⑵　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。

⑴　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。

⑵　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。

⑶　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

⑴　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。

⑵　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

⑴　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。

⑵　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。

⑴　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。

⑵　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。

⑶　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。

⑷　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）。

⑸　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

⑴　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。

⑵　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

⑴　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。

⑵　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。

⑴　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。

⑵　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。

⑶　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。

⑷　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。

⑴　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

⑵　要求安全機能ごとの要求安全度水準

⑶　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