資料４

検討に当たっての論点

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

(1) 概要

労働災害防止という観点から、機能安全をどのように適用すべきか、どのように機能安全の要求水準を設定するのか、安全関連システムが要求水準を満たしているかをどのように確認するか等について検討する。

(2) 国際規格等

ア　国際規格等

① ISO 12100(JIS B9700): 機械の安全性－基本概念, 設計の一般原則

② IE C61508(JIS C0508):電気・電子プログラマブル電子安全関連系の機能安全（第１部～第７部）

③ IEC 62061(JIS B9961) 機械類の安全性－安全関連の電気・電子・プログラマブル電子制御システムの機能安全

④ IEC 60204:機械類の安全性―機械の電気装置―

⑤ ISO 13849:機械類の安全性―制御システムの安全関連部

⑥ ISO/TR 22100:Relationship with ISO 12100

⑦ ISO/TR 23849:Guidance on the application of ISO13849-1 and IEC62061 in the design of safety-related control systems for machinery

イ　検討会資料

① 機能安全とその要求水準の設定-安全度水準とパフォーマンスレベル）-（第１回資料３）

② 福田先生資料（第１回資料４）

ウ　前回検討会での意見等

＜機能安全一般＞

① 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（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り、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。

② IEC 61508 や ISO 13849 では、電気・電子機器の安全関連システムを対象として、安全度水準を規定する。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。（資料３）

③ 危険側故障には、ランダムハードウエア故障と、系統的故障があるが、安全度水準等は、ランダムハードウエア故障を対象とする。
④ 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、故障による結果の重篤度を減少させるものではない。

＜IEC 61508 による安全度水準＞

① IEC 61508 で規定する安全度水準は、低頻度作動要求モードでは、機能失敗平均確率（PFD）が、高頻度作業要求・連続モードでは、危険側失敗の平均頻度（PFH）によって定義され、モードにより求められる確率が異なる。（資料３参照）
② 安全度水準は、平均危険側故障確率（検知できるもの（λ_{DD}）、検知できないもの（λ_{DU}））、検査インターバル（proof test interval）、平均修理時間（MTTR）、共通原因故障（CCF）によって計算される。（資料３参照）
③ 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の検証が必要。

＜IEC 13859 によるパフォーマンスレベル＞

① ISO 13849 のパフォーマンスレベルは、機械設計を前提に、構造要件（アーキテクチャ）のカテゴリという概念を用いて計算方法を簡易化しており、安全度水準の高頻度モードと互換性がある。
② パフォーマンスレベルは、平均危険側故障確率（MTTF）、診断範囲（DC）、カテゴリ（アーキテクチャー）、共通原因故障（CCF）によって計算される。

＜機能安全の適用範囲＞

① 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。
② 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、インターロック、フェールセーフ、ヒューマンファクターを含めた総合的な技術としての観点が必要である。
③ 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のかという点も検討が必要である。

(3) 検討のポイント

ア　労働災害防止のための機能安全の適用

① 労働災害防止の観点から、機能安全の発現が求められる「作動要求状態」には、具体的にどのような場合が想定されるか。

✧ 低頻度モードの適用例

✧ 機械式安全装置が設置されている機械等

✧ 高頻度モードの適用例

✧ 機械式安全装置が設置されていない（できない）機械等

② 労働災害防止の観点から、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」（同一の故障が、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。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。）には、どのようなものが想定されるか。

(a) センサー（センサー故障単独では安全・危険はわからない）

(b) 論理処理装置（リレー回路、コンピューター制御）

✧ 例：制御ソフトウエアのバグ（どのような出力信号が出るかわからない）

(c) 最終出力装置（アクチュエーターなど）

✧ 例：故障によるボイラー給水バルブの開放（通常は安全側であるが、過熱時の急冷による脆性破壊の恐れ）

✧ 例：故障によるボイラー蒸気供給バルブの開放（ボイラーには安全側だが、プラント全体としてみると、蒸気利用側で危険が発生するおそれ）

✧ 例：制御装置の故障による産業用ロボットの保護停止（通常は安全側であるが、重量物を保持している場合などはロボットの転倒のおそれ）

③ 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等には、何が考えられるか。

✧ 低頻度モードの適用例

✧ 爆発等の重篤度の高い結果をもたらす機械等で、機械式の安全装置を装備しているもの（ボイラー、圧力容器など）

✧ 高頻度モードの適用例

✧ 一定の重篤な結果をもたらす機械等で、機械式の安全装置の装備が困難なもの（人間との協働作業中の産業用ロボット等）

✧ どちらのモードに分類すべきか不明なもの

✧ 保護停止のための電気・電子制御の安全装置（プレス機械の光線式安全装置など）

✧ 緊急停止のための電気・電子制御の安全装置（非常停止ボタンなど）
✧ 機械等の事故の重篤度のレベル分けをする指標（温度、圧力、積載過重、速度等）を制御する装置

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

① 定量的な評価は可能か（労働災害の許容可能リスクの設定は可能か）。

② 定性的評価を行うための留意すべき点は何か

✧ 結果の客観的な予測
✧ 望ましくない事象（作動要求事象）の頻度の特定
✧ 客観的な評価を行うためのチーム評価等
✧ その他必要な留意点はあるか

③ 製造者とユーザーの協働について

✧ 要求される安全度水準の設定には、ユーザーが機械等をどのように使用するかについての情報が必要であり、製造者とユーザーが協働する仕組みが必要ではないか。
✧ 要求される安全度水準の設定は、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、専門的な第三者機関の認証が必要ではないか。

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

① 検査インターバルは、連続運転等を行う必要のある機械等（ボイラーなど）については、短くすることは難しい。

② 制御装置の安全関連システムの検査は、機械等に装備された以降に実施することが難しいケースがあり、事実上、全ライフサイクルを検査インターバルにせざるを得ないケースがある。

２ 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

(1) 概要

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り、代替できる措置の内容について、典型的な機械等について検討する。

(2) 国際規格・法令等

ア 欧州連合（EU）指令関係

① 圧力機器指令（Pressure Equipment Directive, PED: 97/23/EC）

② 圧力容器指令適合規格リスト（2014/C 313/02）

イ 主要国の関係法令（ボイラー関係）

① 労働安全衛生規則（BetrSichV）（独）

② 安全取扱技術ルール（TRBS）2141（独）

③ ボイラー安全取扱指針（HSE BG01）（英）

ウ 関連国際規格

① EN 50156：炉及び附属機器のための電気機器

② EN 12952: 水管ボイラー及び附属設備

③ EN 12953: 丸ボイラー

④ ISO 10218(JIS B8433)：産業用ロボット-安全要求事項

エ 検討会資料

① 機能安全の要求事項を満たす機械等の取扱規制-欧州連合におけるボイラーの事例-（第１回資料５）

② 産業用ロボットの安全規格について（主に安全性能）（第１回資料６）

オ 前回の意見等

＜ボイラーについて＞

① 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、EN）に適合しない機械等は市場に流通できない。適合性の評価は、機械等の危険性に応じて、自己宣言や第三者認証が求められる。

② ボイラーの安全関連システムについては、EN 50156 に整合する必要があり、IEC 61508 の要求安全度水準を満たすか、個別製品規格（C 規格）に適合することが求められている。安全関連システムは、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される必要がある。（安全関連システムの安全度水準の如何を問わず、機械式安全装置の省略は認められていない。資料３参照。）

③ 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おり、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となっている。

＜産業用ロボットについて＞

① 産業用ロボットの製品規格として ISO 10218 が定められており、上位規格として、ISO 12100、ISO 13849-1 に準拠している。

② 制御システムの安全関連部は、主に停止するための回路であり、安全性能を維持できなくなったときの保護停止（インターロック）と人間が危険を察知したときの非常停止の２種類がある

③ 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が、電気・電子制御による監視と保護停止が認められた。

④ 安全関連システムは、ISO 13849-1 で規定するカテゴリ３でのパフォーマンスレベル d を満たすか、IEC 61508 で規定する検査インターバルが 20 年以上で、ハードウエアフォールトトレランス(HFT)が１の安全度水準２に適合するように設計することが求められている。（安全度水準のみならず、構造要件を規定。）

⑤ 安全度水準を満たす安全関連システムを安全適合（safety-rated）と呼ぶ。安全適合は、基本的に自己認証である。

⑥ 人間とロボットの協働作業条件として、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。

＜機能安全の労働災害防止対策への活用方策について＞

① 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ことは難しいので、定性的な手法（リスクグラフ等）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必要がある。

② 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、対象となる機械等によっては、安全関連システムの故障確率を減少しても、リスクは下がらないかもしれない。機能安全によるリスク低減効果を総合的に判断する必要がある。

③ 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り、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。

④ 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。

⑤ 機能安全は、設計段階から導入すべきであり、ユーザーが後付けで行うべきではない。

⑥ 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拡げるためには、設計段階での点検間隔を指定して安全度水準が決まるので、それと矛盾しない範囲でなければならない。

⑦ よい安全装置が付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良いということは認められない。

⑧ 点検頻度の緩和は、代替機能（例：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。

(3) 検討のポイント

ア 事故の結果の重篤度の大きな機械等（ボイラなど）については、従来、機械式の安全装置（安全弁など）が義務付けられており、低頻度モードでの安全関連システムが要求安全度水準を満たしても、省略は認められていない。

① 事故の重篤度が大きい場合は、制御機能の故障確率（頻度）が減少してもリスクが十分に下がらないということか。または、重篤度が高いので、機械式の安全装置の信頼度（危険側故障確率）と電気・電子機器による安全関連システムの多重化による頻度の低減が必要ということか。

✧ 機械式安全装置との並列により、共通原因故障（CCF）の可能性はほぼ皆無となるため、多重化の効果が大きい。

② 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は認められるべきなのか。

✧ 事故の重篤度が大きい機械等は、内包エネルギーが大きいため連続運転になることも多く、検査インターバルを小さくする（危険側事故確率を下げる）ことが難しいケースが多く、高頻度モードの要求安全度水準を満たすことは難しいということか。

✧ ただし、自己診断（セルフテスト）機能などの導入により、危険側事故確率を下げることは可能かもしれない。

イ 事故の結果の重篤度が相対的に低い機械等（産業用ロボットなど）については、機械式の安全装置（囲い、ストッパーなど）を電気・電子制御の安全関連システム（監視・保護停止）により代替することが認められつつある。

① この場合、単なる高頻度モードの要求安全度水準のみならず、構造要件（自己診断（アーキテクチャ）や、冗長性（HFT）な

ど）を要件として課すべきか。

② 機械式の安全装置を電気・電子式の安全関連システムで代替できる基準としては、事故の結果の重篤度以外に何か考えられるか。

ウ 低頻度モードの機械等であっても、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認められている。

① 検査インターバル（proof test interval）との関連性をどうするか（PFD 計算の前提としての検査インターバルの範囲内とするか。）

② 要求安全度水準のみならず、構造要件（自己診断（アーキテクチャ）や、冗長性（HFT）など）を要件として課すべきか。

エ 保護停止装置や緊急停止装置については、一定の頻度での点検が義務づけられているものもある。これら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。

① 事故により後遺障害をもたらす機械等（動力プレス、コンベヤー等）には、安全装置や非常停止装置が義務づけられており、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いる。

② 非常停止装置の設置は義務づけられているが、点検の義務がない機械もある。（産業用ロボット、人力車）

オ 機械等の規制のレベル分けや適用除外を行う指標（温度、圧力、速度、積載荷重等）の制限については、機械的に担保しているケースが多い（例：ボイラーの伝熱面積、無圧ボイラーの大気開放、ゴンドラの床面積に応じた最大積載荷重など）が、一部、電子制御によるものを認めているケースもある（例：加熱蒸気遮断機を設けた場合の圧力容器の適用除外、ボイラー技士資格のレベル分けに関する自動制御ボイラーの伝熱面積の算入の特例。）

① 事故の重篤度が高い機械等でも、規制のレベル分けや適用除外に関する指標の制御で、事故との関連性が低い場合は、機能安全を前提とした電気・電子制御を入れる余地はあるのではないか。

カ 遠隔操作については、一定の自動制御の機能を有する場合に、遠隔操作を認めている場合があるが、点検の頻度等の緩和はない（例：自動制御ボイラーの事業場内遠隔監視室、監視装置に

よる監視。)。

① 遠隔操作を理由として点検間隔等を緩和することができるかについては、通信の機能安全について評価する必要があり、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。

３ 機能安全の安全度水準の第三者認証のあり方

(1) 概要

機能安全の要求水準の設定や、安全関連システムが要求水準を満たしているか等に関する第三者機関の認証内容や、第三者機関の要件について検討する。

(2) 国際規格等

ア　国際規格

① ISO/IEC Guide 65(JIS Q0065)製品認証機関に対する一般要求事項

② IEC 62061(JIS B9961) 機械類の安全性－安全関連の電気・電子・プログラマブル電子制御システムの機能安全

③ IEC 60204:機械類の安全性―機械の電気装置―

④ ISO 13849:機械類の安全性―制御システムの安全関連部

⑤ EN 50156：炉及び附属機器のための電気機器

イ　検討会資料

① 安全に関連する機械等（SIL を含む。）の認証の考え方と審査項目（資料７）

② 欧州における安全に関連する機械等の認証制度・審査概要（資料８）

ウ　前回の意見等

＜機能安全の標準的な認証プロセス＞

① 機能安全の第三者認証は、①導入フェーズ（教育訓練・構想）、②コンセプトフェーズ（書類審査・机上評価）、③メインインスペクションフェーズ、④認証フェーズの４段階で実施する。

② 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。エンジニアの資格制度を活用する場合もある。

③ コンセプトフェーズでは、製造者から安全要求仕様、安全コンセプト等の提出を受け、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）等が適切に実施されているかどうかの評価を実施する。

④ 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、最終報告書を作成する。ハードウエア故障挿入試験（fault insertion test)、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。ユーザー向けのマニュアルも審査する。

⑤ 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い、証明書を発行する。

＜審査の対象となる故障の種類＞

① 審査は、無秩序に発生するランダム故障のみならず、決定論的故障についても対象とする。(特にソフトウエア)

② ランダム故障は、確率的な手法（危険側故障確率）で評価する。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（target of evaluation: TOE）で審査する。

＜認証の対象単位＞

① 認証の対象としては、制御装置や安全コントローラのようなデバイスに対して認証を与えるケースが多い。制御装置等を組み込んだ状態で、機器全体の認証を行う場合もある。

② 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。

③ 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＞

① ISO/IEC による機能安全の認証機関になるためには、各国の認定機関（日本では、日本適合性認定協会：JAB）から、認証機関と認められる必要がある。

② 認証機関になるための要求事項は、ISO/IEC ガイド 65(JIS Q17065)に定められている。具体的には、①組織運営機構、②人的資源、③プロセス、④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る。

③ 現在、JAB に認定された機能安全の認証機関はなく、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。

(3) 検討のポイント

ア 専門的な第三者機関による認証の必要性

① 機能安全の要求水準の設定が適切かどうか、専門的な第三者機関の認証が必要ではないか。

② 安全関連システムが要求水準を満たしているかについて、ユーザーが判断するのは困難なため、専門の第三者機関による認証が必要ではないか。

イ 専門的な第三者機関の要件

① ISO/IEC ガイド 62 の要求事項を満たしている必要があるか

② その他必要な要件はあるか

ウ 機能安全の認証は、以下のプロセスにより行う。

① 導入（教育訓練）

② コンセプト評価（安全要求資料、安全コンセプト、安全方策、故障モード影響分析（FMEA）等の評価）

③ 各種試験等の実施（実機による故障挿入試験、ソフトウエア検査、電気安全試験、環境試験、ユーザーマニュアル、マネジメント監査、最終報告書作成）

④ 認証（最終報告書と安全コンセプトの整合性確認等の総合レビュー、証明書発行）

エ 認証機関の認定

① 誰が第三者機関を認定すべきか

② ISO 等の国際規格における認証機関の認定を得ていればよいか

③ イの要件以外に認定基準は必要か

４ その他

(1) 概要

その他検討すべき事項はあるか。