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報告書

平成 28 年３月 30 日

目次

Ⅰ　開催要綱及び参集者

１　趣旨

近年、国際規格においては、全使用期間における事故のリスクを許容可能な水準まで抑制するため、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が採用されている。機能安全の性能は、確率的な尺度である安全度水準で評価される。

欧州では、ボイラー等の一定の危険性を有する機械等で使用される電気・電子制御機器について、必要な安全度水準を満たすことが求められるとともに、安全度水準を満たす機器を使用することを前提に、機械等の取扱いに関する規制を見直す動きがある。

本検討会では、一定の危険性を有する産業用の機械等に関して、機能安全の安全度水準に応じた機械等の取扱いに関する規制のあり方について検討する。

２　検討項目

（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
（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
（３）機能安全の安全度水準の第三者認証のあり方
（４）その他

３　構成

（１）本検討会は、厚生労働省労働基準局安全衛生部長が、別紙の参集者の参集を求めて開催する。
（２）本検討会には座長を置き、座長は検討会の議事を整理する。
（３）本検討会の参集者は、必要に応じ追加することができる。
（４）本検討会は、参集者以外の者に出席を求めることができる。

４　その他

（１）本検討会は、原則として公開する。ただし、個人情報、企業秘密情報を取り扱うなどの場合においては非公開とすることができる。
（２）本検討会の事務は、厚生労働省労働基準局安全衛生部安全課において行う。

参集者名簿（五十音順）

池田 博康	（独）労働安全衛生総合研究所 機械システム安全研究グループ　統括研究員
石田 豊	（一社）安全・環境マネジメント協会　会長
梅崎 重夫	（独）労働安全衛生総合研究所 機械システム安全研究グループ　部長
杉田 吉広	テュフラインランド　ジャパン株式会社 産業サービス部　部長
須藤 浩人	（一社）日本ボイラ協会　技術普及部　次長
平尾 裕司	長岡技術科学大学　システム安全専攻　教授
福田 隆文	長岡技術科学大学　システム安全専攻　教授
○向殿 政男	明治大学　名誉教授

○ 座長

オブザーバー

堀 宏行	経済産業省　商務情報政策局　商務流通保安グループ 電力安全課　課長補佐(火力担当)

Ⅱ　検討の経緯

● 第１回　平成 27 年 12 月 24 日（木）　13:30-15:30
- 現状の把握と、論点提示
- 論点に関するフリーディスカッション

● 第２回　平成 28 年１月 25 日（月）　15:30-17:30
- 第１回での質問等への回答
- 論点ごとの検討

● 第３回　平成 28 年２月 26 日（金）15:30-17:30
- 報告書骨子案提示
- 報告書骨子案の検討

● 第４回　平成 28 年３月 24 日（木）15:30-17:30
- 骨子案の議論を踏まえた報告書案の提示
- 報告書案の検討

Ⅲ　機能安全を用いた機械等の取扱規制のあり方

当検討会は、機能安全を用いた機械等の取扱規制のあり方について検討を行い、機械等の製造者が、従来の機械式の安全装置等に加え、新たに制御の機能を付加することによって機械等の安全を確保するために必要な基準について第１に示し、第２において、第１の基準に従い、機能安全で要求される水準を満たした機械等に対する既存の法令上の特例措置について基本的な考え方を整理した。

さらに、第３において、製造された機械等が第１で定める基準に適合することを証明する第三者機関の必要性と証明の仕組みについて検討した。

第１　機能安全の要求安全度水準の設定及び適合に関する基準のあり方

１　基本的考え方

近年、電気・電子技術やコンピュータ技術の進歩に伴い、これら技術を活用することにより、機械（注１）、器具その他の設備（以下「機械等」という。）に対して高度かつ信頼性の高い制御が可能となってきている。このため、従来の機械式の安全装置等（注２）に加え、新たに制御の機能を付加することによって、機械等の安全を確保する方策が広く利用されるようになっている。

第１に示す事項は、「危険性又は有害性等の調査等に関する指針」（平成 18 年３月 10 日指針公示第１号）、「機械の包括的な安全基準に関する指針」（平成 19 年 7 月 31 日付け 0731001 号。以下「包括指針」という。）と相まって、従来の機械式の安全装置等に加え、新たに制御の機能を付加することによって機械等の安全を確保するために必要な基準を示すことにより、機械等の安全水準の向上を図ることを目的としている。

（注１）　機械とは、連結された構成品又は部品の組み合わせで、そのうちの少なくとも一つは機械的な作動機構、制御部及び動力部を備えて動くものであって、特に材料の加工、処理、移動、梱包等の特定の用途に合うように統合されたものをいう。

（注２）　ボイラー又は圧力容器の安全弁、産業用ロボットのストッパー又は柵、プレス機械の安全囲い、コンベアーの覆いなど。

２　適用

第１に示す事項は、新たに機械等に係る電気・電子プログラマブル電子制御（以下「電子等制御」という。）の機能を付加することにより、当該機械等による労働者の就業に係る負傷又は疾病の重篤度及び発生する可能性の度合い（以下「リスク」という。）を低減するための措置及びその決定方法（以下

「機能安全」という。）(注１) を対象とする。

（注１） IEC61508 における機能安全の定義には、電子等制御以外の手段によるリスク低減措置も含まれるが、本報告書においては、電子等制御の有する機能によるリスク低減措置に限定している。

３ 機能安全に係る実施事項

(1) 実施内容

機械等を製造する者（以下「製造者」という。）は、機能安全に係る実施事項を適切に実施するために、次に掲げる事項を実施する。

ア 製造者は、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、それによるリスクを低減するために要求される電子等制御の機能（以下「要求安全機能」という。）を特定する。

イ 製造者は、要求安全機能を実行する電子等制御のシステム（以下「安全関連システム」という。）(注１)(注２) に要求される信頼性の水準（以下「要求安全度水準」という。）を決定する。

ウ 製造者は、安全関連システムが要求安全度水準を満たすために求められる事項を決定し、それに従って機械等を製造する。

(2) 要求安全機能及び要求安全度水準の内容

ア 要求安全機能には、労働者の就業に係る危険性又は有害性の結果として労働者に就業上の負傷又は疾病を生じさせる事象（以下「危険事象」という。）を防止するための機能及び当該事象によって生じる被害を緩和する機能が含まれる (注３)。

イ 要求安全度水準は、要求安全機能の作動が要求された時に、安全関連システムが安全機能を達成する確率であり、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が用いられる (注４)。

（注１） 安全関連システムには、検出部（センサー）等の入力部、論理処理部及びアクチュエータ等の出力部が含まれる。

（注２） IEC 61508-1: 3.4.1 による。なお、安全関連システムは、運転制御システムに組み込まれてもよいとされているが、個別の規格により、安全関連システムが制御システムから独立していることを要求されることが多い。(例：ボイラー等の安全関連システム（EN 50156:Fig.1））

（注３） 安全度は、安全関連システムが安全機能を達成する確率(IEC61508-1:3.5.4)であるが、その指標である安全度水準は、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とはなっていない(IEC 61508-5 附属書 C)。

（注４） IEC 60158 においては、安全度水準 (Safety Integrity Level: SIL)、ISO 13849 においては、パフォーマンスレベル（Performance Level: PL）で規定されて

いる。

４　要求安全度水準の決定

(1) 危険性又は有害性及び危険事象の特定

製造者は、機械等における機能安全を適切に実現するため、リスク解析（注１）により、労働者の就業に係る危険性又は有害性（予見可能な機械等の誤使用を含む。）を特定し、その結果として発生する危険事象を特定する。

(2) 要求安全機能及び安全関連システムの特定

ア　製造者は、特定された危険事象を防止するために要求される安全機能を特定する。

イ　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。

(3) 要求安全度水準の決定

ア　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（注２）、回避可能性及び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の決定を行う（別紙１～４参照。）。なお、個別の製品規格において、安全関連システムの要求安全度水準が指定されている場合は、それに従って要求安全度水準を決定することができる。

イ　要求安全機能は、その作動が求められる頻度（以下「作動要求モード」という。）により、要求安全度水準の基準値が異なる（注３）。このため、製造者は、要求安全機能ごとに、作動要求モードを適切に選択（注４）する必要がある（別紙５参照）。

(4) 要求安全度水準の決定に当たっての留意点

ア　製造者は、評価尺度である頻度、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。

イ　要求安全度水準の決定には、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（機械等の使用者）と製造者が連携して要求安全度水準を決定する必要がある（注５）。

（注１）　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。要求安全度水準は、機械等によるリスクを許容されるレベルまで低減することを目標に設定されるものであり、適切なリスク解析に基づき設定されなければ、その目標を達成することはできない。リスク解析に当たっては、安全関連システムの故障のみならず、予見可能な機械等の誤使用（ヒューマンエラー）を含めて

解析を行う必要がある。

（注２）　重篤度については、負傷や疾病の程度に加え、被災する者の人数も含めた指標とする。（例：IEC 61508-5 附属書 D 表１）（別紙１参照）

（注３）　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)。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)。パフォーマンスレベルは、高頻度作動要求モードを前提としており、高頻度作動要求モードの安全度水準と対照可能である（ISO 13849-1)。

（注４）　例えば、ボイラーの運転制御装置による温度制御が故障した結果として発生する異常圧力上昇という危険事象に対して、要求安全機能として燃料遮断リミッターを設置する場合、リミッターが作動することを要求される場面は、機械式の安全弁が故障していた場合に限られる。このように、機械式の安全装置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。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。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。

（注５）　注文生産機器については、事業者（機械等の使用者）から十分に情報を得た上で設計することになるが、事業者が使用条件と要求安全度水準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（インテグレーター）も必要である。一方で、量産品については、使用条件などを機械等の使用者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。

５　要求安全度水準を達成するための方法

(1) 数値計算による要求安全度水準の達成

ア　要求安全度水準のうち、安全度水準（注１）については、危険事象に至る安全関連システムの故障の確率（以下「危険側故障確率」という。）で表され、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（λ_{DD})、検知できないもの(λ_{DU}))、検査間隔（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。

イ　製造者は、要求される安全度水準を達成できるよう、安全関連システムの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、検査間隔の短縮等について、安全関連システムに関する要求事項として定める（別紙６参照)。

(2) 要件の組み合わせによる要求安全度水準の達成

ア　要求安全度水準のうち、パフォーマンスレベル(注２)については、安全関連システムの構造に係る要件（以下「カテゴリ」という。)、平均危険側故障確率（MTTF)、診断範囲（DC)、共通原因故障の組み合わせによって決定される。

イ　製造者は、要求されるパフォーマンスレベルを達成できるよう、平均危険側故障確率、診断範囲、カテゴリ、共通原因故障について、安全関連システムに関する要求事項として定める（別紙７参照。)。

(3) 設計方法の決定に当たっての留意点

ア　製造者は、事業者（機械等の使用者）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の信頼性の向上、ヒューマンエラー防止対策、避難待避方法の検討など、深層的な防護による大きな設計方針に従い安全方策を検討し、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。

イ　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、包括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。

ウ　製造者は、機械等を譲渡又は貸与される者に対し、包括指針の別表第５に基づく使用上の情報に加え、危険事象の特定の前提となる機械等の使用条件等に関する情報も提供する必要がある。

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

オ　機能安全は、相反する故障・失敗の潜在危険（同一の故障であっても、発生状況の違いにより、安全側故障又は危険側故障となる危険性をいう。)(注３)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(注４)

においては、安全方策としてフェールセーフ（注５）を採用することを前提として、機能安全の要求事項の一部（要求安全機能の特定等）の適用が免除される（注６）。

（注1） IEC61508-6 による。

（注2） ISO13849-1 による。

（注3） 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。

（注4） 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。

（注5） システムにおいて、誤操作・誤動作による障害が発生した場合、常に安全側に制御すること。

（注6） 複雑度が低いシステムにおいてフェールセーフが機能している場合、制御システムにおいて故障が発生しても、全て安全側故障と見なすことができるため、故障に備えた要求安全機能とそれを実現するための要求安全関連システムの要求安全水準の設定を省略できる（IEC 61508-1: 序文及び 1.2)。ただし、フェールセーフがコンピュータ制御の安全機能によって実現している場合、その安全関連システムは、要求安全度水準を満たすことが求められる。

６ 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。

(1) 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

(2) 要求安全機能ごとの要求安全度水準

(3) 要求機能ごとの要求安全度水準を満たすための安全関連システムの要求事項

第２　機能安全の基準を満たす機械等の取扱規制における特例措置のあり方

１　基本的考え方

第２においては、機能安全で要求される水準を満たした機械等に対する特例的な措置に関して、現行の労働安全衛生法令との関連について、基本的な考え方を整理した。

２　点検や検査等の頻度について

(1) 危険事象の重篤度の大きな機械等の制御装置

ア　危険事象により複数の死亡又は後遺障害をもたらすおそれのある機械等（ボイラーなど）(注１)の制御装置等については、資格者による一定頻度の点検等が義務付けられているものがある(注２)。

イ　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(注３)、電子等制御の安全関連システムの要求安全度水準が高くなることに応じ、資格者による点検等の頻度を下げることは妥当である(注４)。

(2) 安全装置、非常停止装置等

ア　(1)と比較して相対的に重篤度が低い機械等であって危険事象により死亡や後遺障害をもたらすおそれがあるもの（動力プレス、車両系荷役運搬機械、コンベヤー等(注５)）には、安全装置や非常停止装置（以下「安全装置等」という。）の設置が義務づけられており、その多くは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(注６)。一方、安全装置等の設置は義務づけられているが、点検の頻度の規定がない機械もある（射出成形機、軌道装置の人車等）(注７)。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。

イ　安全装置等の点検頻度についても、危険事象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要求安全度水準に応じた規制について、検討する余地がある。

（注1）　労働安全衛生法（昭和 47 年法律第 57 号。以下「安衛法」という。）第 37 条で規定する特定機械等（ボイラー、第一種圧力容器、クレーン、移動式クレーン、デリック、エレベーター、建設用リフト、ゴンドラ）を想定している。

（注2）　例えば、ボイラー及び圧力容器安全規則（昭和 47 年労働省令第 33 号。以下「ボイラー則」という。）第 25 条第４号に、ボイラー取扱作業主任者の職務として、「１日１回以上水面測定装置の機能を点検すること」が規定されている。

（注3）　ボイラー則第 25 条の規定は、自動運転中に水面測定装置の機能喪失により、ボイラーの水位が下がりすぎて空焚き状態になる事故（低水位事故）が昭和 40

年代に続発したことへの対策として規定された。

（注4） 欧州では、EU 指令（圧力容器指令、機械指令等）に整合する欧州規格（EN 規格）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。一方、点検等の機械等の運転に関する事項については各国の規制に委ねられている。英国では、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（HSE/CEA: BG01）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、ボイラーの点検の頻度や資格者の配置基準が緩和される仕組みとなっている。

（注5） 例えば、安衛法第 42 条の規定に基づく厚生労働大臣が定める規格又は安全装置が定められている機械等がある。

（注6） 例えば、労働安全衛生規則（昭和 47 年労働省令第 32 号。以下「安衛則」という。）第 125 条（帯のこ盤の送りローラー）、第 131 条（プレス機械及びシャー）、第 151 条（産業用ロボット）、第 151 条の 31（ショベルローダー）、第 151 条の 78（コンベヤー）、第 194 条の 23（高所作業車）、第 229 条（電気機関車）、第 232 条（軌道装置）、第 274 条（化学設備）などがある。

（注7） 例えば、安衛則第 130 条（木材加工用機械）、第 147 条（射出成形機）、第 211 条（人車）などがある。

３　機械式の安全機能の電子等制御の安全機能への代替について

⑴ 危険事象の重篤度の大きな機械等の安全機能

ア　危険事象により複数の死亡や後遺障害をもたらすおそれのある機械等については、従来、安衛法令では、機械式の安全装置（安全弁など）が義務付けられている。また、国際規格においては、電子等制御の安全機能に要求安全度水準を満たすことが求められているが、その場合であっても、機械式の安全装置等を省略することは認められていない（注１）。

イ　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、多重防護の観点から、異種の方式の安全装置の設置（注２）が求められていること、想定外の事象が発生した場合には、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あげられる（注３）。さらに、センサーが高い安全度水準に適合することが難しいこともある。

⑵ 危険事象の重篤度が相対的に低い機械等の安全機能

ア　（１）と比較して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、機械式の安全措置（ストッパー、柵等）を要求安全度水準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（注４）。

イ　安衛法令においても、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を満たすのみならず、構造要件（カテゴリや、冗長性（HFT）など）に留意する必要がある[注5]。

（注1） 欧州においては、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、機械式の安全装置と併せて設置される必要がある。（安全関連システムの要求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。）エレベーターについても同様である。

（注2） 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できるが、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。

（注3） 機能安全は、危険側故障の確率を管理することによって信頼性を担保するが、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を考慮して、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。

（注4） 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。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。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。

（注5） 産業用ロボットの安全関連システムは、ISO 13849-1 で規定するカテゴリが３でのパフォーマンスレベルが 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で安全度水準が２となるように設計することが求められている。

４ 機械等の規制の適用を決める指標の制御に関する機能安全の活用について

(1) 安衛法令では、温度、圧力、速度、積載荷重等の指標が大きくなることに応じ､機械等に適用される規制が厳しくなる仕組みとなっている[注１]。**現行の安衛法令では、機械式の安全弁等により、これら指標が基準値を超えないことを担保している例が多い**[注２]。**しかし、電子制御によるものを認めている例**[注３]**も存在する。**

(2) 事故の重篤度が高い機械等であっても、指標を制御する安全関連システムの故障によるリスクに応じ、一定の要求安全度水準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。

(注1) 例えば、ボイラーについては、最高使用圧力と伝熱面積に応じ、簡易ボイラー、小型ボイラー、ボイラーの順で安全規制の要件が厳しくなる。圧力容器、クレーン、エレベーター等も同様に安全規制の適用のレベル分けがある。

(注2) 例えば、労働安全衛生法施行令（昭和 47 年８月 19 日政令第 318 号）第１条第３号及び第４号による伝熱面積によるボイラーと小型ボイラーの区分、昭和 37 年 12 月 14 日付け基収第 7217 号による大気開放管の設置によるボイラーの適用除外、ゴンドラ構造規格（平成６年３月 26 日労働省告示第 26 号）第９条による作業床の面積に基づく積載荷重の設定などがある。

(注3) 例えば、昭和 37 年１月 12 日付け基発第 20 号による加熱蒸気遮断装置による第一種圧力容器適用除外、ボイラー則第 24 条第２項４号によるボイラー取扱主任者の資格区分に関する自動制御ボイラーの伝熱面積の算入の特例などがある。

５　遠隔操作機能への機能安全の活用について

(1) 遠隔操作及び遠隔監視に関する現行の規定

ア　遠隔からの機器等の監視については、単に機械等の状態のモニタリング（遠隔監視）のみを行う場合、モニタリング情報を制御システムに入力して処理し、機械等の操作（遠隔監視制御）を行う場合等の監視方法の違いにより、求められる信頼性が大きく異なる。

イ　安衛法令においては、ボイラーなどの機械等に対し、一定の自動制御の機能を有する機械等について、一定の要件を満たす遠隔監視室からの監視制御を認めている場合があるが、資格者による機械等に対する点検の頻度等の緩和はない(注１)。遠隔監視については、機械等に自動制御を求めない半面、より高い頻度で機器等の点検を求めている(注２)。

(2) 遠隔制御への機能安全の適用について

ア　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。このため、通信エラーが発生した場合でもそれ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必要がある。

イ　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、通信機器や通信品質の機能安全について評価する必要があり、機械等本体の機能安全とは切り離して議論すべきである。

(注1) 例えば、平成 15 年３月 31 日付け基発第 0331001 号により、一定の要件を満たす自動制御ボイラーについて、遠隔監視室からのボイラーの遠隔操作が認められているが、作業主任者によるボイラー設置場所での水位計の点検（１日１回）等の業務（ボイラー則第 25 条）は義務付けられている。

(注2) 例えば、平成 15 年３月 31 日付け基発第 0331001 号では、ボイラーの遠隔監視を行う場合、ボイラーの設置場所で、４時間に１回以上の点検を行うことを求めている。

６　型式検定等における機能安全の活用について

国際規格においては、その規格への適合性評価を実施する際、一定以上の要求安全度水準を満たす安全関連システムにより温度等が制御されている場合、温度等に関する試験の一部を省略することが行われている。安衛法上の型式検定等においても同様の取扱が可能か検討する余地がある。

第３　機能安全に係る第三者機関による適合性証明のあり方

１　基本的考え方

国際規格においては、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に適合しているか等に関して、第三者機関が適合性を評価する仕組みを取り入れている。第３では、機能安全に対する第三者機関による適合性の証明の必要性、仕組み、基準、方法や、第三者機関の要件について検討した。

２　専門的な第三者機関による適合性証明の必要性

(1) 電子等制御の安全機能について、第１で示した基準により要求安全度水準の設定等が適切になされているかについて、事業者（機械等の使用者）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適合性の証明が必要である。

(2) 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適合性の証明が必要である。

３　機能安全の適合性証明の法令上の位置づけ

(1) 適合性証明のための基準

ア　電子等制御の安全関連システムについて、要求安全度水準が適切に設定され、かつ、その水準が満たされていることを証明するための基準を法令上、定める必要がある（注１）。

イ　基準には、第１に記載されている事項を盛り込む必要がある（注２）。

ウ　基準は、それを装備する機器の構造基準等からは独立し、様々な安全関連システムに対する適合性について証明できるものとすべきである（注３）。

(2) 適合性証明の単位

ア　制御装置や安全コントローラのような機器単位で適合性証明を行う。

イ　同一の型式で量産される機器については、型式ごとの適合性証明も可能とする。

ウ　適合性証明を受けた制御装置等を組み込んだ機械等の全体に機能安全の適合性の証明が必要な場合は、組み込んだ状態で、再度、適合性証明を行う必要がある（注４）。

(3) 適合性が証明された機械等の取扱い

ア　基準を満たすものとして、適合性証明を受けた制御機器等によって制御される機械等の取扱について、特定の機械等ごとに検討の上、可能

な場合には、一定の法令上の特例を規定する。

イ　既存の機械等に対して、新たに適合性証明を受けた制御装置等を新たに設置し、当該機械等を制御する場合についても、同様に法令上の特例を適用できる仕組みが必要である。

(注1) 例えば、安衛法第 28 条第 1 項に基づく技術上の指針が考えられる。

(注2) 基準では、JIS を引用するが、最新の ISO や IEC の規格に基づく適合性証明も可能とする仕組みを設ける。

(注3) 適合性証明にあたっては、要求安全関連システムの要求安全度水準が適切に設定されているかどうかについても審査対象に含まれる。

(注4) コントローラ等の機器単位で要求安全水準が設定されている場合であっても、組み込んだ機械等の制限によってその安全度水準が達成できない場合がある。このため、組み込んだ状態で、再度、要求安全度水準の適合性を証明する必要がある。

4　機能安全の適合性証明の標準的なプロセス

機能安全の適合性を証明する標準的なプロセスは以下のとおりである。

(1) 導入

製造者からの構想の聴取等

(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(注1)、最終報告書作成

(4) 証明書発行

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

(注1) 同一型式による量産品に適合証明を行う場合、定期的に製造者に対するマネジメント監査を実施する必要がある。

5　適合性証明を受けた機械等に対する特例

(1) 基本的考え方

以下の両方に対応できるよう、法令に個別の規定を設ける。

ア　適合性証明を受けた制御装置等を組み込んだ機械等全体として、機能安全の適合性証明が得られている機械等を設置する場合

イ　既存の機械等に、適合性証明を受けた制御装置等を新たに付加する場合

(2) 具体的な規定の例

ア　特定の省令において、特定の機械等の取扱に関する義務規定に、「厚生

労働大臣が定める基準に適合していることを所轄労働基準監督署長が認めた機械等」に対する例外規定を設ける。

イ　労働基準監督署長に対する認定の申請（注１）において、「厚生労働大臣が定める基準に適合していることを厚生労働大臣が指定（登録）する者が明らかにする書面（適合証明書）を添付することができる」ことを規定する（注２）。労働基準監督署長は、提出された適合証明書に基づき、認定を行うものとする（注３）。

（注1）　例えば、ボイラーの場合、落成検査又は変更検査の申請時が想定される。

（注2）　法令上の特例措置を受ける必要がない機械等については、製造者自らが第１の基準に合致することを宣言することも認められる。

（注3）　労働基準監督署長の認定を受けた機械等の制御装置等について、経年劣化で変更する場合の手続きについても定める必要がある。

６　専門的な第三者機関（適合性証明機関）の指定（登録）

(1) 指定（登録）の基本的考え方

ア　ISO においては、適合性評価を実施する機関を認定する権限は、一般的に政府に由来するとされており、我が国においても、当面、適合性の証明を行う機関の指定（登録）は、厚生労働省が行う必要がある（注１）。

イ　適合性証明機関は、制御の対象となる機械等を限定せず、様々な安全機能を持つ安全関連システムの適合性を確認できる機関とすべきである。

ウ　ISO/IEC スキームにおける適合性評価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。厚生労働省による適合性確認機関の指定（登録）についても、ISO/IEC 17065 の基準に準じたものとすべきである。

(2) 法令上の仕組み

厚生労働大臣が適合性証明機関を指定（登録）する仕組みとして、特定の機械等ごとに検討し、可能な場合は、次に掲げる事項を厚生労働省令に規定するべきである。

ア　業務の範囲

５(2)イの特定の機械等における義務規定の特例規定に基づく厚生労働大臣の指定（登録）は、厚生労働大臣が定める基準に適合していることの証明を行おうとする者の申請により行うべきである（注２）。

イ　指定（登録）基準として、以下の事項を含むものを規定するべきである。

① 欠格事項
② 試験に必要な機械器具その他の設備及び施設
電気試験、放射能・放射線試験、機械・物理試験、化学試験、産業安全機械器具試験に必要な機械器具その他の設備を用いて適合性証明を行うこと。(注３)
③ 証明実施者に必要な学歴や業務経験等(注４)
④ 実施管理者に必要な学歴や業務経験等

ウ 適合性証明機関の実施義務
① 適合性証明の審査要求に対する応諾義務
② 証明実施者による審査及び試験
③ 厚生労働大臣の定める基準に適合する方法による適合性評価の実施
④ 審査及び検査による適合性証明実施者の危険の防止

エ 業務規程の定め及び提出
① 適合性証明の実施方法(注５)
② 適合性証明に関する料金及び収納方法
③ 適合性証明を行う時間及び休日
④ 適合証明書の発行
⑤ 適合性証明実施者の選任及び解任並びにその配置
⑥ 適合性証明に関する書類及び帳簿の保存
⑦ 財務諸表等の閲覧請求の費用
⑧ その他必要な事項

オ 各種届け出
① 業務の休廃止の届け出
② 証明書署名者の届け出

カ 財務諸表等の備え付け及び閲覧、帳簿の備え付け等

キ 厚生労働大臣による監督等
① 適合命令
② 改善命令
③ 取り消し
④ 報告の聴取等

(注1) ISO/IEC 17065 に基づく適合性評価機関でなくても、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結果は、ある程度、公的な検定結果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。

(注2) 特例が認められる機械等に応じ、適合性証明の対象を設定する。なお、法令上、適合性証明の業務として規定されていない機械等についても、民間の自主事業として適合性の証明を行うことは妨げられない。

(注3) 適合性証明機関の事務所において必要な試験を実施することを原則とするが、

ISO/IEC 17025 に基づく試験機関の認定を受けている試験機関又はそれと同等の試験機関に試験を委託することも認める方向で検討。

(注4) ISO/IEC 17065 に基づき認定された適合性評価機関に勤務する評価担当者が含まれる。

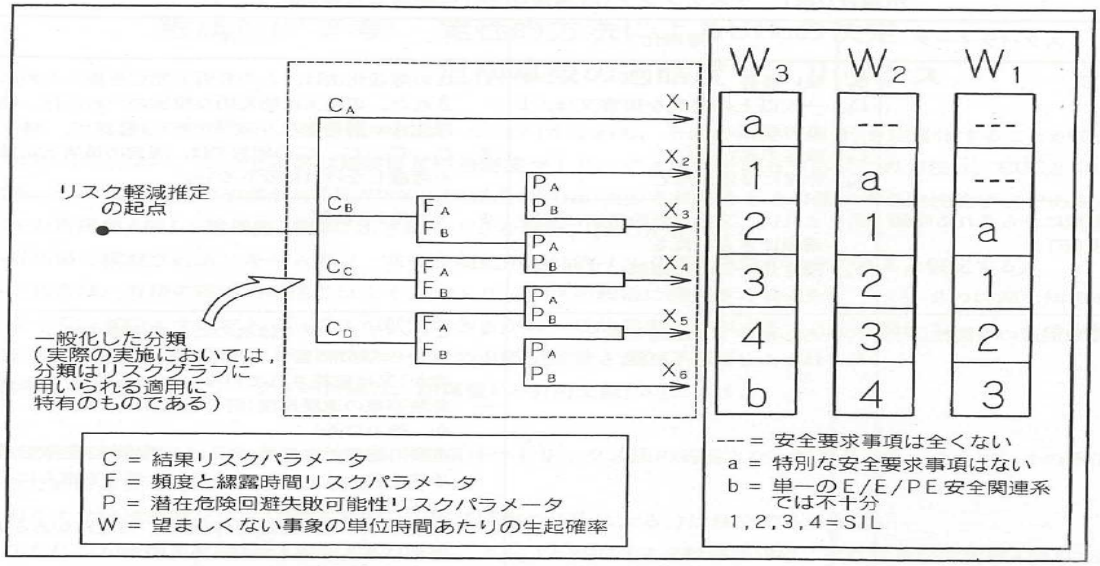
(注5) ４に規定する内容を踏まえる。

Ⅳ　参考資料

資料１　機能安全の概要とその要求水準の設定（第１回委員会資料３）
資料２　安全度水準やパフォーマンスレベルの計算方法（第１回委員会資料４）
資料３　機能安全の要求水準を満たす機械等の取扱規制（第１回委員会資料５）
資料４　産業用ロボットの安全規格について（第１回委員会資料６）
資料５　危険側故障確率の計算方法（第２回委員会資料３）

別紙１

リスクグラフ法による要求安全度水準の決定方法
（IEC61508-5 附属書 D）

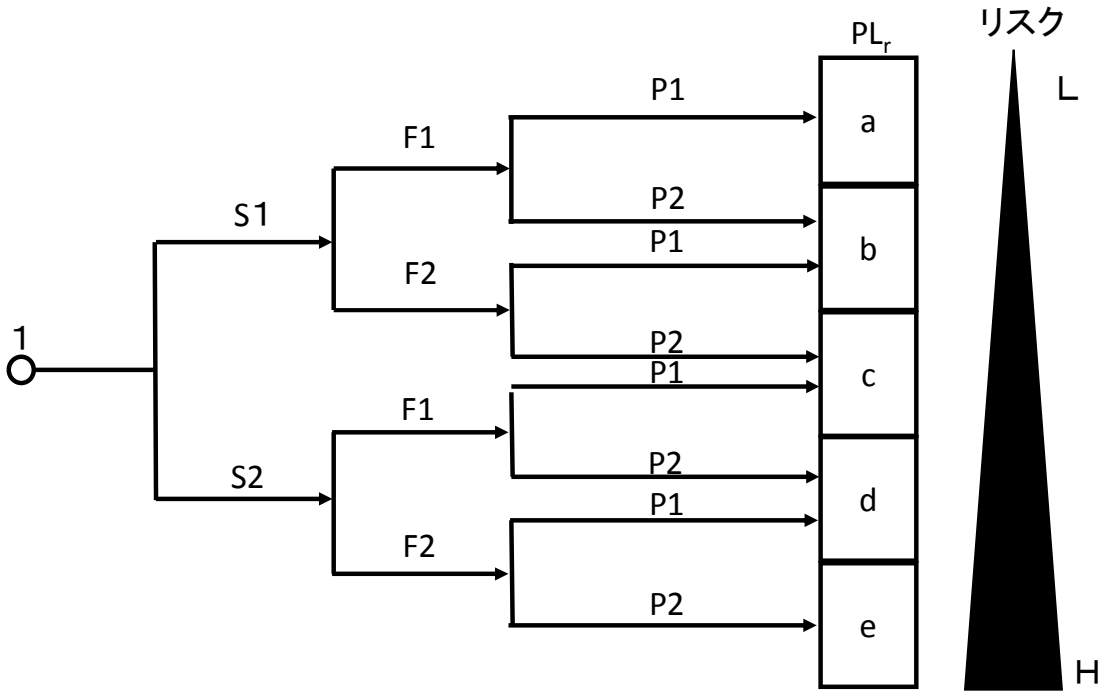


附属書D図1　リスクグラフ：一般的スキーム

結果(C)		曝露頻度(F)		回避可能性(P)		事象発生確率(W)	
C_A	軽傷	F_A	1 日 12 時間以下	P_A	一定程度可能	W_1	非常に低い
C_B	後遺障害	F_B	1 日 12 時間超	P_B	困難	W_2	低い
C_C	死亡					W_3	比較的高い
C_D	複数死亡						

別紙２

リスクグラフ法による要求パフォーマンスレベルの決定方法
（ISO 13849-1 附属書 A）



傷害のひどさ(S)		危険源への暴露の頻度及び／又は時間(F)		危険源回避又は危害の制限の可能性(P)	
S1	軽症（通常，回復可能な傷害）	F1	まれ～低頻度，及び／又はさらされる時間が短い	P1	特定の条件下で可能
S2	重傷（通常，回復不可能又は死亡）	F2	高頻度～連続，及び／又はさらされる時間が長い	P2	ほとんど不可能

別紙 3

マトリクス法による要求安全度水準の決定方法
（IEC 62061 附属書 A）

割り付けられるべき安全度水準（SIL）の求め方として危害のひどさのポイント（**表１**）と危害の発生確率に関するさ 3 要素のポイント（**表２**、**表３**、**表４**）を加算した結果を用いて、**表５**のマトリクスで SIL を求める。

表１　危害のひどさ（*S*e）の分類

障害の程度	危害のひどさのレベル（*S*e）
回復不可能：死亡、目又は腕の喪失	4
回復不可能：手足骨折、指の喪失	3
回復可能：医師の手当てを必要	2
回復可能：応急処置を必要	1

表２　暴露レベル（*F*r）の分類

暴露の頻度及び暴露継続時間から決まる暴露レベル（*F*r）		
暴露の頻度（間隔）	継続時間＞10 分の場合の暴露レベル量	継続時間 10 分未満
1 時間以下	5	
1 時間超、1 日以下	5	4
1 日超 2 週間以下	4	3
2 週間超 1 年以下	3	2
1 年超	2	1

表３　発生確率（*P*r）の分類

発生確率	発生確率の指標
とても高い	5
起こりやすい	4
時々起こる	3
まれには起こる	2
無視できる	1

表４　危険を回避又は限定できる確率（*A*v）の分類

危険を回避又は限定できる確率（*A*v）	
不可能	5
まれには可能	3
かなり可能	1

表５　安全度水準（SIL）割付けマトリクス

危害のひどさ（Se）	クラス（Cl）　Cl=Fr+Pr+Av				
	３～４	５～７	８～１０	１１～１３	１４～１５
4	SIL2	SIL2	SIL2	SIL3	SIL3
3		(OM)	SIL1	SIL2	SIL3
2			(OM)	SIL1	SIL2
1				(OM)	SIL1

(OM)は安全関連電気制御システム（SRECS）以外の方策を推奨することを示す

別紙４

リスク解析による安全機能ごとの要求安全度水準の決定の例
（IEC61508-5 附属書 D の方法による）

キーワード	危険側故障	危険事象	検知方法	要求安全機能	作動要求に関する事項	C	F	P	W	SIL	製造者追加対策	設置者追加対策
蒸気圧力	消費側での蒸気排出の停止	熱交換器での圧力上昇	熱交換器圧力リミッター	リミッターによる熱源のシャットダウン	機械式安全弁の信頼性	C_D	F_A	－	W_1	2		
ボイラー水の水位	給水停止	過熱/空焚き	水位計	水位制御系による熱源シャットダウン	水位低下に対する設計余裕	C_D	F_A	－	W_1	2	水位計に最低水位を明示	水位計の日常点検

別紙５

作動要求モード別の安全度水準の数値(IEC 61508-4)

表 2－安全度水準（SIL）：低頻度作動要求モードで運用する E/E/PE 安全関連系に割り当てられる安全機能に対する目標機能失敗尺度

安全度水準	低頻度作動要求モード運用 （作動要求当たりの設計上の機能失敗平均確率） （PFDavg）
4	10^{-5} 以上 10^{-4} 未満
3	10^{-4} 以上 10^{-3} 未満
2	10^{-3} 以上 10^{-2} 未満
1	10^{-2} 以上 10^{-1} 未満

表 3－安全度水準（SIL）：高頻度作動要求又は連続モードで運用する E/E/PE 安全関連系に割り当てられる安全機能に対する目標機能失敗尺度

安全度水準	高頻度作動要求又は連続モード運用 安全機能の危険側失敗の平均頻度（PFH）［1/h］
4	10^{-9} 以上 10^{-8} 未満
3	10^{-8} 以上 10^{-7} 未満
2	10^{-7} 以上 10^{-6} 未満
1	10^{-6} 以上 10^{-5} 未満

低頻度作動要求モード：安全機能が作動要求だけによって動作し、作動要求の頻度が１年当たり１回以下の場合

高頻度作動要求モード：安全機能が作動要求だけによって動作し、作動要求の頻度が１年当たり１回より大きい場合

連続モード：安全機能が通常運転の一環として被制御機器（EUC)を安全状態に保持する場合

パフォーマンスレベルと安全度水準の関係

パフォーマンスレベル（PL）	安全度水準（SIL） 高／連続作動モード
a	－
b	1
c	
d	2
e	3
－	4

別紙６

危険側故障確率（低頻度モード）の計算方法(IEC 61508-6)

＜基本式＞

$$\mathrm{PFD}_{\mathrm{avg}} = \lambda_{\mathrm{DU}} \times \left(\frac{T_1}{2} + MTTR\right) + \lambda_{\mathrm{DD}} \times MTTR$$

$\mathrm{PFD}_{\mathrm{avg}}$：作動要求当たりの機能失敗平均確率

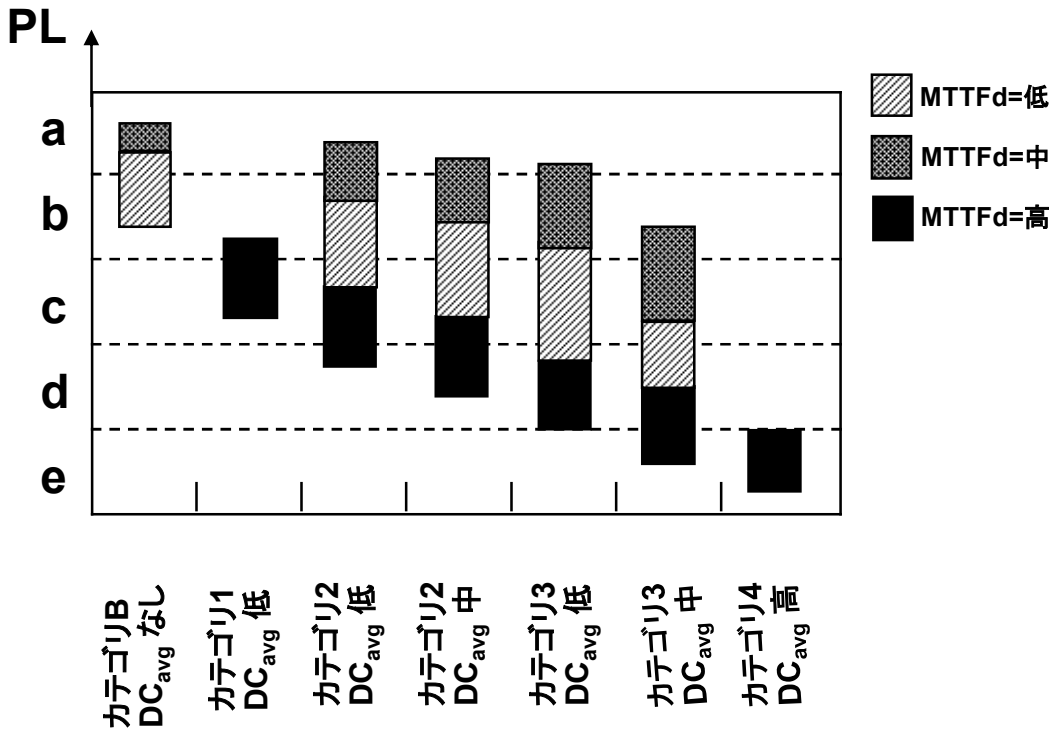
λ_{DU}：検知できない危険側故障確率
λ_{DD}：検知できる故障側確率（故障側確率は、平均故障時間の逆数）
T_1：検査インターバル（proof test interval）
$MTTR$：*平均修理時間*（mean time to repare）

＜考え方＞

- PFD 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**。（安全関連システムが機能しない割合）
- **検知できない危険側故障が発生した場合**、検査するまで機能しないので、**平均すると検査インターバルの半分の時間は機能しない**。それに、修理時間を加えたもの。
- **検知できる故障が発生した場合**は、直ちに修理するので、修理時間だけが機能しない時間となる。

別紙７

パフォーマンスレベルと各設計要素の関係(ISO 13849-1)



MTTFd:安全関連システムの平均危険側故障時間
カテゴリ：安全関連システムの構造的配置、障害検出又はこれらの信頼性を表す指標
DCavg：平均診断範囲