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１回議事録

厚生労働省労働基準局安全衛生部安全課

第１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27年12月24日（木）13:25～15:29

場　所：中央合同庁舎５号館労働基準局第一、二会議室

１　開会

２　議題

（１）検討会の進め方について

（２）機能安全を用いた機械等の取扱規制のあり方について

（３）検討にあたっての論点について

（４）その他

３　閉会

○野澤安全課長　それでは、５分ほど早いのですが、先生方お集まりのようでございますので、よろしいでしょうか。

本日は、お忙しい中を御参集いただきまして、まことにありがとうございます。

少し定刻より早いわけですけれども、ただいまより第１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。

私は、厚生労働省の安全課長、野澤でございます。座長が選出されるまでの間、進行を務めさせていただきたいと存じます。

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を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を申し上げます。

それでは、検討会の開催に当たり、厚生労働省安全衛生部長の加藤から御挨拶を申し上げます。

○加藤安全衛生部長　安全衛生部長の加藤でございます。

本日は、先生方にお忙しいところ御参集いただきまして、まことにありがとうございます。開会に当たりまして、一言御挨拶申し上げます。

もう御案内のように、産業用ロボットでありますとか、工作機械、あるいはボイラーなどの産業機械におきましては、電気・電子制御などの機能により安全を確保する機能安全という考え方が広く適用、採用されておりまして、その信頼性は、確率に基づく安全度水準で評価されております。

ヨーロッパでは、機械等のリスクに応じて必要な安全度水準を満たすことが求められ、かつ必要な安全度水準を満たす機械等に対して、点検頻度など取扱規制を見直す動きがあるわけでございます。

本検討会では、我が国の労働安全衛生規制体系に機能安全の考え方を取り入れるため、リスクに応じた安全度水準の設定のあり方、必要な安全度水準を満たす機械等の取り扱いに関する規制のあり方、安全度水準に関する第三者認証のあり方につきまして御検討いただきたいと思っております。

本検討会では、今後月１回のペースで御議論いただいて、本年度中には報告書を取りまとめていただきたいと考えております。その結果を行政施策に反映していきたいと考えております。

先生方にはまことに申しわけありませんが、大変タイトなスケジュールということでございまして、しかしながら、検討会ではどうぞ自由闊達に御議論をお願いしたいと思っております。

私からの御挨拶でございます。

以上です。よろしくお願いいたしたいと思います。

○野澤安全課長　それでは、続きまして、出席者を御紹介いたします。

資料１の別紙に参集者名簿がございますが、この名簿の順に池田委員のほうから左回り

に紹介をさせていただきます。各委員から簡単に自己紹介もお願いします。
それでは、池田委員。
○池田委員　労働安全衛生総合研究所の機械システム安全研究グループ､池田と申します。機能安全の話をやってまいりました。今日は産ロボに関する話を情報提供していきたいと思いますので、よろしくお願いいたします。
○野澤安全課長　続きまして、石田委員。
○石田委員　公益社団法人産業安全技術協会の技術支援部、石田と申します。よろしくお願いいたします。
私どもは産業安全技術協会、まさに産業安全の部分を担っていまして、私どもの部署では、ここ３年ぐらいの間に、機能安全ということに限って言えば５件ぐらいの評価、認証を行ってまいりました。うち３件は、イギリスのサイラ、現状カナダのCSAに買収されまして、CSAUKという名前に変わっていますけれども、我々はそこと協調して認証書を出しています。うち２件は我々独自の認証書を出させていただきました。そういう活動を行ってまいりましたので、その中で得た知見などをここで発表させていただければいいなと思っています。
よろしくお願いいたします。
○野澤安全課長　梅崎委員。
○梅崎委員　労働安全衛生総合研究所機械部長の梅崎でございます。よろしくお願いします。
私どもは、今、池田が申し上げましたロボット関係の安全性とともに、産業機械全般に関する安全性の研究を行っております。今回、そういう今まで当研究所が培ってきた知見を踏まえた上で、機械安全について対応していきたいと考えておりますので、よろしくお願いいたします。
○野澤安全課長　向殿委員。
○向殿委員　明治大学、もう定年になりましたけれども、向殿です。よろしくお願いいたします。機械安全とか製品安全とか、安全をいろいろやっていまして、最近はなるべく包括的に広く安全を見ようということに努力しています｡どうぞよろしくお願いいたします。
○野澤安全課長　杉田委員。
○杉田委員　テュフラインランドジャパンの杉田と申します｡よろしくお願いいたします。
弊社は、ドイツに本社がある第三者認証機関で、今日のテーマになっておりますボイラーを含む圧力機器指令、もしくは産業機械の機械指令等のノーティファイトボディ公認機関となっておりまして、日本から海外、ヨーロッパに輸出される製品の認証を行っております。
また、海外で製作されたものを日本に輸出する際のお手伝いということで、ボイラーであったり、クレーン等でありましたら、ドイツ本社のほうが指定外国検査機関になっております。その中で得られた知見等を今回の委員会でお話しできればと思っております。よ

ろしくお願いいたします。
○野澤安全課長　須藤委員。
○須藤委員　一般社団法人日本ボイラ協会技術普及部の須藤と申します。
　私からは、ボイラーの制御というのが実態としてどういうふうになっているか、そういった実情のほうを情報提供できればと思います。よろしくお願いいたします。
○野澤安全課長　福田委員。
○福田委員　長岡技術科学大学の福田と申します。よろしくお願いいたします。
　私は、機械安全、どちらかといえばイメージとしては工場に据え置いてある機械というのが主なことなのですが、そこを通して機械安全の基礎を大学では担当しています。
　今日は、パフォーマンスレベルとかSILの計算、これも大学の授業でやっているのですが、その辺の話から御提供申し上げたいと思います。よろしくお願いいたします。
○野澤安全課長　長岡技術科学大学の平尾委員からは本日欠席との御連絡をいただいております。御出席をいただいたときに御挨拶いただきます。
　それでは、本検討会には座長を置くことになっております。事務局といたしましては、向殿先生にお願いをしたいと考えておりますが、皆様、いかがでしょうか。
（「異議なし」と声あり）
○野澤安全課長　ありがとうございます。
　また、座長代理につきましてもあらかじめ決めておきたいと考えておりますが、事務局としては、福田先生にお願いをしたいと考えておりますが、いかがでしょうか。
（「異議なし」と声あり）
○野澤安全課長　ありがとうございます。
　それでは、今後の議事進行については向殿先生にお願いしたいと思います。
　よろしくお願いします。
○向殿座長　それでは、よろしくお願いいたします。
　では、座って進めさせていただきます。
　機能安全と規制というなかなか難しい話ですけれども、よろしくお願いしたいと思います。
　今日は時間が相当限られていまして、いろいろ紹介があると思いますので、円滑な議事進行に御協力願いたいと思います。とにかく実りのある議論をしたいと思いますので、どうぞよろしくお願いしたいと思います。
　それでは、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　資料の確認をさせていただきます。
　資料としては、ホチキスどめの資料１つでございますが、１枚目が次第でございまして、１枚めくっていただきますと資料１というのがございます。
　下のほうに続き番号のページ数が打ってございますが、７ページが資料２でございます。
　９ページが資料３でございます。

17ページが資料４でございます。

41ページが資料５でございます。

45ページから資料６ということでございます。

51ページが資料７ということでございます。

57ページが資料８。

最後に、63ページが資料９ということでございます。

○向殿座長　資料、過不足はないですか。石田さん、よろしいですね。

○石田委員　はい。

○向殿座長　それでは、議題１から進めさせていただきたいと思います。まず、事務局から資料２、検討会の進め方について御説明をお願いいたします。

○安井副主任中央産業安全専門官　まず、３ページの開催要綱から御説明させていただきます。

趣旨につきましては、先ほど部長から説明があったところでございますけれども、電気・電子制御などの機能により安全を確保する機能安全という方策につきまして、それを踏まえた形で機械の取扱規制というものについて御検討いただくという趣旨でございます。

検討項目につきましては、「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」「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」「機能安全の安全度水準の第三者認証のあり方」、大きくこの３点について御検討いただきたいということでございます。

１ページめくっていただきますと、参集者の名簿でございますので、省略させていただきますが、先ほど御挨拶はいただきませんでしたが、オブザーバーで経済産業省の堀補佐に御出席をいただいております。

資料２「検討会の進め方」ということでございます。全体で４回予定してございまして、第１回は本日でございますが、現状の把握と論点提示、論点に対するフリーディスカッション。

第２回目が１月25日を予定してございますけれども、第１回での質問等への回答と論点ごとの検討。

第３回が２月26日でございまして、ここで報告書の骨子案の御検討をいただきます。

最後は３月24日で、骨子案の議論を踏まえた報告書案につきまして御検討いただきまして、報告書の公表をできれば年度内に行いたいと考えているところでございます。

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。

今の御説明に何か御質問がありましたら。かなり厳しい日程ですね。これだけ厳しいのは珍しいですね。皆さん、頑張ってやっていただきたいと思います。

それでは、第１回は「現状の把握と、論点提示」。とにかく今日はフリーディスカッションをしようということで、まず資料に基づいていろいろ御説明願いたいと思います。

資料９に事務局が論点をまとめておりまして、論点が３つあるというふうになっていますので、今回は論点ごとに資料を説明していただいて、質疑応答するというやり方で、３回に分けて資料を説明、そして議論という形で進めさせていただきたいと思います。

それでは、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」ということに関して、事務局から資料３に従って10分程度御説明をお願いしたいと思います。

○安井副主任中央産業安全専門官　それでは、９ページの資料３につきまして御説明をさせていただきます。

まず、機能安全の導入の背景ということでございますが、機能安全の定義につきましては、完全に定まったものはございませんが、ここに書いてございますのは、主にIECで定められているものをベースにして資料を作成してございます。

簡単に申しますと、電気・電子・プログラム可能電子制御の機能による安全方策ということでございまして、当然機能でございますので、安全関連システムという制御関係のシステムに限定されたリスク低減方策ということでございます。

当然のことながら、従来からあります機械的な安全方策、そういったものに付加するということでございまして、これは後ほど御説明しますが、作動要求状態ということで、既存の安全方策が機能しないときに機能するといったものでございます。

これが導入されるようになった背景ということでございます。設計仕様の規定と非関税障壁問題というのは、特にEUにおいてあったというふうに聞いてございますけれども、各国で定めている詳細な設計仕様に基づく安全規格の統一というのは非常に難しいということを踏まえまして、製品の定性的・定量的な安全性能に立脚した性能の標準化を図っていくという方向があったということと、事後安全計画の限界ということでございまして、これは特にハードウエアの事故でございますが、事故・災害の減少が非常にまれになってきているということでございまして、その事故を教訓にして再発防止対策を実施する、そういった対策のとり方がなかなか難しくなってきたという背景がございます。

それからもう一つは、製品・システムの複雑化ということでございまして、産業用機械に限らず、おおよそほとんどの機械に最近は電子技術の進展により自動制御が入ってございます。これは非常に複雑で、それによる安全性を担保するというのがかなり難しくなってきている。

もう一つはコンピュータ制御、プログラマブル・ロジック・コントローラというものでございますけれども、これはソフトウエアで管理いたしますので、ソフトウエアにバグがあると、それがそのまま危険につながる。そういったものに対する安全規格というのが必要になってきたということでございます。

続きまして、３枚目のスライドでございますが、これがIECのほうで考えておられる機能安全が必要な状態となっております。縦軸は「故障原因の予見性と不確実性」となっておりますが、まず故障原因がある程度予見されるというものにつきましては、「ランダムハードウエア故障」と分類する。それから、予見できない、想定外。最近よく言われている

想定外ということでございますが、想定外の故障というのは、起きてみて初めてわかるということですので、なかなか予測ができないという前提のもとで、ランダムハードウエア故障で想定されるものについて、まず議論をするということでございます。

横軸は、システムが単純か複雑かということでございますが、単純なシステムと申しますのは、例えば何かのトラブルがあったときに、それが必ず危険側になる、あるいは安全側になるときっちり決まっているようなものにつきましては、故障したときに必ず安全側に保証するようにフェールセーフをつくるという形でできるということでございますが、これが複雑なシステムということになりますと、全く同じ故障が起きたとしても、あるときは危険側で、あるときは安全側というような複雑な場合がございます。こういったところについてはフェールセーフというのが簡単にできないということでございまして、こういうものについては機能安全ということで、より確率的な対応をすべきだということでございます。そういった内容でこの部分について必要だということになっているということでございます。

スライドの４枚目は、機能安全の導入ということでございます。もともとはISO12100というところで、リスクアセスメントをすべきだというのがあったわけでございますが、これに加えて、IEC61508（グループ安全規格）が定められまして、2000年に機能安全というのが規格上で初めて出てきたということでございます。

2005年に機械類の機能安全に使えるようにしたのがIEC62061でございまして、それを踏まえまして、ISO、機械をつかさどる国際機関のほうも機械類の機能安全の評価ということを2006年から定めてきたということでございまして、それぞれの個別の規格の中に随時取り入れられてきつつあるという状況でございます。

基本的な考え方といたしましては、ライフサイクルの基本的枠組みの構築ということでございまして、製品をつくってから、それを破棄するまでのライフサイクル全体のそれぞれの場面の安全度の尺度として危害のリスクという概念を使います。

従来の機械的な安全方策に加えて、安全関連システムの機能、制御の機能によってリスクを低減していくということを目指していく。

これの一つの特徴として、評価尺度に確率を使うということでございます。

５枚目のスライドは「全ライフサイクルにおけるリスク低減」ということでございます。５点ほど考え方がございますが、まず潜在的な危険とリスクを事前に洗い出しましょうということでございまして、合理的に予見される範囲内で潜在的な危険と危険状態、危険事象というのを明らかにしていきます。大きなプラントの場合は、HAZOPという形で、ハザード分析と言われる場合もございます。

あとは、そういった危険状態を踏まえて、必要な機能安全を達成するために、安全関連システムやほかのリスク低減措置の仕様を示して、安全度水準の割り当てを行う。

そして、要求された機能安全、安全度水準が実現されるような仕様を定めて、それを実現する。これは設計の段階でございます。

あとは、制御以外のリスク低減措置。例えば機械的な安全弁とか、そういったものも含めて、それもきちんとやる。

トータルとして全てのリスク低減措置を使って安全要求仕様を満たしているかどうかを確認していく。そういうシステムでございます。

６枚目のスライドにその概念図が出ております。左側から始まりますが、被制御機器、EUCと書いてありますが､制御装置が入っている機械にどういうリスクがあるかというのはもちろんありますけれども、一番右側に許容リスク目標というのを設定した上で、ここでさまざまな外的リスク軽減施設、あるいは安全関連システム、あるいはほかの技術、機械的な安全技術、そういったものを使ってリスクの低減を図っていきましょうという考え方でございます。

スライドの７枚目は、機能安全の対象となる安全関連システムということでございますが、これにつきましては、センサーとロジック部とアクチュエーター、そういったもので構成されていて、センサーで何型かを検知して、それをロジックで処理して、実際的にどのように対応するのかというのを決めるという一連のシステムでございまして、これがたくさんあるようなものもあるということでございます。

定量的な評価尺度ということでございますが、安全関連システムの機能によるリスク管理の性能は、確率論的な尺度である安全度水準。これはSafety Integrity Level、SILというもの。あるいはISOで使っておりますのがパフォーマンスレベル。PLと表記されますが、そういったものであらわしますということでございます。

安全度水準についてはIEC61508、パフォーマンスレベルにつきましてはISO13849-1でそれぞれ規定されております。

スライドの９枚目は、具体的にはどういうふうに決まっているかということでございます。安全度水準につきましては低頻度作動要求モード。要するに、まれにしか作動しないような安全関連系につきましては、１、２、３、４ということでございますけれども、数字が大きくなるに従って故障の頻度を下げていきなさい。一番厳しいのは10^{-5}ということでございます。

高頻度作動要求モード、非常に高い頻度で作動するような機械につきましては、同じ安全度水準４でも10^{-9}レベルまで下げなさい。そういったことが決まっております。

10枚目のスライドです。パフォーマンスレベルと安全度水準というのは、確率の関係でございますのでちょっとずれておりますけれども、安全度水準１に関するのはパフォーマンスレベルではｂということでございまして､以下そのような形で決まっておりますので、パフォーマンスレベルで考えても安全度水準で考えても相互の互換性があるようになってございます。

続きまして、要求安全度水準の設定ということでございます。

これは､そもそもある機械があるときにどれぐらいの機能安全のレベル､SILで言うと１、２、３、４、どれですかというのを決めるという考え方でございます。

大きく２つ考え方がございまして、まず定量的評価。これは数字、パーセントで何分の１という確率で計算する方法でございますが、これは前提として許容リスクを数字で特定する必要がございまして、例えば労働災害であれば、50万分の１とか100万分の１以下であれば許容するということを社会的に決めないといけないということですので、日本での実施はなかなか難しいという概念でございます。

もう一つは定性的評価でございまして、これは例えばリスクグラフ法というのがございますが、事故の結果とか、頻度とか回避可能性、望ましくない事象の発生頻度、そういったパラメータを入力していって、枝分かれ法で水準を決めていくという形で、最も広く行われている方法でございます。

過酷度マトリクス法というのがございますが、これは複数の施設がある場合に使われる方法でございます。これはちょっとややこしいですので、今回は説明を省略させていただきます。

スライドの12番は、定量的評価ということでございまして、先ほど御説明した図とよく似ていますけれども、被制御機器のリスクを作動の頻度と事故が起きたときの結果を掛け合わせてリスク評価するわけですが、一番右側にありますのが許容リスク目標ということでございますが、これは許容されるリスクというものに危険事象の結果を掛けるということでございますので、Ftというのが決まらないといけないということになります。これを実現するためにそれぞれ確率計算をしていきましょうというのが定量的な方法でございます。

続きまして、リスクグラフというのがスライド13ページにございますが、これは枝分かれ方法でございます。

まず、Ｃで結果リスクのパラメータというのがございますけれども、C_Aというのが一番軽くて、治るようなけが。C_DとかC_Cになると死亡するようなけが。

Ｆというのは頻度と暴露時間ということですので、そういった機械のそばにどれぐらいの頻度でいるのですかと。頻度が高い、低いで分かれてある。

Ｐというのは、事故が起きたときに逃げることができるかどうかという回避の可能性。逃げられる場合と逃げられない場合がございます。

Ｗというのが望ましくない事象の生起確率でございまして、これは、例えばボイラーとかであれば、安全弁のような機械的な安全装置が壊れたときということになりますので、そういう壊れやすい機械なのか、壊れにくい機械なのかによって、W_1、W_2、W_3というのを分けていく。それを当てはめていきますと、SILが１、２、３、４というふうに決まってくる。そういった簡単な考え方でございます。

次のスライド14でございますけれども、具体的にどうやって決めているかということで、これはボイラーの例で恐縮でございますが、例えばキーワードとして「蒸気圧力」で、原因としては消費側で蒸気の排出弁が急に閉じてしまったと。そうなると、熱交換器の中で圧力が上昇するわけですが、そこでリミッターが検知して、リミッターによってシャット

ダウンしますということでございます。

ただ、シャットダウンしても、結局、圧力が上がってくれば、最後機械式安全弁で外に逃がすわけですけれども、機械式安全弁が壊れる確率もございますし、リミッターが壊れる確率もあるということなので、それを踏まえてどう考えるかということで、事故が起きてしまうと、ボイラーですから、破裂してしまえば死亡まで至るということで、C_Cということで、死亡です。

F_Aというのは、それほど長い時間ボイラー室に人がいるわけではないということと、Ｐについては、爆発ですので、逃げられる余地はないということで、考慮もされない。

一方、こういった機械式安全弁とかはそうそう壊れるわけでもありませんので、事象発生確率は低いと評価して、最終的にはSIL2ですと。こういった評価をしていくというやり方でございます。

私から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、もう一つありますので、福田先生のほうからパフォーマンスレベルの計算方法について御紹介していただきたいと思います。資料４です。10分ほどでよろしくお願いいたします。

○福田委員　17ページからということで、資料としては枚数が多いですが、後で見ていただくときに具体的にはこんなものだなということで、一番大切なのは17ページの下でございまして、大まかな手順。これが今日、皆さんの共通理解が必要かと思います。

SILとかパフォーマンスレベルは、今、安井さんのほうから御説明があったとおり、作動信頼性の指標になるわけです。どれぐらい確実に働いてくれるのですかと。SIL1よりはSIL4のほうが確実に働く。パフォーマンスレベルＡよりはＥのほうが確実に働く。そういうものであるということです。

では、これをまずやっていくわけですけれども、少しそもそも論的な話になりますが、どういうことをやるか。それはリスクアセスメントをやって、どんな安全機能が必要なのですかということをまず明らかにしなければいけない。逆に言えば、リスクアセスメントでそれが出てこないと、機能安全はおろか、何の対策もとられないものになる。

極端な例は、金属の板を曲げるプレスという機械がありますが、あれに手を入れたら手を潰されるということがリスクアセスメントで出てこないと、何にも手当てをしないプレスができてしまう。もちろん、法令があるとかはあれですけれども、そうだということです。

でも、手を入れるかもしれないからライトカーテンをつけようねということになったときに、ライトカーテンとロジック部があって、とめるコンダクターかブレーカーがどれぐらい働くかということを見積もらなければいけない。それが必要な作動信頼性の決定。これがパフォーマンスレベルかSILを割り当てるということになります。

今度、パフォーマンスレベルＤでなければいけませんよとか、SIL３でなければいけませ

んよとか、決まったらば、今度それに合うような回路を設計していく。回路以外にも部品を選ぶとか、それからハードウエアの設計もありますけれども、やっていく。

最後に４番目ですが、それはもともと決めたパフォーマンスレベルＤが必要だと決まった回路とか、そういうシステムになっているかというのをチェックする。SIL3と決まったのに、ちゃんとSIL3ができているかなと最後計算していく。主に計算も入るし、それから違った意味の妥当性の確認もありますけれども、そういうことをしていくというのが大きな流れです。

この流れに沿ってですが、まずリスクアセスメントから必要な機能の決定というのが18ページです。

先ほどもプレスの例を出しましたが、手を入れたら危ないということに気がつかないとだめなわけで、手を入れると危ない、作業者は入れるかもしれない。そうすると、そこで危険な状態が出てくる。だから、危険な状態があって、安全な状態に持っていくのが安全機能ですから、まず危険な状態に見つからないものは全然だめ。ということは、リスクアセスメントが大切だということになります。

そうすると、もとの機械は、安全な状態がない機械はあり得ないというか、安全な機械がないものはこんな議論をしてもしようがないというところもあります。プレスの場合だったら、多分とまって上型がおりてこないようになっていれば安全な状態。手を挟むということに関してです。感電とかというのはまた別な話になります。

だから、このプレスは、確実にとまっているのが安全な状態。それがあるから、おりてくるとき､手を入れたということに対して､機械をとめるという安全機能がわかってきて、作業者はどれぐらい入れるかなということから､パフォーマンスレベルとかSILが決まってくる。そういうスキームになります。

では、決まりましたので、今度は安全装置をつけるわけですけれども、18ページの下のほうに「安全関連系」と書いてありますが、これは61508の図をただ描き直しているだけです。プロセスというのが化学プラントであったり、旋盤でもいいし、化学プラントプロセスでもいいのですが､プロセスがある｡それに対して､普通制御系がついているわけです。例えば旋盤だったら､1,000回転で回らなくてはいけないとか､いろんな意味で制御系がついているはずです。

もう一つ、今の安全に関して言えば、扉が閉まったことを確認してスイッチを入れてという、そういうシークエンスも組んであるはずです。

それは扉が閉まって、次にモーターを回していくわけだから、安全機能も実は持っているのですけれども、基本的に安全関連系というのは、それとは独立して、プロセス情報をとって、危ないとき、例えば不意に開けるはずがないときドアが開いたとか、ライトカーテンなどは、手を入れるはずがないのに手が入ったとかというときに急にとめに入る装置がつく。

特に61508はEUC制御系、いわゆる生産のための制御系に対して、確実に分けなさいよと

いうことを規定しています。安全関連系がEUC制御系になっていい条件というのは、また別に定めてあります。

61508を受けて62061がある。それは先ほど安井さんからお話があったとおりです。

13849も基本的には同じスキームです。

では、どうやってどの程度の性能を決めるのということになると、リスクグラフ法であったり、マトリックス法であったり、これは先ほど安井さんからも御説明があったとおりです。

こういうのが決まってきました。

次に、安全関連部の設計をしなくてはいけません。ここで何を基準にするかということですが、先ほどどの程度正確に動くかという話ですけれども、61508は、高頻度、連続モードというのがございます。これは故障率で議論しています。

それから、低頻度モードは機能失敗確率でやっています。先ほど安井さんが言い間違えられていたのは気がついたのですが、安井さんの資料に戻っていただいて、13ページの上、コマで言えば９です。低頻度モードは、機能失敗平均確率で議論します。高頻度モード、連続モードは、「危険側失敗の平均頻度」と書いてありますけれども、いわば故障率で、１時間当たりで議論しています。これは時間当たりという単位がついています。この違いはちょっと大きくて、場合によったら後で問題になってきます。

戻っていただいて、そういうふうになっている。

62061は、61508を受けた機械版ですから、これも先ほど御説明がありました。これは、機械の場合には一般的に高頻度だと言われているので、高頻度モードである故障率を指標とします。

13849はそもそも機械専用ですから、故障率で計算します。

62061あるいは61508の高頻度モードと13849の相互比較ができるのは、故障率を使っているというところにあります。

もう一つ特徴と言えば、61508は、SILの計算を非常に数学的に厳密に持ってきています。

62061は、機械に合わせて少し定型化して楽にしてくれています。

13849は、後で御説明する標準構成、アーキテクチャと言っていますけれども、それを使うことを前提に、かなりばさっと簡易化しています。まず、これが大きな位置づけです。

ここまで来たところで、パフォーマンスレベルについて３分ぐらい、SILについて３分ぐらいお話しします。

19ページに、これからパフォーマンスレベルの話をしますと書いてありますが、パフォーマンスレベルは、定義だけで言えば、20ページの上、コマ７に故障の平均確率と書いてありますけれども、故障の平均確率（/h）で規定されています。これが定義です。

ですから、これから御紹介する指定アーキテクチャを使うという方法がありますが、61508ばりにすごく厳密な計算をしてこれを証明してもルール上では構いません。やる人がいるか、いないかは別ですけれども、ルール上は構わないということです。

では、そもそもどれぐらいパフォーマンスレベルが必要か。これは先ほどの安井さんと同じで、ただ、13849は機械だけなので非常に簡単にリスクグラフが描いてあります。シビアリティー、要は、大けがをするか、軽いか、それからしょっちゅうか、あまりないか、いざというときに逃げられるか、逃げられないかということで、Ｓ、Ｆ、Ｐで振っていって、最終的にどうなると決めます。

重症で、余りないけれども、いざというときは逃げられないとなると、S2、F1、P2でｄになるとか、こういうふうに決めていきます。

そうやって決まると、パフォーマンスレベルのリクワイアメント、Ｒが決まってきます。

済みません、こま９をダブってつけてしまったことに今、気がつきました。

こうやって決まって、今度先ほど言ったように61508ばりにばりばりに計算してもいいのですけれども、それでは機械設計が大変だと。特に非常に単純な安全装置についてそこまでやる必要はないだろうということで、21ページの下に出ていますが、大きく４つのパラメータでもう決めてしまいましょうということです。

フローチャートの真ん中あたりを見ていただきますと、カテゴリ、MTTFd、DC、CCFと書いてあります。この４つのパラメータで決めてしまいましょうということです。

この４つのパラメータだけを抜き書きにして図式にしたのが左下です。要は、MTTFdがlow、medium、high、どれであるかを決めて、それからDCが60％以下か、60～90か、90～99か、99以上かということで決めて、それからカテゴリという昔からあったものを決めて、このグラフを見ると、しかるべきパフォーマンスレベルだとわかるということです。

次に、これをどうやってやっていくかという話をします。そのためには、指定アーキテクチャというのを使ってくださいということになっています。それが22ページです。それはいろんな過程があるので、それは後で読んでいただくとして、結論から言うと、22ページの下です。カテゴリB/1。Ｉ、インプット、センサーとロジックのＬとコンダクターであったり、いろんなものがあるけれども、出力であるＯ、これが一列に並んでいれば、カテゴリB/1。

カテゴリ２というのは、それにテストイクイプメントとアウトプット・テストイクイプメント。要は、試験診断装置とそれの出力がついている。これがカテゴリ２。

カテゴリ３と４は、Ｉ、Ｌ、Ｏのペアが２つあって、Ｌの間で相互チェックする。Ｃと書いてありますけれども、相互チェックする。それから、Ｏが確実に動いたかどうかを、Ｌは、ちゃんとあなた、動いたかと聞いてくださいと。これは回路的にはバックチェックとかいろいろあるのですが、とにかくそういうことを要求する。こういうのが回路的にまずできていますよというと、以下の簡便な方法ができる。

MTTFd。これは３年、10年、30年、100年と区切っていますけれども、やる。各パーツのMTTFdは、メーカーさんに聞かないとわかりませんから、メーカーさんからもらっている。それを回路としてどう計算するのというのが、パーツ・カウント・メソッドであったりするのですが、大きくチャネル１、チャネル２、２つのMTTFdが計算できたら、「対称化する」

という言葉を使っていますけれども、それを一つの系として考えたら、幾らとみなしていいのというのが24ページの上になる。ここでMTTFdが出てきます。

２つ目のパラメータはDC。DCは、25ページの上を見てください。定義の範囲はともかくとして、MTTF分の１を相加平均して平均値を出して、それで60％以上90％以下とか、そういうふうに決めていこうというものです。これで２つ目は決まった。

CCFに関しては、共通原因故障の話なので、具体的にはスコアをつけていきます。例えば設計者は教育を受けていますか、そしたらば何点と。この表を見てつけていって、それが100点満点中65点以上になっていればいいというふうに判断します。こんなふうにやっていきます。

ちなみに、カテゴリというのは、先ほどのB/1、２、３、４の話です。あれが指定アーキテクチャという形で入っています。

あと、計算例を２つつけておきましたが、単一チャネルの例。これは13849の附属書をそのまま持ってきています。ここで先ほど見た式があるなと眺めていただければ結構です。

あるいは27ページの下は２チャンネルある場合ですけれども、こうなっているのだなと。これも先ほど出た式があるなと思って眺めておいていただければ結構です。

28ページの上と下は特異なやり方で、MTTFdをくれるメーカーさんと故障率をくれるメーカーさんとあったときに、両方をどうやって一緒に計算すればいいかという計算のことで、今日の議論にそんなに関係ないので、こんなのかなと思ってください。

それから、先ほどフローチャートを見ていただいたときに、ソフトは別と書いてありましたが、ソフトは基本的にこういう管理をしていくということで、Ｖモデルと言われていますけれども、ソフトウエアについては、安全関連ソフトウエア仕様があり、それを設計し、さらにモジュールを設計し、コーディングをしていくのですが、そのときに結果と検証。さらに、右上がりに上がっていくときに、モジュールの設計に対する検証、それからシステム全体の統合試験をやって、最後に妥当性を確認して、ソフトはいいですねということをやっていきます。

ちょっと大急ぎでしたけれども、これが13849の話です。

では、61508、パフォーマンスレベルの話です。パフォーマンスレベルについては、先ほど安井さんから御説明があったとおりなのですが、ランダムハードウエア故障は、指数分布に従って壊れるという前提がありますので、信頼性工学で計算できます。これが難しいわけです。

それから、ソフトウエアのようなシステマティックフェーリア、系統的故障については管理的な手法をやっています。委員の中でこれについて一番詳しいのは平尾だと思います。平尾にしゃべらせると、いろいろしゃべると思います。フォーマルメソッド、そもそも失敗しないソフトのつくり方とか、いろんな技法があるようです。

30ページの下に61508の図２というのがございます。ここを見ていただくと、全ライフサイクルについて考えてくださいと。まず、１のところで概念。こういうプラントあるいは

こういう機械は何をやるの。どういう対象なの。それでは、そこでリスクアセスメントをしましょうねといって、安全機能は何ですかと出てくるわけです。ここで電気・電子・プログラム電子であれば61508の世界ですから、次に対して、保全だとかいろんなことを考えたほうがいいけれども、一番のトピックスは多分９だと思います。安全関連部を設計して、実現する。設計し、製作するということになります。

では、SILの要求レベルをどう決めるかというのは、先ほど安井さんから御説明があったとおりで、同じものを引用していますけれども、こんなものでやっていきますよということになります。

61508は一般論なのでこうやっていっていますが、62061は機械に特化していますので、一つの方法として、もともとリスクというのは、危害のひどさと発生確率。発生確率は暴露頻度と危険事象の発生確率と回避の可能性なのだから、それぞれこういう点数をつけたらということで、31ページから32ページ、33ページに点数のつけ方が出ています。これは61508。要は、機械のときです。

今日はこういう質問が出ると思わないけれども、死亡は４点で、骨折は３点、この理由はなぜかとよく言われるけれども、よくわかりません。これは国際会議でこの点数を決めたときも含めて、エキスパートが集まって決めた。ある意味ではそれしか言いようがありません。これが妥当かどうかというのは、またちょっと違う問題かなと思います。

最終的に34ページで、これは安井さんの資料の13ページに描いてあるのと全く同じ表ですけれども、こういうものになってくるということであります。

ここで安井さんの資料の11ページを見ていただきたいのですが、あらかじめそういうものをつくられるとわかっていたので省きましたが、11ページ、あるいは14ページの下を見ていただいたほうがもっといいかもしれません。今のお話でわかるように、安全装置がどれぐらい働くかということを議論しています。EUCリスク。そこはFnp掛けるＣ。安全装置がなかったら、どれぐらいの頻度で危険事象が起こるのという話。

次に、許容リスク目標は、Ft掛けるＣになっている。FtとFnpの比が、ある意味ではSILです。これを何万分の１にするのですかというのがSILです。

ちょっと御注意いただきたいのは、Ｃは変わっていないということなのです。だから、安全装置が働けばとまりますけれども、安全装置が働かなかったら事故が起こってしまうわけです。だから、被害の程度を下げるのではないのだと。61508の考えは、被害の程度を下げることでなくて、確率を下げることを議論しているのだということ、これを我々は認識しておかなくてはいけないと思います。

実は危害の程度を下げる機能安全というのもあるのです。例えば身近では車のシートベルトです。あれは逆に頻度は下げていないのです。ぶつかるときはぶつかる。運転手の技量で決まります。でも、ぶつかったときに、肋骨を５～６本折って、手術で助かるか、車から飛び出ていって死んでしまうかという意味では、Ｃを下げている機能安全もあるのです。これが電気・電子・プログラム電子ではないから、61508は何も言いませんけれども、

あるのです。でも、61508にしろ62061も、Ｃを下げるということでなくて、確率を下げるという議論をしている規格だというのを私たちは知っておくべきだと思います。

戻りまして、今、34ページまで御説明しました。

35ページですが、要は、故障率という意味では、安井さんが出された13ページ、あるいは私の資料の34ページの表ですけれども、故障率という意味では同じなので、数字が同じところで持っていけるので、SIL3はＥ、SIL2はＤ、SIL1はＢとＣというふうに割り当てられる。これは同じ数字が同じだからということで割り当てられる。ただ、その前提はちょっと違うので、故障率がいいけれども、実はＤ、Ｃの考え方が違っていたとか、いろいろありますので、学問的に本当に横並びにしていいかと言われたら、ちょっとそれはと答えますが、実際的にはこんなものだということです。

故障について、62061は、アーキテクチャ、例えばハードウエアが幾つ壊れたときはこれ以上行ってはいけないというのをいろいろ決めています。それも詳しい話をここでしてもしようがないと思うので、必要なら後で見ておいてください。それから御質問いただければお答えします。

最後にPFDの計算と故障率の計算に触れておきます。PFDの計算は、37ページの下に書いてあります。今日は結果だけ必要だと思います。

38ページの上です。いろんなものがついて、例えば二重系とかを組んだときにどういうふうになるかというと、低頻度作動要求モードのPFDは、左上の表のように計算されます。これで気をつけてください。T_Pというパラメータが入っています。T_Pというのは検査頻度です。安全装置は、設計段階で１年後とか半年後とか１カ月後とかわかりませんけれども、ある点検周期を決めます。それをやった前提でSILが満たされるということです。

それから、故障率のほうは右下です。これもT_Pが入っていますので、決めた点検間隔でやって初めてSILは保証されるということになります。

あと、直列系、並列系、この辺を知っているといいです。38ページの下とか39ページは省略します。

後ろのほうは参考資料です。

以上です。すごく早口になりましたが、こういう仕組みだということです。

○向殿座長　どうもありがとうございました。

論点１に対して、機能安全の安全度水準の話、決め方ということで、お二人の御説明に対して、何か御質問等。皆さんはプロだから、もう質問はないかな。要するに、皆さんの意識を一応統一しておく必要があるということでありますけれども。もし御質問があれば。

いいですか。要するに、安全度水準というのは確率を考えているということで、シビアリティーというひどさのほうは、とりあえず考えていないということですね。

○福田委員　少なくとも規格の数値上。

○向殿座長　実際の事故はシビアリティーと確率の両方、組み合わせで起きますので。しかも、これは付加装置というか、安全装置の信頼度というふうに考えれば、非常にわかり

やすい話になります。本体は本体で、本質安全設計はまた別の話と。よろしいですか。この辺の意思統一というのは、大体皆さんできたでしょうか。専門家の方が何人かいらっしゃるけれども、そうでない方もいらっしゃるので。後でゆっくり質問していただいても結構です。

では、論点１については、皆さん、意思水準は合ったというか、わかったということで、次の論点２に行きたいと思います。これは安全水準、要求水準を満たす機械と取り扱いの規制のほうについてどう考えるかという話でありまして、これについても資料５に基づいて、安井さんのほうから10分程度で御説明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、41ページの資料５につきまして御説明をいたします。これは欧州連合におけるボイラーの事例ということでございます。

「ボイラ・圧力容器へのEU指令の適用」と書いてありますが、これは基本的なスキームはどのようなものでも同じでして、例えば機械であれば、機械指令というのがございますけれども、それを満たすEN規格。ISOがあればISO、EN規格があれば、EN規格を満たしていないと基本的にそれを流通させることができない。そういった形で規制をしているわけでございます。これがEU域内で共通に使われるというのが、EUのハードウエアに関する規制の基本的な考え方でございます。

ボイラーに若干特化した話をさせていただきますと、圧力容器指令、PEDというのがございますが、これも比較的安全なボイラーから非常に危険なボイラーまでございますので、これは最高使用圧力と容積を乗じた値によってカテゴリがⅠからⅣと分かれております。カテゴリⅠの場合は自己認証でいけるということでありますが、カテゴリⅡ、Ⅲ、Ⅳについては、ノーティファイトボディの認証、第三者機関にちゃんと見てもらわないといけませんよということが決まっているということでございます。

続きまして、３のスライドでございます。では、どの規格を満たしていればEU指令を満たしたことになるのかというのを、整合規格という形で規格が全部リストアップされておりまして、日本で言う官報のようなものに載っております。

そこの最新のリストという中に、例えばボイラーであると、EN12952とか水管ボイラー、丸ボイラーは12953、そういった規格が決まっている。その規格の中の一連のものとして、４枚目のスライドにございますが、EN50156というのがございます。ここで安全関連システムをどのように設計するかというのが決まっていまして、これを満たしていないと販売できないということになるということでございまして、基本的な考え方は、先ほど御説明しましたIECのSILの考え方なのですが、もうちょっと具体的に、例えばEN50156に何が書いてあるかといいますと、安全関連システムでは、故障アセスメントをしなければいけないよということ。あと、安全関連システムに個別の規格がありますので、個別の規格を満たしているものの場合は、例えば先ほど言った確率の計算をしないでいいとか、そういったことも決まっております。

それから、50156-2というのがありますけれども、この中でもうちょっと詳しく。先ほど

御説明がありましたが、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。それから、関連規格、Ｃ規格に合致していれば、ややこしい確率の計算はしないでいいですよということが決まっていたりするということでございます。

ただし、対応するような細かな規格がないような機械については、必ずSILの許容レベルの設定をしてくださいねというのが書いてあります。

それが５枚目の資料にちょっと書いてございます。上のひし形のところで、61508ですから、確率計算をすれば、その下にあるような個別の規格がなくていいですよというような飛ばし方もできるということになっております。ただ、ここで書いてあるのは安全関連システムだけですので、当然別のハードウエア規格をかわせるというわけではないので、実際問題としてこれのとおりにきちんと設計できるわけではありませんが、どちらか選択のような形になっているということでございます。

では、こうやってきちんと設計され、販売されたボイラーに対してどういうユーザー規制をかけているかというところがございます。これは英国の事例を６枚目のスライドに入れてございます。英国は、労働安全衛生法という法律があるわけでございますけれども、事業者に広範な裁量を与えていまして、合理的に実施可能な範囲で措置の実施をしなさいと。合理的に実施可能な判断基準としてガイドラインが定められておりまして、そのガイドラインと同等以上の措置をとっていれば、それでいいですよというガイドライン行政をやっているというところでございます。

ガイドラインの一例を44ページに記してございます。これはボイラーと人員の配置と機器の安全度、そういったものについてまとめられているものでございますが、一番左の列がボイラーの信頼度といっていいと思います。

配備１というのは、最新の規格に適合していないボイラーです。

配備２というのは、最低限満たしてはいますけれども、それなりのものです。

配備３になってきますと、最高レベルの自動化となっていますので、それから、ENに定められている追加のリミット機器があったり、追加機器がない場合は、ちゃんとリスクアセスメントをしていますよということで、かなり信頼度が高い。

配備４のほうは、先ほどの話ですが、safety function、安全機能について、SILがちゃんと設定されていますということになります。

それぞれの人員配置について違いが明確に決まっておりまして、配備１については、ボイラーの資格者をオンサイトに常駐させなさいと。

配備２については、適切に教育・指示された人がいて、トラブルがあったら、その人が資格者を直ちに呼び出すことができるという状態で運転して構いませんと。

配備３になりますと、３日に１回ボイラー運転者の点検があればいいということなので、３日間は無人で連続運転できますということになります。

配備４も基本的に同じということでございます。

ただ、機器の安全度というところでは、例えば配備１はフェールセーフが求められてい

るとか、配備３になってくると、ボイラーの制御及び機器について最も高い信頼性が要るとか、そういった信頼度の話も出てくるということでございます。

こういった形でグレード別に分けた規定がなされている国もあるという御紹介でございます。

○向殿座長　どうもありがとうございました。

ボイラーに関しては、ヨーロッパ、EN、一応こういうのがありますよと。ある意味では規制が少し楽になっているというか、安全度が高いものを使っている場合は手を少し抜いていいですよというような例があると。

ついでに、論点２では産業ロボットの安全規格についてもお話があるということで、池田さんのほうから資料６の御説明をお願いいたします。

○池田委員　それでは、45ページから簡単に説明します。

まず、産ロボの安全規格ですが、これはメーカーのためのものです。ISO、JIS規格。メーカーとインテグレーターのものです。

今日お話しするのはこの２つの規格、ISO10218-1とISO10218-2。これは今年JIS B8433として発行されております。

まず、背景なのですが、この規格は、機械安全体系のＣ規格と呼ばれるもので、個別の安全要件を定めたものです。この上層に今日お話のありました機能安全の規格。さらにトップに機械安全の原則やリスクアセスメントがあるISO、Ａ規格と呼ばれまして、結局、ロボットの規格というのは、上の規格の下にある。全部両肩にのしかかっているというものになります。という前提で見ていただきます。

45ページの下、重要なところだけ述べますが、まず、Ｃ規格、産ロボの安全規格は上位規格に準拠しているということで、安全原則とかリスクアセスメントとか機能的安全に全て準拠しているというところが特徴になっています。

３番目に「安全設計要求事項」と書いてありますが、準拠しているということに従って、リスクアセスメントをして、まずメーカーは自分がつくるロボットの安全のスペックを決めなさいという原則になっています。ですので、出発点は、先ほど福田先生がおっしゃったように、リスクアセスメントで安全の仕様、目標を決めなさい。その中に安全性能というのが入ってきます。

ページをめくっていただいて、46ページの上のスライドに「６．安全関連回路システムの性能」というのがございまして、基本的にリスクアセスメントでロボットの安全関連部の性能、安全の目標を決めるのですが、もしリスクアセスメントをやらないのだったら、この規格ではデフォルトでこの性能を決めていますというのが特徴です。先ほど説明がありましたように、安全関連システムというのは、主にとまる回路なのですが、パフォーマンスレベルＤ、アーキテクチャで言うと、カテゴリ３の二重系、インテグリティレベルで言うとSIL2を指定しています。ですので、メーカーがアセスメントによって、うちのロボットはもっとリスクが高いからと言ってこれより厳しいのをやってもいいし、あるいはリ

スクアセスメントによって、そんなにリスクは高くないと言うと、これよりも下の目標を設定してもいい。ただし、そういうプロセスを経ないで設計するのであれば、これが標準ですよと決め打ちをしているというのが特徴です。

下のスライドの停止機能というところ。停止というのは、実は２つございまして、危険な状態になったら、ロボットシステムがそれを検知して自動的にとまるインターロック、保護停止と呼ばれるものと、人が危険を察知してロボットをとめるという非常停止、２つございまして、基本的には両方ともアセスメントで性能を規定しないのであれば、先ほど６番で述べましたやや高目と。プレスほどではないが、プレスの下くらいのランクにあるパフォーマンスレベルＤ、SIL2をデフォルトにしています。

停止の場合、特にその性能が維持できなくなったときは、最終的には動力源を遮断してとまることを確保しなさいというのが、これはロボットだけではないですが、機械安全の原則になっております。

47ページに行きまして、産ロボの場合は、停止以外にも位置の監視というのが入っていまして、それが９番の軸制限です。ここは今日の議論のところにもなるのですが、もともと産ロボは、自由に動けるところを余り動き過ぎると人をぶん殴るから、位置を決めなさいということで、メカストッパーというものを標準にしていたのですが、メカストッパーでぼこぼこ当てるとロボットは壊れてしまうというところで、そこをだんだんと緩和してきています。それでも一番トラベル量が多いところはメカストッパーで当ててとめなさい。２番目、３番目の範囲量の大きいところは、飛び道具といいますか、電気・電子デバイスでもいいよとなっています。ただし、その性能というのは、６番で述べた原則の性能が求められるということです。

2006年の改定から、ここにソフトウエア、いわゆるダイナミックな位置監視、バーチャルフェンスと呼ばれるものですが、その概念が入ってまいりまして、プログラムによって動的に位置の監視範囲を決めてもいいと。ただし、そのハードウエアとソフトウエアもデフォルトでPL=d、SIL2は求められるというところです。

最近のトピックスとして11番に協働運転というのがございまして、これは新しく入ってきた概念です。ロボットが自動運転あるいは特殊な運転モードのときに、人がロボットのそばにいて一緒に動く。人とロボットがともに働くということで、日本語では「協働」、言語では「collaboration」と割り当てていますが、これについても位置、速度、それから直接人に仕事をする場合は、人に与える力というのもアセスメントで検討する必要がありますので、位置、速度、力というものの監視もアセスメントで決めていいけれども、デフォルトではこの規格に従って決めなさいとなっています。

ただし、力の場合は、本質的な方策というのを認めておりまして、そもそもそんな力は出ないよという場合は、制御によらなくてもいいというふうになっています。

その次に、ISO10218のパート２のほうなのですが、これは複数のロボットを使う場合や、実際にユーザーのところでロボットを設置してロボットシステムをつくる場合の規格です

ので、安全性能についてはパート１を準拠しているということで、説明は割愛します。

49ページの下のスライドに、産ロボの規格で一応カバーしている基本的な安全の要件と、制御に係るコンポーネントを抜き出したものがこういう形になっています。ロボットですので、いろいろなデバイスがかかわってきていますが、基本的にここに挙げているデバイスは、このロボットの規格の上層のＢ規格であります制御に関連するデバイスの規格で定められたものを使うというのが原則になっています。

50ページの上のスライドに安全性能について、まとめということで出しております。

まず、産ロボの規格で重要用語として「安全適合」という言葉が随所に出てきます。言語で言うと「Safety-rated」ということで、安全適合したハードウエアとか、安全適合したソフトウエアということで、リスクアセスメントあるいはこの規格で決めているデフォルトの安全性能を持つという意味でこの言葉が使われています。

その下は規格の本文を抜き出したものですので割愛しますが、四角で囲った真ん中、第１部5.4.2項のところが集約してあるところですが、産ロボで安全関連システム、制御で安全を確保する場合のデフォルトは、機械系のJIS B9705（ISO13849）のカテゴリ３のアーキテクチャでのPL=d。これはちょっと注意が必要なのですが、先ほどの福田先生の説明のとおり、PL=dというのは、３つぐらいの要素の組み合わせで選択できるので、自由度はあるのですが、この産ロボの規格ではアーキテクチャがカテゴリ３でPL=d をつくりなさいということ。そこだけ制約がございます。

あるいはSILのほうの規定ですと、プルーフ間隔。先ほどT_Pと御説明がありましたが、それが20年以上で、ハードウエアフォールトトレランスが１のSIL2に適合するということを求めています。

下に矢印で書いてありますが、カテゴリ３というのは、実はこの規格が最初に改定された2006年のときに、機能安全の規格がまだできていないのに産ロボだけ先走って安全の規定をしてしまったので、その名残でこのアーキテクチャをまず決めろという思想が今でも残っているというところです。

以上です。

○向殿座長　どうもありがとうございました。

産ロボの場合の安全度水準というか、決め方。デフォルトの場合はかなり厳しいことをやって、それよりもっと何とかしようと思うのは、リスクアセスメントをやってちゃんと説明すれば、もうちょっと安全度水準が低くてもいいですよという話ですね。

○池田委員　はい。

○向殿座長　それから、今のハードウエアは、アーキテクチャ、カテゴリ３にして、しかもPLはｄだということで、アンドになっているのが１個あるのですね。それは歴史的な経緯があるようであります。

それでは、論点２、要求水準、安全度水準をどうやって規制の中に取り入れるのかという説明ですけれども、何か御質問、御意見ございましたら。どうぞ。

○梅崎委員　これは論点にないことなので、今、この段階でお話しするのがいいかどうかわからないですが、機能安全を実際に産業機械に適用していくような適用範囲については、若干検討が必要かなと思うのです。何かというと、機能安全というのは、広い普遍的な技術ですから、それはさまざまな機械に適用できるのです。ただ、技術が適用できるということは、それを法として使ってうまく効果が上がるかどうかというと、ちょっとまた。技術の適用と法の適用の問題というのは別かなと。つまり、作動信頼性の向上ということが働く人の安全に一直線に結びつく場合とそうでない場合があるので、その２つは、いろいろ関係する団体の方がいらっしゃると思いますので、そういう人の意見を聞きながら、どこまでを機能安全でやっていくことで働く人の安全というのをきちっと担保していくことができるかということ、そこを議論する必要がまず１点あると思うのです。

２点目は、先ほど機能安全の話の中でフェールセーフという話も出てきたのですが、要は、この辺、単純に機能安全というのが独立してあるのではなくて、要するに、インターロックの技術、フェールセーフの技術、機能安全の技術、それから人の注意力に依存するところではヒューマンファクターの技術があって、これが一塊になっていると思うのです。決してその技術はばらばらでないと思うので、そういうトータルな技術として見たときどうなのだという議論は、もう一つ重要なのではないかと思います。

３点目は、産業安全の現場では新しい設備を入れるということはもちろんそうなのですけれども、既存の設備をいろいろと改善してうまく使っていくという流れも非常に大きいとなったときに、既存設備に対して作動信頼性の改善、機能安全というのをどういうふうに活用していくかということは、今の論点からずれるかもしれませんけれども、意外と大事な話だと思うので、これの検討は、この委員会全体で結構ですので、ぜひ議論してもらいたい。

○向殿座長　かなり本質というか、根底にちょっとかかわる。いいですか。では、安井さんのほうで。

○安井副主任中央産業安全専門官　後ほど御説明いたしますが、資料９の論点の中に梅崎先生から今、御指摘があった機能安全の適用についても入っておりますので、適用範囲をどうするかということとフェールセーフとの連続性という議論は一応論点の中に入れてございます。

ただ、先ほどの既存の設備をどうこうというのはなかったので、これはまた考えたいと思います。

○向殿座長　わかりました。

というわけで、今、梅崎さんから３つ提案がありました。２つは議論しようと思っている課題です。３つ目の既存のものはどうするか。既存不適格をどうするかというような話が出た。

ほかに質問ございませんでしょうか。どうぞ。

○安井副主任中央産業安全専門官　すごく簡単な質問ですが、50ページの下、御説明を飛

ばされてしまった協働運転条件のところなのですが、ここで「安全適合」という言葉が出てきていますけれども、これは自己認証でいいのですか。それとも第三者認証が要るようなものなのでしょうか。

○池田委員　基本的には自己認証。

○向殿座長　ありがとうございました。

ほかに御質問はよろしいですか。今の梅崎さんの議論は最後にやるということで。

現状の規制で安全度水準がどう使われているかとか、使われようとしているかという例を御紹介いただいたということです。よろしいですか。

それでは、論点３、機能安全に関する安全度水準の第三者認証について。資料７で、石田委員から御説明をよろしくお願いします。これも10分ほどでお願いいたします。

○石田委員　それでは、51ページの資料７から話させていただきます。私のほうは、今までとは視点が変わって、評価、認証する側からの話をさせていただきます。我々はどういうところを評価しているかという根本的な考え方について話をさせていただきたいと思います。手法についてはちょっと置いておいて、どういう考え方でやっているかということだけをお話ししたいと思います。

まず、51ページの下の図です。これはJIS C0508-1。これは61508と整合したJISなのですけれども、そこの図２よりそのまま持ってきました。なぜこれを持ってきたかというと、機能安全はこれだけがスコープですよということをまず知っていただきたかった。

○向殿座長　ここが全部ですね。

○石田委員　ええ。基本的には全部ですよということを知っていただきたかった。

多くの場合、この中でカラム10、この辺の論点がすごく注目されてしまって、ほかのカラムのところは結構軽く扱われているなというような気持ちがあります。これはあえて言うまでもなく、ここにおられる方は見なれたことだと思いますので、これぐらいにして。

次の52ページです。我々が機能安全を評価していくときに製造者の方に３つ説明しています。まず、安全状態を決めてくださいねと。括弧の中に書いているのは「安全が達成されているEUCの状態」。これはそのまま規格を引用した言葉なのですけれども、その下「EUCが、どのような入力に対しどのような出力をしている時が安全な状態なのかを決める。この安全状態に如何に失敗なく到達するか？を問うもの。EUCの安全状態はユーザが、また、EUCサブシステム（例センサ）の安全状態はその製造者が決める」という考え方で我々はやっています。この括弧の中は規格で決まっていることで、下の括弧で囲んでいないところは私のコメントです。

次に、ランダムハードウエア故障。「時間に関して無秩序に発生し、ハードウエアの多様な劣化メカニズムから生じる故障」ということで定義されているのですけれども、ハードウエアはランダムに故障が発生すると想定したうえで検出できない危険側故障がどれぐらいの割合で発生するかを机上で計算する」。一般に「FMEDA」という言葉を使っています。でも、規格では「FMEA」という言葉を使っています。

次は、決定論的原因故障。決定論的原因故障の事例。これはJIS C0508-4の3.6.6項から引用しています。

どういうものかというと、安全要求仕様（中のヒューマンエラー）。ハードウエアの設計、製造、設置及び運転（中のヒューマンエラー）。ソフトウエアの設計、実施、その他（中のヒューマンエラー）。

決定論的原因故障は全てヒューマンエラーなのです。

以上は、設計の部分改修、製造過程、運転手順、文書化またはその他の関係する要因の修正によってだけ除くことができると定義され、マネジメントで故障を回避しましょうということです。

下のスライドです。これは安井さんが書かれていたものとダブっているのですが、ハードウエアの故障に関しては、決定論的原因故障、ランダムハードウエアの故障、この２つの要因があります。

決定論的原因故障というのは、ヒューマンエラーで起こります。設計ミスとか部品選定ミスということで起こります。

ランダムハードウエア故障は、FMEDAで解決していこうと考えています。

ソフトウエアは、全て決定論的原因故障で起きています。

我々は、決定論的原因故障をどういうふうに評価していくかということで、手法の名前をつけているのですけれども、「TOE（Target of Evaluation）」という言葉を使って、TOEで解決していこうと。

それが次のページの上の表です。こういうチェックリストをもって、どういうシステムで決定論的原因故障を回避していくかということを評価していきます。例えば61508-2。これは部分的に引用したものなのですが、18まで項目がありますけれども、大体61508-2で50項目。-3、ソフトウエアの項目で約数百評価項目があります。我々は、製造者の方にこの評価項目、こういうところを見ますよということを事前に見ていただいた上で評価に入ります。ですから、評価する方法も最初にオープンにした上で評価していくようにしています。

もう一つ考え方があるのですが、我々は、日本の中で評価していく場合には、53ページの下のフローチャート、労働安全衛生法のもとで機械の包括的な安全基準に関する指針を使っています。これは厚生労働省のほうから一応国際規格に整合していますよということなので、我々は、日本のメーカーさんに対しては機械の包括的な安全基準に関する指針に基づいて設計してねと。その結果、ISO12100に整合することになりますよということをお伝えしています。どちらもリスクアセスメントを要求しています。リスクアセスメントの中で危険源はちゃんとリスト化されていますので、それに基づいてどうなのですかと聞いています。

産業安全技術協会は、防爆電気機器の評価で結構実績がありますので、防爆の分野では、例えば欧州ではATEXというのを適用しています。EMCに関しては、欧州ではEMC指令があり

ます。電気に関しては、EN/IEC60204-1がありますというように、機械の包括的な安全基準をきっちりやっていくことによって欧州などのシステムに適合させていくことができるということで、その考え方でやっています。

ただ、爆発に関してちょっと残念なのは、欧州の場合は、電気機器と非電気機器を分けて、トータルでEquipment Protection Levelという方法で評価していますけれども、日本は残念ながら検定は電気機器だけの評価しか行っていない。防爆機器の話に絞りますけれども、我々は、トータルで評価する場合、あるいはそれを日本でも売り、欧州にも持っていくという場合には、機械の包括的な安全基準に関する指針を使って評価した上で、テクニカルコンストラクションファイル、技術構成ファイルと適合性宣言書をつくってもらっている。そこまで今やっております。

次のページです。私がある意味感動したことがあります。2012年にIEC60079-33というのが改正されて出てきたのですが、そのINTRODUCTIONに「この規格は、基本的な安全要求事項が今ある規格によりカバーしていない場合どのようにして本質的安全要求事項に合致することができるのかをデモンストレートし、革新を受け入れ、未知のものを取り扱うフレームワークを規定することを意図している」ということで、これはすごく大事なことで、これから世界は新しい技術がどんどん出てくるはずなのです。それを従来は従来の規格でカバーしようとしていたのだけれども、これからはそんなものだけではないですよ、新しいものをどういうふうに評価していくかということを考えましょうということで、この60079-33が出てきています。

引用規格として61508、61511、62061、13849-1、13849-2。今、出てきた規格が満載で、防爆規格の中に出てきているわけです。

防爆は、多分一歩進んでこのINTRODUCTIONのことが出てきたのだと思いますけれども、私はこれを見たときに、あ、ようやくこういうふうなモードになってきたなということでちょっと感動したことがあったので、紹介しておきます。

「機械安全認証の今後」ということで、54ページの下のスライドを見ていただきますと、60079-33の中に「8.2　アセスメントおよび試験仕様」ということで、「アセスメントおよび試験仕様は、製造者により準備され～」ということです。そうすると、我々は今後どういう役割を担っていかなければならないかというと、製造者が実施した試験仕様を評価していく、バリデートしていくという立場になっていくのかなと思っています。

では、我々はどういうところで縛られるのかということが次の55ページです。これもJIS Q 17065ということで、これもISO、IEC17065のコンパチで、認証機関に対する要求事項なのです。どういうことが要求されているかというと、製品プロセス及びサービス、ここまで適用範囲なのです。これを認証する機関に対する要求事項です。

用語及び定義は飛ばします。

55ページの下、組織運営機構に関する要求事項。資源に関する要求事項。この辺、公平・公正とか、認証機関の要員の資質とか、プロセスに対する要求事項とか、次のページに飛

んで、マネジメントの要求事項、こういうことがあります。

８項のマネジメントの要求事項に関しては選択肢ＡとＢがあって、選択肢Ａの場合は、ISO9001を取得していない認証機関に対しての要求事項です。選択肢Ｂというのは、ISO9001の認証取得をしたところに対してです。結果的に８項は選択肢Ａの認証機関に対する要求事項なので、認証未取得のところに対する要求事項ということになっています。

我々は日本の中でどういうふうにやっていかないといけないかというと、まずISO9001を取る、その次に17065の認証を取るということをやっていかないといけないのかなと思っていますが、日本の中で17065の認定を取ろうとするとちょっと問題がありますので、それは別の機会にお話ししたいと思います。

とりあえずこういう縛りがある中で、我々は、メーカーさん、製造者さんが実施した安全設計のバリデーション評価をしていこうと今、思っていて、ある意味トレーニングなのですが、過去３年間の間に５件やりました。うち３件はイギリスのノーティファイトボディに評価してもらって、そのままデータを受け入れてもらって、欧州のノーティファイトボディの証明書も出してもらっているという状況にあります。

簡単ですけれども、我々の発表をさせていただきました。

○向殿座長　どうもありがとうございました。

産業安全技術協会では、実はこういう機能安全の認定をやった経験があったゆえ、幾つか出しているということですね。しかも、JIS Q 17065をちゃんと適用されないと認証機関になれないのですね。

○石田委員　なれないです。オフィシャルの。今はプライベートの認証という形でしか出さない。

○向殿座長　プライベートであればいいけれども、オフィシャルに国際的に通用するためにはこれを適用しないといけないということ。しかも、これは何か問題がありそうなのですね。それはまた別のときに。

○石田委員　はい。

○向殿座長　ありがとうございました。

もう一つは欧州ではどうなっているか。杉田さん、よろしくお願いします。これも10分ぐらいでお願いします。

○杉田委員　資料の57ページの下です。EU指令と整合規格ということで、最初のページには機械指令、昇降機指令ということで、それぞれの整合規格ですが、まずISO13849、IEC62061というのが機能安全にかかわるＢ規格としてあります。

Ｃ規格。これはあくまで例なのですが、EN81。これはエレベーターに関連する規格になります。EN81-20の中のAnnex Aの中では、機能安全の要求としては、SILへの適合というのを要求しています。

その次のEN289というのは、Plastics and rubber machinesということで、要は、成形機なのですが、この中ではEN13849-1でPLrを要求しています。SILではなくて、13849のPLを

要求しています。

次はEN869ですが、これも安全規格で、pressure metal diecasting unitsですから、簡単に言うとプレスです。これに関してもEN18349-1、PL、Categoryというのを要求している。同じ機能安全の整合規格の中でもSILによるものと13849でPLを要求しているものがあります。これはあくまで事例です。

基本的に、2006年に13849が出た後に2009年の改定で、「EN869＋A1：2009」と書いてありますが、このときに多くの規格が、従来カテゴリだけだったものにPLを入れて、2006年に新しく出た13489に追随するようになっています。

エレベーターの場合は電子制御が非常に進んでいるということもあって、PESSRALと言われる電子制御がありまして、その中ではSILを要求しています。

次のページは、圧力機器指令に対する整合規格です。先ほど安井さんの説明でもありましたけれども、水管ボイラー、12952であったり、シェルボイラーであれば、この中ではEN61508-3を参照しています。SILを要求しています。この中で、既に御説明があったように、EN50156-1を参照しているということになっています。基本的にEN61508-3ですので、ソフトウエアに関してということが入っています。

EN50156そのものに関しても、パート２の中にパート１から７全部となっています。基本的にSILというのになっています。

その次にEN12263というのがあるのですが、これはSafety Switching devices for limiting the pressureということで、圧力のリミッティングデバイスなのです。圧力機器指令の中にはボイラーであったり、圧力容器そのもののほかに、圧力の制限素子としての要求があります。こういったものに関する規格がEN12263なのですが、この中で、機能安全と言えるかどうかあれなのですが、安全要求、圧力制限素子に関しては、EN60730-2-6を参照しています。

これは、タイトルを見ていただくと、Automatic Electrical controls for household and similar useということで、householdなので、家電というふうになるのですが、60730シリーズというのは、古くから使われている部品の安全性を確認する規格になっています。

この中でもソフトウエアに関しては61508-3を見るということですので、基本的にソフトウエアに関してはSILを要求しています。

その下の段に行きまして、機能安全に対して認証する場合、どうしているかという一つの手順です。次のページとあわせて見ていただくといいのですが、我々は、１、２、３、４と４つのフェーズに分けています。導入フェーズ、教育訓練、構想があって、コンセプトフェーズがあって、その後、メーカーさんによる設計、試作があります。その後にメインインスペクションフェーズ、認証フェーズと分かれています。

59ページの下に行きまして、では、導入フェーズとは何かといいますと、トレーニングというところからスタートしています。これは当然お客様の機能安全に対する習熟度によりけりなのですが、61508を進める中で、どのような教育訓練を行っているか、どういうレ

ベルの方が設計するのかということが要求されていますので、我々としては、そういった意味で、機能安全のワークショップであったり、オンサイトのトレーニングを設定しています。

また、機能安全のエンジニアの資格制度というのを設けて、例えば規格別に61508であったり、13849であったり、自動車であれば26262というものでエンジニアの資格を設けて、提供させていただきます。

ここで所定の機関のトレーニングを受けて、試験を受けて合格した人たちは、我々は、FSエンジニアとかFSエキスパート。当然エキスパートのほうがエンジニアよりも上のレベルになります。そういう資格を与えています。

基本的にこういう方たちが設計している案であれば、そこのメーカーさんの設計というものに関しては信頼があるというような考え方をしています。

60ページは、コンセプトフェーズということで、簡単に言うと書類審査、机上評価。石田さんの御説明にあったように、メーカーさんが用意した試験データであるとか、安全要求仕様、安全コンセプトというものをメーカーさんに提出いただいて、そういったものを評価させていただいているということです。FMEA、FMEDAということです。これから設計をするに当たって、その考え方、コンセプト、何を制御しようとしているのか、そういったものも含めてここでやらせていただいているということです。

機能安全の評価を進めるに当たってここが一番重要になっていまして、よくあるのが、最初石田さんから、E、10番からという話がありましたけれども、ここを抜いていきなり製品ができました、評価してくださいというのがある。機能安全の場合、できたもので評価することは、できないことはないですが、ここが欠けているので整合性がとれないので、不適合になる可能性が非常に多い。ですから、新規のお客さんだろうが、十分実績のあるお客さんであろうと、ここを十分しっかりやっていただいて、何に対して何を制御しようとしているのか、どういうコンセプトでつくろうとしているのか、それに対して十分な人員がいて、どういうふうにやるのかということをはっきりさせています。これなしではほとんど進まないということです。一般的な電気安全製品では、試験だけやればとりあえずもつということも可能なのですが、機能安全に関してはここが少し難しいところです。

これが終わった後にメーカーさんのほうで、このコンセプトに沿って設計していただく。

その後にメインインスペクションフェーズということで、ここが実際の試験をやります。検査、試験ということですので、ハードウエア故障挿入試験、Fault Insertion Test、要するに、故障状況をシミュレーションして、どういうことが起こるのかと。コンセプトフェーズで出たFMEA、FMEDAとの整合性、同じようなことが起こるか。

ここで、ソフトウエアがあればソフトウエアの検査。

機能安全マネジメント監査ということも行います。

一般的な電気安全試験。

あとは環境試験ということで、温度試験、湿度、振動。EMC試験も環境という大きい意味

でここに入れています。

あとはユーザー向けの文書、設置マニュアルとかオペレーションマニュアルというものをここで判断します。

アウトプットとしては最終報告書を出させていただいています。

次のページへ行きまして、認証フェーズ。最後のフェーズです。最終的にはここで最終報告書とコンセプトフェーズで行ったコンセプトの照合をして､テスト結果の検証をして、総合的なレビューをし、認証書を発行して登録させていただく。ちょっと小さいですが、我々の認証書の絵が出ています。

下にあるのがその認証のマークということで、製品に張っていただくということになっています。

ここの例で言いましたのは、我々、機能安全の認証の中でいろいろ述べてはいるのですが、製品に対しての認証か、システムに対しての認証か。簡単に言うと、例えばPLC、安全コントローラのようなものに対して認証を与えます。そうすると、認証されたものを機械メーカーさんが導入して、使って設計した機械をつくるとか、ボイラーの制度を使ったりということができます。

反対に、そういったものが組み込まれた状態でやるという場合もあります。これは最終製品のメーカーさんがどのようにされるかということになってきますので、日本で一番多いのは､やはりPLCとかセーフティーコントロールのメーカーさんが多いので､我々はそれに対しての評価をさせていただいている。

反対に、ボイラーの最終用途が温水であろうが、発電所であろうが、そちらのオーナーの方々は､そういうボイラーがあって､制限素子があって､制御回路があって､要求仕様、SIL3なのか､SIL4なのか､SIL2なのかによって全体を評価するということがある｡我々は、それに対して、現場サイドといいますか、発電所サイドとかであれば、再評価をすることがある。日本では、今、ここで決めようとしているぐらいですから、現場での機能安全の評価、認証がないので、主に輸出される製品の認証をしているというのが一番多いというのが実情です。

以上です。

○向殿座長　どうもありがとうございました。

欧州における認証の現状、それから先ほど石田さんから日本の現状を御紹介いただきました。

何か御質問ございませんでしょうか。これは多分日本では余り発達していなくて、非常に苦労しているところだと思います。

プロセスの認証と製品の認証は、価格で言うと１桁ぐらい違うのですか。直接的で申しわけないですが、相当違う話ですか。

○杉田委員　価格は何とも言えませんので。

複雑さが増せば増すほど費用は上がっていく。当然我々の人件費が上がっていくという

ことです。プロセスでも、例えば全てが認証されたシステムを使って構築され、機能が制限されていると、多分それほどかからないでしょう。一番困るのが、何の用途も決まっていない。SIL4で、プログラムコントローラをやりましょう、全てに対応できますとなったら、無限大になるので。そこは一様に比べられないと思います。
○向殿座長　わかりました。
　何か。どうぞ。
○安井副主任中央産業安全専門官　先ほども話がありましたが、例えばPLCだけ認証するということで、例えばPLCをボイラーにつけたとき、それはボイラーとしての認証をもう一回やり直すのですか。それともそれはそれでいいのですか。
○杉田委員　我々、ヨーロッパに出すときの認証の手順として、ボイラーの認証、機能安全のコントローラの認証というのがあるのですけれども、今、日本のメーカーさんの中では、どちらかというと個別に対応されているのが多いので、例えば我々、圧力容器を評価する部門では、圧力容器だけ、ボイラーだけ。そこにどういう制御装置がついているかというのは、安全弁は認証されたものがつきますとか、もしくはそれをヨーロッパで購入して後でつけますと。制御に関しては、何らかの制限素子があって、ほかの信号は、その制御に関しては別ですというふうになってきます。たまたまそれに使われる制御装置を我々の機能安全を認証する部門で評価しているかもしれない。もう既に認証されたものを使っているかもしれない。とすると、あとはオンサイトでそれを組み合わせて、日本のメーカーさんのボイラーを使って、日本のメーカーさんの制御措置を使ってシステムを組みましたと。それに対して、今度はユーザーさんのほうで評価をされるということになります。
○安井副主任中央産業安全専門官　そのユーザー評価も第三者評価があるのですか。
○杉田委員　第三者評価を望まれる場合もありますね。
○安井副主任中央産業安全専門官　義務づけられてはいないということなのですね。
○杉田委員　基本的にはPEDであれば、圧力容器の設計、据えつけまでと。運営に関しては国内法規になってきますので、それが必要であれば、そこになってきます。
○安井副主任中央産業安全専門官　それは国内法規次第ということですね。
○杉田委員　はい。指令に関して言うならば、設計、製造、据えつけまで。それをどう運用するか。要は、機械であっても単体で。ほとんどの場合が製造ラインになると思うのですけれども、たとえＣマークのついた機械であっても、ラインで導入してしまえば、当然それの接続部分というのは再度リスクアセスメントをしてやらなければ。一機械メーカーではできないのと一緒ですね。
　だから、制御機器メーカーとして、例えばSIL3でしか認証されていないPLCを、たまたまそのボイラーの制御にはSIL4が必要だったとすると、明らかに間違いですと。それを見た人間は、不適合と言わざるを得ないですね。SIL4で認証されたものであれば、SIL3のボイラーの制御が要ると言われても、それには使うことはできますけれども。でも、PLCの場合は、使い方次第でSIL4にもSIL3にもSIL2にもなりますから、もし使い方を間違っていると、

本来SIL3が必要なのにSIL1のような制御をしているということであれば、それは使用方法の間違いということになります。
○安井副主任中央産業安全専門官　わかりました。
○向殿座長　よろしいですか。
　どうぞ。
○須藤委員　先ほどの関連ですけれども、例えばボイラーというのは、現地組みのボイラーなどというのがありまして、PLCを使うこともあります。PLCというのは、それだけでは動かなくて、当然センサーも要るし、アクチュエーターも要ります。それぞれが認証を取れているとして、実際には現地の工事、配線もありますね。そのボイラーが例えば72時間見なくていいボイラーですというためには、現地工事も含めて、全体で受けろという話になるわけですね。
○杉田委員　そうですね。
○須藤委員　それは大変ですね。
○向殿座長　製品は製品でやっても、インテグレートした場合は、インテグレートした全体で認証を受けろという話ですね。
　ほかに。どうぞ。
○石田委員　質問ではないのですけれども、すごく気になっていることがあります。資料の50ページの上のスライド、池田さんが書かれたものなのですが、第１部5.4.2の四角で囲んだ中「プルーフテスト間隔が20年以上で、ハードウエアフォールトトレランスが１のSIL2」と規定したものでないとだめなのですね。SIL2だけではだめなのです。メーカーさんは、FMEAの結果をもって、例えばSIL2に到達していない場合、平気でプルーフテスト間隔を縮めます。20年どころか、朝と晩というふうな形にして、部品の信頼性が一見上がったように見せてSIL2を取りますので、ユーザーさんはこれをすごく気にしておいたほうがいいです。SIL2は、ひとり歩きをさせてはちょっと危ないです。
○向殿座長　ということで、SIL2というのは、余り高くはないという話ですね。
○石田委員　はい。
○向殿座長　ほかに。よろしいですか。
　いろいろ御説明いただきまして、ありがとうございました。今の認証についての御説明と御質問。
　それでは、議論３になります。本検討会の論点につきまして、事務局のほうから説明をしていただいて、時間があればフリーディスカッションをやりたいと思います。
　では、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、63ページの資料９につきまして御説明をさせていただきます。論点は大きく３つありますが、１点目は「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」ということでございます。これは労働災害防止という観点から機能安全をどうやって適用すべきか、それからどのような機能安全の要求水準

を設定するのか、それから安全関連システムが要求水準を満たしていることをどのように確認するかについて御検討いただくということです。

国際規格等は出てきておりますので、省略させていただきます。

検討のポイントといたしましては、まず、労働災害防止のための機能安全の適用ということでございます。特にIECの考え方は、機能安全が発現することを求められる作動要求状態というのをまず設定しますので、そもそも論として、既存の安全装置なりそういうものが故障したり、失敗しているというのを前提にいたしますので、そういったことになりますと、当然労働安全衛生を担保するために設けられている安全装置とか自動制御装置とか、あるいは機械のハードウエアそのものの構造的な欠陥というのがありますので、どういった場合が想定されるのかというところを御議論いただきたいと思います。

もう一つ、機能安全の発現の要件としてシステムが複雑であるということでございまして、安全関連システムの相反する故障・失敗の可能性。これは同一の故障がある場面では安全側、ある場面では危険側故障となる潜在危険性があるようなものということですけれども、これについて、そもそもどういうものがあるのかというところを御議論いただかないと、どういうところに使えるのかよくわからないということになってきます。

安全関連システムですので、センサーとロジックと最終出力装置があるわけですが、センサーそのもので相反するということはないと思うのですけれども、ロジックについては、PLCのようなものはそもそも故障の仕方がわからないので、そういうのがわかる。非常にわかりやすい例だと思うのですが、それ以外の例が、頭の体操でいろいろ考えてみたら、例えば故障でボイラーの給水バルブを開放する。通常は冷えるので安全側なのですが、加熱するときにいきなりどぱっと水が入ってくると、それで壊れてしまうというケースもあるようですし、あと、故障によってボイラーの蒸気供給バルブが開放する。これはボイラーにとってみれば、圧が下がって安全側なのですけれども、蒸気利用側にとってみたら、たまったものではない話でございまして、ボイラーのみならず、ボイラーを含む全体のシステムとして考えたときにはかなり複雑な問題が出てくるということです。

あと、ロボットの関係ですと、今日御説明いただきましたが、急停止がありますが、とめたら転んだという話もちょっとあるみたいですので、そういったところも複雑系になるのかもしれないというところですが、この辺は、そもそもどういうところで使うべきものなのかというのを御議論いただきたいと思います。

あと、機能安全というのは、あくまで安全関連システムに対する機能ですので、そういった安全関連システムを組み込んで意味のある機械というのはどういうものか。定性的に考えているのは、そもそも労働者をメカニカルに巻き込んでしまう産業ロボットとかプレスとか、そういったもの。あるいはボイラーのように爆発してしまう、化学設備のように爆発するようなものもございますし、あと、安全装置そのものもございまして、例えば安全装置で安全を担保していると、安全装置が壊れてしまうとそれでおしまいなので、そういったものも当然あろうかと思います。どういった機械があるのかとある程度定性的に御

議論いただけると、すごく助かります。

安全度水準の設定のあり方につきましては、先ほど御説明いただいたとおりですので、余り議論の余地はないと思うのですが、ちょっと気になるのが、ヒアリングしたときに欧州でも気にされているようでしたが、機械の使用方法によってリスクアセスメントの結果が違うというのがままあるということで、例えばボイラーを人里離れたところに設置するのか、病院の中に設置するのかで爆発したときのインパクトが全然違います。それによってSILががらっと変わるということがあるということですので、日本の製造者とユーザーが協議してというのがどこまで生きるのかというところがございます。

次のページでございますが、そこで法的な問題として気になるのは、では、要求される安全度水準が正しくなかったときは、製造者とユーザー、どちらに責任があるのですかという問題もございます。

そういった意味も含めて、専門的な第三者機関に見てもらうというのが必要ではないのかということでございます。

安全関連システムの安全度水準の算定方法につきましては、福田先生に御指摘いただきましたけれども、これも労働災害防止の観点から留意する点があれば、御指摘いただきたいと思います。

続きまして、論点の２つ目「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して、これは機能安全で要求される水準を満たした安全関連システムによって代替できる措置です。現在規制されている措置で代替できるような内容があるのかどうかということで、典型的な機械について具体的に検討いただきたいと考えてございます。

検討のポイントでございますが、例えば機能安全で要求される安全度水準を満たすことによって代替できる措置ということで、先ほどボイラーの話も出ましたが、無人の連続運転で時間が延びる。あるいは点検の頻度が下がる。点検の頻度は、先ほど石田さんからも話が出ましたが、下げていいのか、下げてよくないのかという議論もあると思いますが、そういったもの。

それから、ロボットのように従来柵の中に囲っているものについて、柵を外していいよという話もあると思います。ほかにどういったことが考えられるのかというところについてもちょっと御議論いただきたいと思います。

あとは、機能安全を導入する対象となる機械はどういうものがあるのかというところで、これも先ほどと同じですけれども、巻き込む危険性のある機械とか、爆発の危険性のある機械とか、安全装置とかあると思うのですが、こちらもどういうものが考えられるのかということを御議論いただければ大変助かります。

３つ目が第三者認証の関係でございまして、機能安全の要求水準の設定、安全関連システムが要求水準を満たしているか等について、第三者機関の認証、どういう内容を認証するのか。第三者認証の要件、こういったところについても御議論いただきたいと思ってお

ります。
検討のポイントでございますけれども、第三者認証の必要性といたしましては、機能安全の要求水準の設定がまず適正かどうかというのを第三者的にチェックする必要があるのではないか。
もう一つは、要求水準を安全関連システムが満たしているかどうかについて、ユーザーが判断するというのは極めて難しいので、こういったものは第三者のお墨つきが要るのではないかということでございます。
専門的な第三者機関の要件につきましては、IECのGuide 65とか、既に決まっているものがありますので､そういったものを適用する中でどういう留意事項があるのかということ。
あとは第三者機関の認定です。認定者は誰なのか。国がやるのか、あるいはほかのやり方があるのかというところ。
それから､ISOで既に認証機関としての認定を受けているところとの関係をどうするのか。そういったものについても御議論いただければと考えてございます。
これが論点でございます。
○向殿座長　どうもありがとうございました。
残った時間、あと15分ぐらいですけれども、御説明に従って今の論点を議論したいと思います。何か御意見、御質問等ありましたら、お願いいたします。
ツールを認定している機関はどこですか。
○杉田委員　認定機関は、日本だとJABさんです。ドイツではDAkkS。同じような認定機関として見ています。例えば労働安全衛生法では、ドイツの本社は指定外国検査機関になっています｡ボイラーとクレーンと某機器に関しては指定外国検査に｡これも一つ認定です。それが65だったり、17025だったり。ISO9000も持っていますね。
○向殿座長　国というのは、直接関与は。
○杉田委員　ドイツ国内では、国に関して、その指令に対してはないです。でも、ノーティファイトボディは国から｡DAkkSに認定されていることが一つの条件で､ドイツからノーティファイトボディとして指定されています。
それと、定期検査とかをするに当たっては、ドイツ国内法がありますので、それが指定検査機関として認定を受けています。それは圧力容器だったり、発電所だったり、エレベーターというのが、その機関になっています。
○向殿座長　なるほど。
ほかに御質問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　特にこの検討のポイントの適用のところで梅崎さんに補足いただければ。
○向殿座長　先ほどのどこまで適用するかという話。
○梅崎委員　こういうことを言ってしまうと極論になると思うのですけれども、要は、機能安全というのは、基本的に確率で評価をします。そうしたときに、逆に労働災害防止と

いう観点からどれだけの確率であればいいのかという議論がまずは出てくると思うのですが、その辺、逆に厚労省さんのほうではどうお考えなのですか。もちろん、確率だけの問題ではないと思うのですけれども。
○安井副主任中央産業安全専門官　先ほどちょっと御説明しましたけれども、定量的な考え方、定性的な考え方がありますので、日本のリスクアセスは定性的でやっているのがほとんどだと思います。諸外国を見ても、数字で決めてきているのは大体イギリスぐらいで、ドイツもやっていないみたいですので、どうしても定性的なリスクグラフ的な考えにはなると思います。
○梅崎委員　そうすると、やはりそこで言う機能安全の安全目標というのは、ISO、IECの中で定められた安全目標をそのまま援用することが、要するに、働く人の安全確保のために重要なものなのだということで。
○安井副主任中央産業安全専門官　いや、全てについて必要だとは思っていませんので、どういう機械に対して、どういう機能についてというのをちょっと御議論いただきたい。
○向殿座長　そこのところはちゃんと確認しておかないと。
○梅崎委員　わかりました。
○向殿座長　どうぞ。
○池田委員　安井さんとは安全弁の話もあったのですが、結局、対象となる機械がどういうアセスメントのルールを使っているか。リスクを下げるというのに、安全関連部の制御の確率を下げるというところがどのくらい支配しているかによって、その効果も評価も変わりますので、確率を下げただけで危害の程度を下げられなかったら、リスクが何にも下がらないではないかという話もあるかもしれないので、対象の機械でどういうルールを標準にして、その中で制御によってリスクを下げるのをどのくらいにすべきかというところから論じないといけない。
○向殿座長　本質的な安全制御をちゃんとやって、危害の大きさもちゃんと小さくしていってリスク低減策をやって、残ったものに対して制御系で下げようと。ここに確率が入ってくるのですよと。その場合に確率とか第２次ステップだけでなくて、第１ステップをちゃんとやった上で第２をやるのですよという意味ですか、今の話は。
○池田委員　という前提で。
○向殿座長　前提でやっているという。
○池田委員　はい。
○梅崎委員　ですから、一日丸々。先ほど石田さんが言われた機械の包括的な安全基準に関する指針との連携がどうしても欠かせなくて、しかも、そこは明確な優先順位があるわけです。その優先順位に従ってやっていく中で機能安全の位置づけというのがはっきりしたときに、この機能安全を使ったら物すごく効果がある話なのではないかなというふうに思います。逆にそういう視点がなくて、機能安全だけがひとり歩きしてしまうと、すごい怖いかなという。

○向殿座長　極めて危ないことになるわけですね。
○杉田委員　それが一番ポイントですね。そこだけやろうとするか。反対にできないのですけれども。だから、石田さんの資料の53ページにある指針等の下にどうやって機能安全が入るか。今、対象としている機械が労働安全衛生の特定機械だけなのか、それ以外の機械なのか。そこもはっきりして、どれに対して機能安全をやるのか。では、それに対して要求は機能安全構造規格みたいなものをつくってやるのかとなるし、それはIECとかをそのまま使うのかというので変わってくるので、その辺からはっきりしていかないと、論点が。
○池田委員　我々がメーカーさんにいろいろアドバイスするときに、なるべく機能安全というか、制御でリスクを下げるのは最後に回して。ちょっと商売の邪魔になるかもしれませんが、お金も手間も時間もかかるので、そこは最後の最後にして、うちは全部機能安全でやりますと宣言してやっていただいてもいいのですが、そこは難しいので、なるべくそこの負担を減らすように設計しなさいと一般的には言っています。
○梅崎委員　今の池田の意見ですが、先ほど安井さんも言われたのですが、もしこの話を入れるのだったら、設計段階できちっとやるという仕組みをしっかり入れておくというのが必要だと思うのです。ユーザーの段階で無理無理やるのでなくて、まず設計でやるのだと。それが一番効果があり、かつ安い対策なのだということをはっきりさせていくことが重要だろうと思います。
○向殿座長　要するに、包括安全基準というのがまずあって、そこの中でやるべきことをちゃんとやって、その中で位置づけとして機能安全と制御の安全があるという、この順番を間違えないでいただきたいということですね。それと、ある意味では安く済むこともあるし。全体の位置づけの中での機能安全の役割というのをちゃんと明確にして議論していってほしいという御提案ですね。
○梅崎委員　はい。
○向殿座長　ほかに何か。
　列車なら、とめればフェールセーフだというのがあるけれども、飛んでしまっている飛行機は、いかに機能を維持して着陸するかという話になると、かなり機能安全的色彩が強くなるのですね。だから、それはシステムによってかなり違う可能性がある。
○安井副主任中央産業安全専門官　まさにそこはシステムの複雑性だと思うのですが、とめればいいという機械なのか、そうではないのかというところだと思います。
　ボイラーとかは、単体でとめるのはとめられるのですけれども、システム全体として、ボイラーがダウンすると、ほかのところで危険が発生するようなものもあるみたいなので、それは個別の機械を通り越した議論になるのですが、メーカーさんはとにかくとめない、とめたくないと。とめればいいではないかと言っても、いや、これはとめられないのですという話がすごく多いので、そういう意味では機能安全の話が。
○向殿座長　とめると、別のリスクが出てきてということで。
○安井副主任中央産業安全専門官　ええ。何かが起きてしまうというのがあるみたいです

ね。
○向殿座長　どうぞ。
○池田委員　ロボット絡みで。今日は資料を入れていなかったのですが、産業用から外れますが、いわゆるサービスロボットは、人を持ち上げるために力を出さなければ仕事をしないので、資料にも書きましたように、本質的な方策というのがとれないのです。
○向殿座長　エネルギーが小さいとできない。
○池田委員　小さいと仕事をしない。とすると、そこを何でリスクを下げるかというと、制御で頑張るしかないので、サービスロボットの安全規格では、安全性能は決め打ちでかなり細かく決まっています。
○向殿座長　なるほどね。やはりシステムによって大分違いますね。
○池田委員　違います。
○向殿座長　ほかに何か御質問。お願いします。
○杉田委員　確認ですけれども、ボイラーの話が出てきますが、一般的にボイラーと言った場合、蒸気ボイラー、発電用ボイラーは入るのですか。
○安井副主任中央産業安全専門官　定性的な議論としては、またやっていただいて構いませんが、できれば用途を問わないようにしていただければ。厳密に言うと、発電用のボイラーは、電気事業法になりますので。
○杉田委員　それによって安全度も違うといいますか、ドイツでもそのニュアンスで決めていますし、単純な温水ボイラーは、非常に圧の低いものから、高いものもありますので、ここで一般にボイラーと言うと何を指すのか。
○安井副主任中央産業安全専門官　蒸気ボイラーは当然含まれますので、用途を問わず蒸気ボイラーというのは議論していただいて問題ないと思います。
○杉田委員　わかりました。
○向殿座長　どうもいろいろとありがとうございました。まだまだ議論が尽きないと思いますけれども、時間ですので、この辺で終わらせていただいて、御意見が当然あると思いますので、来年の１月８日金曜日までに事務局にメール等で御提出くださいということでありますので、今日気になったこと、質問、要望、その他、メールで事務局へお願いしたいと思います。
事務局のほうは、今日いろんな議論が出ましたので、追加意見も踏まえて資料をつくって、次回資料として提供していただければと思います。相当詰まった日程ですので、皆さん、健康に気をつけて頑張ってください。
では、事務局へお返しします。
どうぞ。
○福田委員　次回が１月の二十何日だったですね。
○安井副主任中央産業安全専門官　７ページに日程が全部書いてあります。
○福田委員　今、８日というお話が出たのですが、つまらないことで済みません。今日の

議事録はいつごろもらえますか。読み直したいなという。
○安井副主任中央産業安全専門官　済みません。即答できませんが、できるだけ。
○福田委員　８日までに質問ということで、25日が次回ということで。
○安井副主任中央産業安全専門官　８日までには無理だと思います。年末年始がありますので。
○福田委員　わかりました。
　もちろん、メモはしたし、覚えているつもりではいるのですけれども。そういう意味では、８日を少し緩和していただくとうれしいかなと。
○向殿座長　８日を過ぎても少しぐらいは。
○安井副主任中央産業安全専門官　もちろん、多少遅れても問題ないです。
○向殿座長　それでは、よろしいですか。
　では、事務局から情報がなければ、これで終わります。
　では、安全課長、お願いします。
○野澤安全課長　それでは、何点か事務連絡をさせていただきます。今も話題になっていましたが、次回の予定でございますが、第２回の検討会は来年の１月25日月曜日午後３時半から２時間程度。場所は、この建物の６階の専用第23会議室でございます。
　それから、これは原稿に書いてあるのですけれども、後日、本日の議事録をお送りしますので、御確認もお願いしますとなっておりますが、できたらお送りいたします。
　それでは、以上で第１回の「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。
　長時間どうもありがとうございました。