資料３

# 検討会報告書の骨子案

## 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及び適合のあり方

(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）

(3) これまでの検討会での意見等

ア　機能安全の基本的考え方

① 機能安全では、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（安全な状態）を実現する機能を要求安全機能として定義する。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危険故障確率のレベルを安全度水準やパフォーマンスレベル（以下「安全度水準等」という。）として決定する。

② 設計者は、要求安全機能ごとに、要求される安全度水準等を満たすように、安全関連システムを設計する。

イ　安全機能、電子等制御、安全関連システムの内容

① IEC 61508 や ISO 13849 では、電気・電子・プログラマブル電子制御（以下、「電子等制御」という。）の安全関連システムを対象として、その要求安全機能が、要求安全度水準等を満たすかを評価する。ボイラー等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。（第２回資料３）

② 安全機能には、危険事象を防止するための機能、危害事象によって生じる被害を緩和する機能のいずれもが含まれる（IEC 61508-1: 3.4.1）。安全度は、安全機能を果たす確率（IEC61508-1:3.5.4）であるが、その指標である安全度水準等は、典型的には、安全関連システムの危険側故障の発生頻度を減少させるための指標として扱われ、故障による結果の重篤度を減少させる指標ではない(IEC 61508-5 附属書 C)。（第２回）

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。

ウ　システムの複雑性に応じた機能安全の適用

① 機能安全は、「相反する故障・失敗の潜在危険」がある複雑なシステムにおける安全関連システムに対して、特に必要なものである。相反する潜在危険がない状況（低複雑度システム）における安全関連システムに対しては、安全方策としてフェールセーフを採用することを前提として、要求事項の一部の適用が免除される。（IEC 61508-1: 序文及び 1.2、解説 2.2.4）

② フェールセーフが機能している場合、故障が発生しても、全て安全側故障と見なすことができるが、フェールセーフを電子等制御によって実現している場合、その安全機能に対して安全度水準等が求められる。

エ　IEC 61508 による要求安全度水準への適合方法

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。（第２回資料３参照）

② 安全度水準の指標となる危険側故障確率は、概念的には、安全関連システムが機能していない時間を運転時間（安全関連システムが機能している時間）で除したものであり、平均危険側故障確率（検知できるもの（$\lambda_{DD}$）、検知できないもの（$\lambda_{DU}$））、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）によって数値的に計算される。（第２回資料３参照）

③ 設計者は、異なる方法による多重化による共通原因故障の低減、自己診断による検知できない危険側故障率の減少、検査インターバルの短縮等により、要求安全度水準を達成する。（第２回）

オ IEC 13849 による要求パフォーマンスレベルへの適合方法

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、平均危険側故障確率(MTTF)、診断範囲(DC)、カテゴリ、共通原因故障(CCF)の組み合わせによって決定される。（第１回資料４参照）

② 設計者は、これらの要件を選択することで、要求パフォーマンスレベルを達成する。（第２回）

③ パフォーマンスレベルは、高頻度作動要求モードの安全度水準と対照可能である。（第１回資料４参照）

カ 機能安全の労働災害防止対策への活用の基本的考え方

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 機能安全により、安全関連システムの危険側故障確率を低減させても、重篤度を低減するわけではないため、対象となる機械等によっては、リスクは十分には下がらないかもしれない。

③ リスクを十分に下げるためには、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 プラントのような大きな設備の場合、安全関連システムだけではなく、運転用の制御システム、ヒューマンエラー、避難待避など、深層防護で大きな設計方針を立てて、安全方策を決定し、それでも残るリスクについて、機能安全によってどれぐらい低減させるのか、という考え方が必要である。

⑤ 要求安全度水準等を満たすために安全方策の検討を行う際、単純に危険側故障確率が下がれば良いという訳ではなく、ISO13849-2の安全原則などを踏まえ、構造要件を優先して検討すべきである。

⑥ 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。また、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。

キ 作動要求モードの適用の考え方

① 安全度水準の低頻度作動要求モードは、作動要求の頻度が１年当たり１回以下の場合に適用され（IEC 61508-1: 3.5.16)、その指標である危険側機能失敗確率（PFD）は、作動要求が発生した所定の瞬間における安全機能が実行されない確率（無次元）である（IEC 61508-1: 3.6.17)。

② 安全度水準の高頻度作動要求モード又は連続モードは、作動要求の頻度が１年当たり１回より大きい又は連続の場合に適用され（IEC 61508-1: 3.5.16)、その指標である時間平均危険側故障頻度（PFH）は、指定する期間にわたって、安全関連システムの危険側故障が発生する平均頻度(1/h)である(IEC 61508-1: 3.6.19)。

③ 機械式の安全装置（例：ボイラーの安全弁）の故障が作動要求となる安全関連システムには、低頻度作動要求モードを適用するのが妥当である。

④ 非常停止ボタンのように、使用頻度が１年に１回を下回ることが想定される電子等制御の安全装置の安全関連システムについても同様であるが、非常停止ボタンの安全関連システムが運転用の制御システムから独立していない場合は、高頻度モードの適用が妥当である。

⑤ その他の電子等制御の保護停止装置（プレス機械の光線式安全装置など）の安全関連システムについては、一般的に、高頻度モードの適用が妥当である。

ク ユーザーから設計者への情報提供について

① 要求安全度水準等を決定するためには、機器の設置場所等の情報が必要である。このため、機械の包括指針に基づき、事業者（ユーザー）と製造者双方が連携を図りつつ、リスク分析を実施する必要がある。

② 現実論としては、量産品については、使用条件などをユーザーから得ることは困難であり、一定の仮定をおいてリスク分析を行う必要がある。その場合、取扱説明書等により使用条件の制限や、メンテナンス頻度の指定などを行うことになる。注文して製作するような機器であれば、ユーザーから十分に情報を得た上で設計することになるのではないか。

③ 注文品の場合、ユーザーが使用条件と要求安全度水準等が釣り合わないような要求をしないように、中間に入って調整する安全技術者も必要である。

【骨子案】

(1) 基本的考え方

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した。

(2) 適用

以下の事項は、電気・電子プログラマブル電子制御（以下「電子等制御」という。）により、労働者の就業に係る負傷又は疾病を回避できる状態（安全な状態）を実現する機能（以下「安全機能」という。）による保護方策の決定方法（以下「機能安全」という。）を対象とする。

(3) 機能安全の実施内容

ア 製造者の実施事項

機械等を製造する者（以下「製造者」という。）は、機能安全の実施内容として、次に掲げる事項を実施する。

① 製造者は、リスク解析（HAZOP や FMEA など）を用いて、機械等による労働者の就業に係る危険性又は有害性を特定した上で､それによる負傷又は疾病の発生を回避するために要求される安全機能（以下「要求安全機能」という。）を特定する。

② 製造者は、要求安全機能を実行するシステム（以下「安全関連システム」という。）の信頼性の度合い（以下「安全度」という。）として要求される水準（以下「要求安全度水準等」という。）を決定する。

③ 製造者は、要求安全機能ごとに、要求安全度水準等を満たすように、電子等制御の安全関連システムの要求事項を決定する。

イ 安全機能及び安全度水準等の内容

① 安全機能には、危険事象を防止するための機能、危害事象によって生じる被害を緩和する機能のいずれもが含まれる。

② 安全度は、安全機能の作動要求時に安全機能が実行される確率であり、その水準を表す指標として、安全度水準又はパフォーマンスレベル（以下「安全度水準等」という。）が用いられる。

(4) 労働災害防止のための機能安全の適用に関する留意事項

ア 機能安全は､「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。）がある複雑なシステムにおける安全関連システムに対して、特に必要なものである。

① 例えば、ボイラーの場合、火炎センサーの故障による火炎の未

検出は、着火前工程であれば危険側であり、着火後の工程であれば安全側の故障となる。

イ　相反する潜在危険がない状況（低複雑度システム）における安全関連システムに対しては、安全方策としてフェールセーフを採用することを前提として、要求事項の一部の適用が免除される。

① 例えば、プレス機械の光線式安全装置であれば、全ての故障について機械を停止させることができれば、全て安全側故障となる。

(5) 要求安全度水準等の決定

ア　リスク解析による危険性又は有害性及び危険事象の特定

① 製造者は、機能安全を適切に実現するため、リスク解析により、予見可能な誤使用を含む、労働者の就業に係る危険性又は有害性及びその結果として発生する事象（以下「危険事象」）を全ての運転モードについて特定する。

② 具体的なリスク解析手法としては、故障モード影響分析（FMEA）やハザードオペレーション分析（HAZOP）、フォールトツリー解析（FTA）などがある。

イ　要求安全機能及び安全関連システムの特定

① 製造者は、洗い出された危険事象等を防止するために要求される安全機能を特定する。

② 製造者は、要求安全機能を実現するために必要な電子等制御の安全関連システムを特定する。

ウ　要求安全度水準等の決定

① 製造者は、労働者が危険性又は有害性にさらされる頻度、生ずる負傷又は疾病の重篤度と回避可能性、安全機能の作動が求められる頻度等を用いた定性的評価によって要求安全度水準等の決定を行う。

② 製造者は、評価尺度である頻度や重篤度等について客観的な評価を行うため、複数者による合同評価を実施する必要がある。

③ 要求安全度水準等の決定には、機器の設置場所等の使用条件に関する情報が必要である。このため、機械の包括指針に基づき、事業者（ユーザー）と製造者が連携して要求安全度水準等を決定する必要がある。

④ 安全機能は、その作動が求められる頻度により、必要な安全度水準の基準値が異なる。このため、製造者は、要求安全機能ごとに、作動要求頻度に応じて作動要求モードを適切に選択する

必要がある。

(6) 要求安全度水準等に適合するための設計手法

ア IEC 61508 による要求安全度水準への適合方法

① 安全度水準の指標となる危険側故障確率は、概念的には、安全関連システムが機能していない時間を運転時間（安全関連システムが機能している時間）で除したものであり、平均危険側故障確率（検知できるもの（$\lambda_{DD}$）、検知できないもの（$\lambda_{DU}$））、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）によって数値的に計算される。

② 製造者は、異なる方法による多重化による共通原因故障の低減、自己診断による検知できない危険側故障率の減少、検査インターバルの短縮等により、要求安全度水準を達成する。

イ ISO 13849 による要求パフォーマンスレベルへの適合方法

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、平均危険側故障確率（MTTF）、診断範囲（DC）、カテゴリ、共通原因故障（CCF）の組み合わせによって決定される。

② 製造者は、これらの要件を選択することで、要求パフォーマンスレベルを達成する。パフォーマンスレベルは、高頻度作動要求モードの安全度水準と対照可能である。

ウ 設計方法の決定に当たっての留意点

① 製造者は、事業者（ユーザー）と連携し、設備全体のリスク低減対策を検討する場合、電子等制御の安全関連システムの危険側故障確率の低減だけではなく、運転用の制御システム、ヒューマンエラー、避難待避など、深層防護で大きな設計方針を立てて、安全方策を決定し、それでも残るリスクについて、機能安全による危険側故障率の低減措置を採用すべきである。

② 製造者は、機能安全による危険側故障確率の低減を図る場合、「機械の包括的な安全基準に関する指針」の本質的安全設計方策（ISO13849-2 の安全原則）などを踏まえ、構造要件等を優先して検討すべきである。

③ 製造者は、特定の安全機能について高い安全度水準等を実現できたことにより、他の安全機能の安全度水準等を低下させることは行うべきでない。

(7) 記録

製造者は、製造した機械等に関する機能安全に係る実施事項につい

て、次の事項を記録し、保管する。

ア　リスク解析により特定された要求安全機能及びその機能を実現する安全関連システム

イ　要求案全機能ごとの要求安全度水準等

ウ　要求機能ごとの要求安全度水準等を満たすための安全関連システムの要求事項

## 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）

(3) これまでの意見等

ア 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。

イ　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、電子等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。

ウ　機械式の安全装置の必要性について

① 化学プラントのように重篤な災害が発生するものについては、深層防護、多重防護の観点から、異種の方式の安全装置の設置が求められている。例えば、バネ式の安全弁は、仮に不具合があっても、圧力が高まればいつか開くことが期待されるが、電子等制御の弁の場合、センサーが故障していれば、圧力が上昇しても絶対に開かないという違いがある。

② 機能安全は、危険側故障の確率によって信頼性を担保するが、ある想定に基づく計算であることから、想定外のことが起きた場合には、物理的な構造や機械式の安全装置で安全を担保する必要がある。

③ 電子等制御の安全関連システムについては、センサーの信頼性が重要であるが、例えば、温度センサーについては、高い安全度水準に適合するものがない。この場合、そのセンサーを使った安全関連システムの安全度水準は高くならない。

④ エレベーターやボイラーも、各種安全装置については電子等制御の安全関連システムの安全度水準等を担保するが、最後には機械

式の安全装置の設置が必要となっている。

⑤ 産業用ロボットについては、ロボットの物理エネルギーに関わらず、保護停止装置について、使い勝手をよくするために機械式のものを電子等制御の安全関連システムに代替することが認められてきている。

エ 安全装置の点検頻度について

① 機械式か電子等制御かを問わず、定期的な点検を求められる安全装置とそうでないものがある。

② 事故の重篤度が高いものや、安全装置の信頼度が低いものに定期点検が必要とされているのではないか。

＜遠隔監視＞

① 遠隔監視については、単に機器の状態をモニタリングするだけなのか、モニタリング情報を制御システムに入力して処理するかどうかで、求められる信頼性が大きく異なる。

② 通信機器や通信品質の信頼性の評価を機器の設計者が行うことは難しい。通信エラーを安全側故障とするような安全関連システムの設計を行う方法はある。

オ 制御システムの安全度水準等に応じた試験の省略

① 各種規格への適合性評価を行う際、一定以上の安全度水準を満たす制御装置で制御されている場合、それに関する試験を省略するということが行われている。

② 評価期間が短くなり、製品開発の期間も短くなる利点がある。

【骨子案】

⑴ 基本的考え方

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、代替できる既存の措置の内容について、基本的な考え方を整理した。

⑵ 点検や検査等の頻度について

ア 事故の重篤度の大きな機械等の制御装置

① 事故の結果の重篤度が大きい機械等（ボイラーなど）の制御装置については、資格者による一定頻度の点検等が義務づけられている。

② これら点検等は、制御装置の故障を早期に発見して事故を防止する趣旨であることから、電子等制御の安全関連システムの安全度水準等に応じ、資格者による点検等の頻度を下げることは妥当である。

イ 非常停止装置、安全装置等

① 事故により死亡や後遺障害をもたらす機械等（動力プレス、車両系建設機械、コンベヤー等）には、安全装置や非常停止装置の設置が義務づけられており、作業開始前点検や定期的な点検・検査が義務づけられている。一方、安全装置や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。（射出成形機、軌道装置の人車等）これらの違いは、事故が発生した場合の重篤度や、安全装置等の信頼性の度合いによると考えられる。

② 緊急停止装置等についても、事故による重篤度に応じ、電子等制御による安全関連システムの安全度水準等に応じた規制について、検討する余地がある。

(3) 機械式の安全機能の電子等制御の安全機能への代替

ア 事故の結果の重篤度が相対的に低い機械等の安全機能

① 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、機械式の安全機能（囲い、ストッパーなど）を安全度水準等の高い電子等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国際規格で認められつつある。

② このような機械等について、一定の程度、機械式の安全機能の代替を認めることは可能であるが、電子等制御の安全関連システムについては、単に要求安全度水準等を満たすのみならず、構造要件（アーキテクチャや、冗長性（HFT）など）を要件として課す必要がある。

イ 事故の結果の重篤度の大きな機械等の安全機能

① 事故の結果の重篤度の大きな機械等（ボイラーやエレベーターなど）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、国際規格においても、電子等制御の安全機能が要求安全度水準を満たしても、機械式の安全装置等を代替することは認められていない。

② この理由としては、重篤な災害が発生するものについては、深層防護、多重防護の観点から、異種の方式の安全装置の設置が求められていること、想定外のことが起きた場合には、物理的な構造や機械式の安全装置で安全を担保する必要があることが上げられる。さらに、センサーについて、高い安全度水準に適合することが難しいこともある。

③ これらから、事故の重篤度の大きな機械等については、機械式

の安全機能を電子等制御の安全機能によって代替することは困難である。

ウ　機械等の規制の適用指標に関する制御機能

① 機械等の規制の適用を決める指標（温度、圧力、速度、積載荷重等）に関する制御機器の制限については、機械式の安全機能で担保している例が多い（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）。しかし、電子制御によるものを認めている例（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。）も存在する。

② 事故の重篤度が高い機械等でも、関連する指標（例：温度と圧力）に多重的な安全機能があり、そのうちいずれかが機械式の安全機能で担保されている場合など、事故との関連性が低い場合は、規制の適用を決める指標の制御装置について、一定の安全度水準等を満たすことを前提として、機械式の安全機能に代わり、電子等制御による安全機能を認めることについては検討する余地がある。

(4) 遠隔操作機能への機能安全の活用

ア　遠隔操作に関する現行の規定

① ボイラーなどの機械等では、一定性能を有する自動制御の機能を有するものについて、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。）

② 遠隔監視については、単に機器の状態をモニタリングするだけなのか、モニタリング情報を制御システムに入力して処理するかどうかで、求められる信頼性が大きく異なる。

イ　遠隔制御への機能安全の適用について

① 通信機器や通信品質の信頼性の評価を機器の設計者が行うことは難しい。通信エラーを安全側故障とするような安全関連システムの設計を行う方法はある。

② 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ある。

## 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 17065 製品認証機関に対する一般要求事項

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　これまでの意見等

＜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、必要な場合、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。さらに、機器全体の安全の構想について確認する。

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 による機能安全の適合性評価機関（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 17065 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。

＜認証機関の育成について＞

① ISO でも、認定機関の権限は、一般的に政府に由来するとなっており（ISO/IEC 17000:2.6)、認証機関の育成についても、政府が主導する必要がある。

② ISO に基づく認証機関でなくても、厚生労働省の構造規格に関する登録検定機関による検定は、ある程度、公的な検定として国際的に通用する。機能安全についても同様であろう。

〈機能安全の認証と法令上の位置づけ＞

① 機能安全の認証を行ったとしても、それが法令から独立していると意味がなく、認証を受けた機器の扱いを法令上位置づける必要がある。

② 既存の機器に後付けで安全関連システムの安全度水準を満たす制御ユニットや制御デバイスを設置するケースが多いと思われることから、認証は、制御デバイス単位でできる必要がある。さらに、そのような認証された制御システムを装備している規制対象機器に対して、法令を適用できる仕組みが必要である。

＜機能安全の認証基準、認証機関＞

① 制御デバイス等の機能安全の認証基準を法令上、定める必要がある。基準には、リスク分析に基づく要求安全機能について、要求安全度水準等を満たしていることを盛り込む必要がある。認証基準は、それを装備する機器の構造基準等からは独立し、様々な安全機能に対する安全度水準等を認証できるものとすべきである。

② 機能安全の認証機関については、用途や使用機器を限定せず、様々な安全機能を持つ安全関連システムの安全度水準等を認証できる機関とすべきである。

【骨子案】

⑴ 基本的考え方

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必要性、認証の仕組み、基準、方法や、第三者機関の要件について検討した。

⑵ 専門的な第三者機関による認証の必要性

ア 電子等制御の安全機能について、要求安全度水準の設定が適切になされているかについて、ユーザーが判断することは困難であるため、専門的な第三者機関による認証が必要である。

イ 製品の電子等制御の安全関連システムが要求安全度水準等を満たしているかについても、同様に、専門の第三者機関による認証が必要である。

⑶ 機能安全の認証の法令上の位置づけ

ア 認証基準

① 電子等制御の安全関連システムが、要求安全度水準等を満たしていることを確認するための認証基準を法令上、定める必要がある。

② 基準には、リスク分析に基づき、①要求安全機能が適切に設定されていること、②要求安全機能に対する要求安全度水準等が適切に設定されていること、さらに、③要求安全機能を実現するための電子等制御の安全関連システムが要求安全度水準等を満たしていること盛り込む必要がある。

③ 認証基準は、それを装備する機器の構造基準等からは独立し、様々な安全機能に対する安全度水準等を認証できるものとすべきである。

イ 認証された機器の取扱い

① 認証基準を満たすものとして、認証を受けた制御装置等を有する機械等の取扱について、法令上の特例を規定する。

② 既存の機械等に対して、認証された制御装置等を新たに追加する場合についても、法令上の特例を適用できる仕組みが必要である。

(4) 機能安全の認証の内容

ア 認証のプロセス

① 導入（構想の聴取、必要な教育等）

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）

イ 認証の単位

① 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。

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。

(5) 認証を行う専門的な第三者機関（認証機関）の認定

ア 認定の基本的考え方

① 国際的に、認証機関を認定する権限は、一般的に政府に由来するとなっており、我が国においても、当面、認証機関の認定は、政府が主導する必要がある。

② ISO に基づく認証機関でなくても､厚生労働省の構造規格に関する登録検定機関による検定は、ある程度、公的な検定として国際的に通用する。機能安全についても同様であると考えられる。

③ 認証機関は、用途や使用機器を限定せず、様々な安全機能を持つ安全関連システムの安全度水準等を認証できる機関とすべきである。

④ ISO スキームにおける認証機関になるための要求事項は、ISO/IEC 17065 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。厚生労働省による認証機関の認定についても、ISO スキームの認定基準に準じたものとすべきである。

イ 法令上の仕組み

厚生労働大臣が認証機関を登録（指定）する仕組みについて、次に掲げる事項を厚生労働省令に規定する。

① 欠格事項を定める。
② 登録（指定）基準として、以下の事項を含むものを規定する。
イ）実施管理者に必要な学歴や業務経験等
ロ）認証署名者に必要な学歴や業務経験等
ハ）試験等に必要な機械器具その他の設備及び施設
③ 認証機関の実施義務、業務規定、財務諸表等の備え付け及び閲覧、帳簿の備え付け等の認証機関の義務を定める。
④ 適合命令、改善命令、取り消し、報告の聴取等の履行確保関係の規定を設ける。