうで手当てをするという考え方か、あるいは構造要件の中に入れてしまうのか、大分そこで考え方が違うのですが、そこは今回いろいろ御議論いただいて、そもそもどのような形で機能安全を使えるのかというものに応じて法令の書き方も多分違ってきてということにはなろうかと思います。
○須藤委員　確かに圧力容器は、圧力容器構造規格が今の制御のことは何も書いていないですね｡ボイラーは実は書いてありまして､ボイラー構造規格というのがあるわけですが、この中には実は燃焼安全装置や低水位遮断が盛り込まれていて、ボイラーというのは機能が限られているから､そういうことが書けるのでしょうね｡でも､圧力容器は千差万別で、確かにドンガラをつくるメーカーはドンガラしかつくらないでしょうから、制御というのは、組み込まれてフローシートができ上がってみないとどういう制御をするかわからないということですね。そういう点ではボイラーのほうは盛り込める可能性はあります。今、盛り込んではあるのです。こうしなければいけないとか書いてありますが、その信頼性までは規定はないのですが、そういう意味では、ボイラーという機械、一固まりでの規格には、ボイラー構造規格にはなっていると思います。
○向殿座長　ありがとうございました。
　ほかに。
○福田委員　関連して一ついいですか。ここで機能安全の認証と言っているのは、例えばソフトウエアのつくり方だったらこういうプロセスでいろいろ決まっているとか、あるいはSILの計算､パフォーマンスレベルの計算とかありますが､その話にとどまっているのか、そもそもこういう装置にはこういう安全機能が要る、そこも正しくちゃんと設定しているかというのを含んで皆さん議論しているのか、あるいは厚生労働省さんはそこはどこで切られて機能安全の認証という言葉を使っておられるのでしょうか。
○安井副主任中央産業安全専門官　基本的には、論点のポイントに入っていますように、コンセプト評価も含めて、FMEA、HAZOPとかも含めた形で認証するのを想定しています。
○福田委員　そもそもどういう機能安全をつけなければいけないかというところから含めてということですね。
○安井副主任中央産業安全専門官　そうです。一応はそういう考えにしております。
○福田委員　わかりました。
○向殿座長　ありがとうございました。
　ほかに御質問、御意見は、石田委員、どうぞ。
○石田委員　例えばボイラーというくくりで規制を設けるとなったときに、ボイラーに似たような製品でもボイラーではないというような境界線上の製品がこれからどんどん出て

くるかと思います。圧力容器でもないし、でも圧力容器のような機能もあるし、そういう危険性を持ったものを包括的に一旦、傘の下に置いておいて、どうするかということを議論してもらえればありがたいと思います。

というのは、法律の中で決められていない新しいコンセプトの製品が出てきたときに今どうなっているかというと、それを設置して動かすのに、例えば地元の消防署や地方自治体のオーケーをとったりしながら動かしていくときに、第三者認証がないと、地方自治体も安全なものかどうかわからないし、消防署もわからない、だから、ちょっと待ってという話が結構あります。

ここは早く第三者による評価認証のシステムをとっていかないと、せっかく新しいコンセプト、新しい技術でつくった製品が世の中で貢献できないという状況に陥りますので、何かうまくカバーして機能安全を認証していく方法があればいいなと常々思っています。

○安井副主任中央産業安全専門官　今の御指摘は､法令の適用があるかどうかは別として、幅広く第三者認証できるようなスキームがあれば、法令が適用されていない機械についてもできるということですね。御指摘はわかりました。

○向殿座長　包括的にやるには非常に重要なところで、お墨つきとして、それに最初から国が関与することは可能ですか。

○石田委員　立ち上がりは緩やかに、例えば先ほど言いましたが、機械の包括的な安全基準を適用しながら、あれはすごくよくできていると思うので、あれを適用して自己評価して、それを第三者に見てもらい、それが妥当だったかどうかという証明書を出すというシステムを構築していくことができれば、世の中どこへ持っていっても、消防署なり地方自治体に持っていっても認めてもらえるという制度がおのずとでき上がってくるのではないかという気がしています。

○向殿座長　ありがとうございます。

この議論からちょっと大きくなったけれども、ほかにございませんか。

まだなかなか難しいところがあるけれども、ぜひ認証というのを日本でちゃんと位置づけてスタートさせたいですね。卵が先か鶏が先かというよりも、動かすというふうにしないと、外国にばんばん負けて何年たつのだとよく言われているけれども、少しも立ち上がらないですね。

まだまだあるかと思いますが、時間になりましたので、本日はこの辺で終了させていただいてよろしいですか。安井さん、何か残ったことがあるようでしたら。

○安井副主任中央産業安全専門官　追加で御意見等ございますれば、できれば今月中、31日ぐらいまでに事務局にメールいただければ次回に反映したいと思います。

次回は、本日の議論を踏まえまして、骨子案をつくって、それを御議論いただきたいと考えております。

○向殿座長　よろしいですか。次回、たしか日程は決まっていましたね。

○野澤安全課長　日程につきましては、２月26日（金）午後３時半ということで先生方の

一通りの御予定は確認させていただいております。よろしくお願いいたします。
○向殿座長　ありがとうございました。
　それでは、今日はこれでよろしいですね。事務局に進行を返します。
○野澤安全課長　それでは、今日はこれでよろしければ、以上で第２回「機能安全を用いた機械等の取扱規制のあり方に関する検討会」を閉会いたします。どうもありがとうございました。