機能安全による機械等に係る安全確保に関する技術上の指針
（平成 28 年厚生労働省告示第 353 号）

1　総則

1－1　趣旨

本指針は、近年、電気・電子技術やコンピュータ技術の進歩に伴い、これらの技術を活用することにより、機械、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中で、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方策が広く利用されるようになっていることを踏まえ、危険性又は有害性等の調査等に関する指針（平成 18 年危険性又は有害性等の調査等に関する指針公示第 1 号）及び機械の包括的な安全基準に関する指針（平成 19 年 7 月 31 日付け基発第 0731001 号厚生労働省労働基準局長通達。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の必要な基準等について規定したものである。

1－2　適用

本指針に示す事項は、新たに機械等に電気・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の可能性の度合い（以下「リスク」という。）を低減するための措置（以下「機能安全」という。）及びその決定方法を対象とする。

2　機能安全に係る実施事項

2－1　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として次に掲げる事項を実施すること。

(1) 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。）を特定すること。

(2) 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。）に要求される信頼性の水準（以下「要求安全度水準」という。）を決定すること。

(3) 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こと。

2－2　要求安全機能及び要求安全度水準の内容

(1) 要求安全機能には、機械等による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危険事象によって生じる被害を緩和する機能が含まれること。

(2) 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当該要求安全機能を作動させることができない確率であり、その水準を表す指標として、国際電気標準会議の規格 61508 の安全度水準又は国際標準化機構

の規格 13849 のパフォーマンスレベルが用いられること。

２－３　実施に当たっての留意事項

製造者は、機能安全に係る実施事項を適切に実施するために、次に掲げる事項に留意すること。

(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ものであり、機械等の運転制御のためのシステムから独立していることが望ましいこと。

(2) 安全度水準又はパフォーマンスレベルについては、国際電気標準会議の規格 61508 若しくは国際標準化機構の規格 13849 の基準又はこれらと同等以上の基準に適合するものとすること。

(3) 機能安全を含む機械等の設計等を行う者に対して、必要な教育を実施するものとすること。

３　要求安全度水準の決定

３－１　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、リスクを解析することにより、労働者の就業に係る危険性又は有害性を特定し、その結果として発生する危険事象を特定すること。

３－２　要求安全機能及び安全関連システムの特定

(1) 製造者は、特定された危険事象を防止するために必要な要求安全機能を特定すること。

(2) 製造者は、要求安全機能を実現するために必要な安全関連システムを特定すること。

３－３　要求安全度水準の決定

(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、危険事象を回避する可能性、要求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こと（別紙１から別紙３まで）。ただし、個別の機械等に関する日本工業規格又は国際規格において、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こと。

(2) 要求安全度水準は、要求安全機能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、その基準値が異なるため、製造者は、要求安全機能ごとに、作動要求モードを適切に決定する必要があること（別紙４）。

３－４　要求安全度水準の決定に当たっての留意事項

製造者は、要求安全度水準を適切に決定するため、次に掲げる事項に留意すること。

(1) 要求安全度水準の評価尺度である危険性又は有害性にさらされる頻度、負傷又は疾病の重篤度等について客観的な評価を行うため、複数の担当者により評価を実施すること。

(2) 要求安全度水準の決定には、機械等の設置場所等の機械等の使用条件に関する情報が必要であるため、包括指針を踏まえ、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こと。ただし、大量に生産される同一型式の機械等については、あらかじめ機械等の使用条件に関する情報を得ることは困難であるため、一定の使用条件を仮定してリスクを解析し、機械等の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等を行うこと。

(3) リスクの解析の実施に当たっては、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）等の手法を実施するものとし、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こと。

(4) 負傷又は疾病の重篤度については、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こと（別紙１）。

(5) 作動要求モードの決定に当たっては、以下の事項に留意すること。

ア　機械式の安全弁の故障時に作動する燃料遮断リミッターのように、機械式の安全装置の故障によって作動が求められる安全関連システムには、低頻度の作動要求モードを適用するのが妥当であること。

イ　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、高頻度の作動要求モードの適用が妥当であること。

ウ　その他の保護停止装置（プレス機械の光線式安全装置等）の安全関連システムについては、一般的に、高頻度の作動要求モードの適用が妥当であること。

４　要求安全度水準に適合するために設計上求められる事項の決定等

４－１　数値計算による要求安全度水準への適合

(1) 要求安全度水準のうち、安全度水準については、危険事象に至る安全関連システムの故障（以下「危険側故障」という。）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安全関連システムが機能している時間で除したもの等であり、平均危険側故障確率（検知できる危険側故障に係る確率（λDD）及び検知できない危険側故障に係る確率（λDU））、検査間隔（proof test interval）、平均修理時間（MTTR）及び共通原因故障（CCF）によって計算されること。

(2) 製造者は、要求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、自動的な診断等による検知できない危険側故障に係る確率の低減、検査間隔の短縮等を安全関連システムに設計上求められる事項（以下「要求事項」という。）として定め、これらに基づいて機械等を製造すること（別紙５）。

４－２　要件の組み合わせによる要求安全度水準への適合

(1) 要求安全度水準のうち、パフォーマンスレベルについては、安全関連システムの構造等に係る要件（以下「カテゴリ」という。）、平均危険側故障時間（MTTFd）、 平均診断範囲（DCavg）及び共通原因故障の組み合わせによって決定されること。

(2) 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、カテゴリ、平

均危険側故障時間、平均診断範囲、共通原因故障等を要求事項として定め、これらに基づいて機械等を製造すること（別紙６）。

４－３　要求事項の決定に当たっての留意事項

製造者は、要求事項を適切に決定するため、次に掲げる事項に留意すること。

(1) 機械等の使用者と連携し、機械等を含む設備全体のリスクを低減するための対策を検討する場合、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、機械等の誤使用（ヒューマンエラー）を防止するための対策、避難待避方法の検討等、多重的な防護による設備の設計方針に従い安全方策を検討し、それでもなお残るリスクについて、機能安全によるリスクの低減を図ることが望ましいこと。

(2) 機能安全によるリスクの低減を図る場合、包括指針の本質的安全設計方策等を踏まえ、機械等の構造要件等を優先して検討することが望ましいこと。

(3) 機械等を譲渡又は貸与する者に対し、包括指針別表第５の使用上の情報に加え、危険事象を特定するため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こと。

(4) 特定の要求安全機能について要求安全度水準を実現できたことにより、他の要求安全機能の要求安全度水準を低下させないこと。

５　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、保管すること。

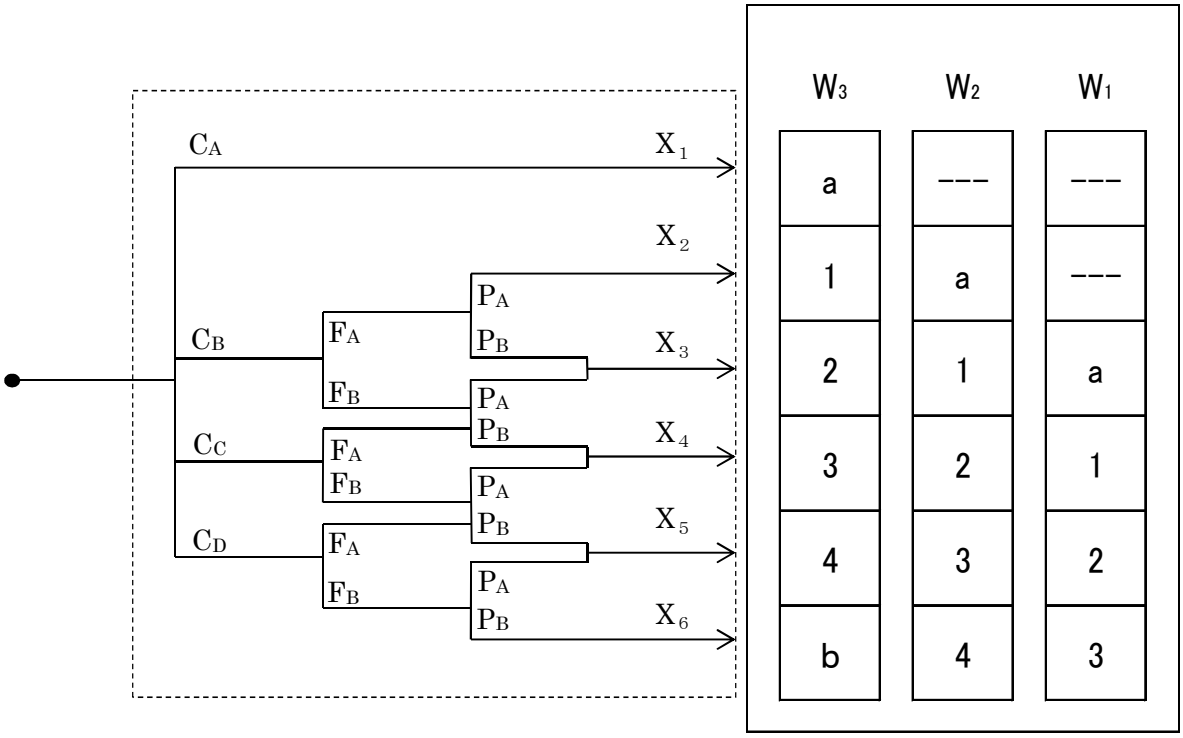
(1) リスクの解析により特定された要求安全機能及び当該要求安全機能を実現する安全関連システム

(2) 要求安全機能ごとの要求安全度水準

(3) 要求安全機能ごとの要求安全度水準を満たすための要求事項

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の例
（国際電気標準会議の規格 61508-5 附属書 D 及び国際標準化機構の規格 13849-1 附属書 A を参考にしたもの）



a:要求安全度水準の設定は必要ない。

b:単一の安全関連システムでは要求安全度水準を達成することはできない。

負傷又は疾病の重篤度(C)		危険性又は有害性へのばく露頻度(F)		危険事象の回避可能性(P)		要求安全機能の作動要求確率(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	高い
C_D	複数死亡						

別紙２

マトリクス法による要求安全度水準の決定方法の例
（国際電気標準会議の規格 62061 附属書 A を参考にしたもの）

適用されるべき要求安全度水準の求め方として、負傷又は疾病の重篤度のポイント（表１）と危険事象の発生確率に関する 3 要素のポイント（表２、表３及び表４）を加算した結果を用いて、表５のマトリクスで要求安全度水準を求める。

表１　負傷又は疾病の重篤度の分類

負傷又は疾病の重篤度	負傷又は疾病の重篤度の指標（*Se*）
回復不可能：死亡又は目若しくは腕の喪失	4
回復不可能：手足骨折又は指の喪失	3
回復可能：医師の手当てが必要	2
回復可能：応急処置が必要	1

表２　危険性又は有害性へのばく露レベルの分類

ばく露の頻度及びばく露継続時間から決まるばく露レベルの指標（*Fr*）		
ばく露の頻度（間隔）	継続時間が 10 分以上の場合	継続時間が 10 分未満の場合
1 時間以下	5	
1 時間を超え、1 日以下	5	4
1 日を超え、2 週間以下	4	3
2 週間を超え、1 年以下	3	2
1 年を超える	2	1

表３　危険事象の発生確率の分類

発生確率	発生確率の指標（*Pr*）
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　危険事象を回避又は危険事象を制限できる確率の分類

回避又は制限できる確率の指標（*Av*）	
不可能	5
まれには可能	3
かなり可能	1

表５　要求安全度水準割付けマトリクス

負傷又は疾病の重篤度の指標（*S*e）	クラス（Cl）　Cl=*F*r+*P*r+*A*v				
	３～４	５～７	８～１０	１１～１３	１４～１５
4	2	2	2	3	3
3			1	2	3
2				1	2
1					1

別紙３

リスクの解析による要求安全機能ごとの要求安全度水準の決定の例
（国際電気標準会議の規格 61508-5 附属書 D を参考にしたもの）

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（注）	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	過熱又は空焚き	水位計	水位制御系による熱源のシャットダウン	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

（注）国際電気標準会議の規格 61508 の安全度水準

別紙４

作動要求モード別の要求安全度水準の数値
（国際電気標準会議の規格 61508-4 を参考にしたもの）

低頻度の作業要求モードで作動する安全関連システムに適用される要求安全機能に対する要求安全度水準の基準値

要求安全度水準	低頻度の作業要求モード(注1)における基準値（要求安全機能の作動が求められた時に、当該要求安全機能が作動しない確率）（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

（注１）要求安全機能の作動が求められる頻度が１年当たり１回以下の場合

高頻度の作業要求モード又は連続モードで作動する安全関連システムに適用される要求安全機能に対する要求安全度水準の基準値

要求安全度水準	高頻度の作業要求モード(注2)又は連続モード(注3)における基準値（要求安全機能に係る危険側故障の平均頻度）（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

（注２）要求安全機能の作動が求められる頻度が１年当たり１回を超える場合
（注３）通常運転の一環として要求安全機能の作動が連続的に求められる場合

国際標準化機構の規格 13849 のパフォーマンスレベル（PL）と国際電気標準会議の規格 61508 の安全度水準（SIL）の関係

パフォーマンスレベル（PL）	安全度水準（SIL）（高頻度の作動要求モード又は連続モード）
a	－
b	1
c	
d	2
e	3
－	4

別紙５

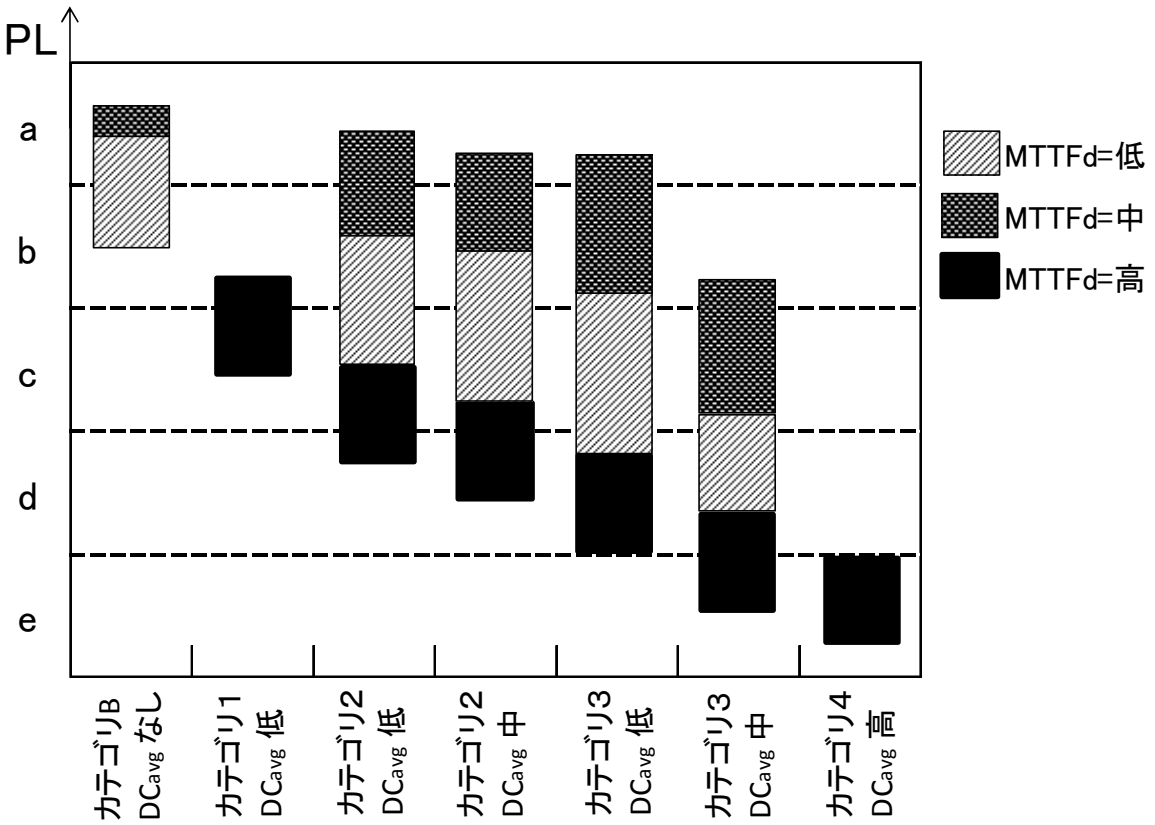
低頻度の作動要求モードにおける要求安全度水準の計算例
（国際電気標準会議の規格 61508-6 を参考にしたもの）

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

$\mathrm{PFD}_{\mathrm{avg}}$：要求安全機能の作動が求められた時に、当該要求安全機能が作動しない確率
λ_{DU}：検知できない危険側故障に係る確率
λ_{DD}：検知できる危険側故障に係る確率
T_1：検査間隔（proof test interval）
$MTTR$：平均修理時間（mean time to repair）

別紙６

パフォーマンスレベルと各設計要素の関係
（国際標準化機構の規格 13849-1 を参考にしたもの）



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等に係る要件
DCavg：平均診断範囲