機能安全活用テキスト

平成 29 年度厚生労働省委託

機能安全を活用した機械設備の安全対策の推進事業

平成 30 年 3 月

中央労働災害防止協会

はじめに

「機能安全」は比較的新しく誕生した用語であり、欧州電気標準化委員会（CENELEC）において主にプラント設備や鉄道分野で安全制御の観点から議論されてきた。同委員会の SC (Subcommittee) が IEC の SC65A に引き継がれて、IEC 61508 シリーズ（JIS C 0508 シリーズ）が 1998 年に制定されて以降、機械安全分野を始めとして医療機器、家電製品、自動車など広く展開されてきている。その背景には、コンピュータ等電子機器の高信頼化に伴い、これらを用いて安全制御を実現することが可能となってきたこと、機械設備の複合化・複雑化に伴う不具合等への対応のために、システム全体の安全に取り組む必要が生じていることがある。既に、欧州を中心に機能安全の採用が機械システムへの要求事項となりつつあり、機能安全に関する規格に準拠した製品（安全コンポーネント）がコントローラを中心に市販されるようになってきた。

このような状況下で、国内でも機械設備のシステム構築に当たって、機能安全を導入する環境が整いつつある。しかし、機械設備のシステム設計者が機能安全の関連規格を入手しても、必要な安全コンポーネントを選定して、これらを組み合わせて機能安全を実現することは容易ではない。特に、複数の機械設備を統合して設計するシステム統合者(システムインテグレータと呼ぶ)に対しては、参照すべき資料が少なく、また、機能安全を導入した機械設備システムの実施例もまだ多くはない。

そこで、システムインテグレータに対する機能安全の導入、普及を目的として、厚生労働省の「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」において、ボイラーや産業用ロボットへ機能安全の導入可能性が検討され、「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）などの参考資料が作成されている。

本書は、ボイラーと産業用ロボットの制御系の設計者やシステムインテグレータに向けて、機能安全機器を利用する制御システムの設計方法の基礎を指南する。そのため、本書の内容は、機能安全の基礎知識について主眼を置き、ボイラー及び産業用ロボットに対する具体的な設計手法や技術は各々の「機能安全活用実践マニュアル」で説明される。なお、本書は「機能安全の活用促進に関する検討委員会」において作成され、ボイラーと産業用ロボットシステムの制御系の設計者やシステムインテグレータを対象とした 3 日間の指導（トライアル事業）の最初の 1 日間の講義説明を想定している。本書の内容を理解の上でボイラーと産業用ロボットの各マニュアルをご覧いただきたい。

平成 29 年度　機能安全活用テキスト

目次

第１章　機械設備の安全概論

１　機械設備による労働災害の状況

(1) 平成 28 年の労働災害概況

国内の労働災害による死傷者数の推移は、全体的な傾向として緩やかに減少しており、平成 28 年は死亡者数が、1,000 人を下回って 928 人であった（平成 28 年の死傷者数は 117,910 人）。労働災害死傷者数の内訳は、建設業と製造業の合計でほぼ 4 割を占めるが、近年の特徴は第三次産業における死傷災害の割合が増加傾向にある。

一方、全産業の死傷災害の事故型別分類では転倒、墜落･転落、挟まれ･巻き込まれの順に多い（図 1-1）が、製造業に限ると挟まれ・巻き込まれが最も多く、死傷者数では 26.5%、死亡者数では 35.0%を占めており、機械的エネルギーが大きいことから、このような事故の型では重篤な災害に至る可能性が高い。

次に、機械設備に起因する労働災害の死傷者数は全災害の 21.9%（平成 28 年、製造業においては約 4 割）を占めており、依然として多発している。その内訳を見ると、動力運搬機（トラック、フォークリフト等）が最も多く、一般動力機械、金属加工用機械（プレス機械、研削盤等）と続いている。近年の第三次産業の災害増加傾向に合わせて、一般動力機械による災害の約 3 割が食品加工用機械によるものである。

なお、平成 28 年では、ボイラーを起因とする労働災害は 13 件（内 7 件が高温・低温の物との接触）であり、産業用ロボットでは 24 件（内 12 件がはさまれ・巻き込まれ）であった。

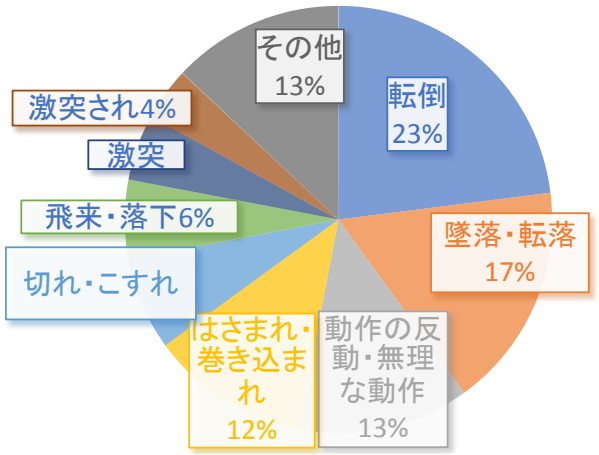


図 1-1　全産業における労働災害の事故の型別分類（平成 28 年死傷）

(2) 産業用ロボットに起因した死亡災害事例

自動車製造業のアルミ鋳造工場において、鋳造ライン内のシリンダーヘッドを搬送す

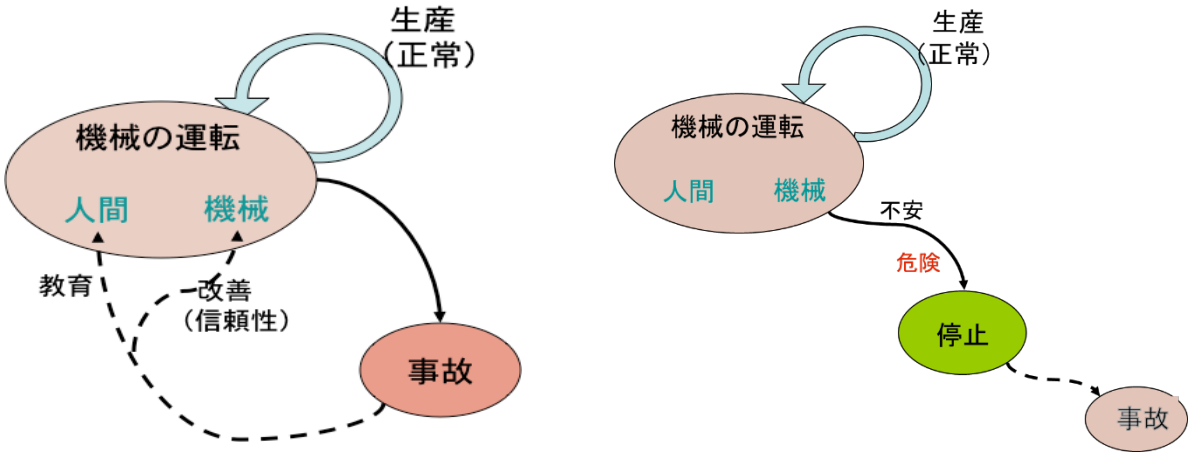
るロボットのクランプに挟まれて死亡した事例[1)]があった。このライン内に立ち入るためには、リミットスイッチ付きのドアを開ける必要があったが、被災者が搬送ロボットの異常を発見してこのドアを開けて立ち入ったときに、ロボットが不意に起動して挟圧された。自動化機械であるロボットが正常作動時には被災者はライン内に立ち入る必要がないが、異常時に近接したときに不意に起動して被災するというパターンは典型的な自動化機械の災害である。

この災害の原因は、被災者が動力源を遮断せずにライン内へ立ち入ったという不安全行動と、ドアを開けるとライン停止するというインタロックが機能しなかったという不安全状態の相乗作用とされた。しかし、インタロック不全が発生してもライン停止に至る仕組みが実現されていれば、たとえ不安全行動があったとしても災害は防げたはずであり、インタロック停止の制御（安全制御）システムの故障を考慮した設計が求められる事例であった。

2　機械設備の安全状態と安全確保

(1)　2つの安全状態

機械設備本来の目的である仕事を行うために、機械自体は正常に機能を発揮して動作し、それに関わる人間は不安なく安全を確保できる。このように、安全状態を維持しつつ機械運転を継続して生産性を向上するのが理想であるが、一度このサイクルから逸脱すると、最悪、事故に至ることになる。事故から生産のプロセスに復帰するためには、機械は修理、改善をし、人間は教育(反省)してリセットすることになる（図 1-2(a)）。しかし、このような事故のフィードバックでは事故の再発は防ぐことはできるが、新しい事故を経験しない限り対策が採れない。そこで、正常な生産サイクルから逸脱しても、事故に至る前にリセットできる段階を準備しておけば、事故を経験せずとも生産のサイクルに戻すことが可能となる。この事故手前の段階は「機械の停止」であり、機械は本来の機能を中止してしまうが、少なくとも人間に危害を及ぼすことはない(図 1-2 (b))。



(a)　事故フィードバック　　(b)　停止の確保

図 1-2　人間-機械系における機械停止の仕組み

(2) 安全関連部によるインタロック

一般に、機械を運転する制御系は目的の仕事を達成するために様々な情報や物理量を処理して、結果的に人間の安全状態が確保される。例えば、ボイラーの燃焼制御や圧力容器の内圧制御が目的の燃焼状態や圧力値を生成していれば関係する人間には危害が及ばず、移動するロボットでは、走行路上の障害物検知によりナビゲーションが成功していれば周囲の人間に衝突することはない。したがって、これらの制御系はなるべく本来の機能を維持できるように、高信頼化設計が指向される。正常な制御機能が維持されている限り、人間の安全も確保できることになる。

しかし、運転のための基本制御系も故障や異常の発生は避けられず、これらの機能不全に対して何らかの措置が必要となる。対象機械が簡単で基本制御系が複雑でなければ、制御の放棄により機械停止に至る仕組みを組み込むことは可能であるが、通常、基本制御系の制御対象は人間ではないため、別途、人間の安全を確保する制御系を用意することになる。この制御は基本制御系をオーバーライドしなくてはならず、たとえ基本制御系が暴走しても機械の運転停止をもたらす機能が求められる。このようなインタロック機能を有する制御系を安全制御系と呼び、通常、基本制御系とは分離して独立で機能させる。これは、インタロック機能の(性能)評価を容易にするためであり、特に、大規模な機械設備では独立性が問われる。

図 1-3 は安全制御系を独立させたシステム構成であり、基本制御系の状態如何によらずインタロックが優先して機能する。このようなインタロックを成す制御部を本書では安全関連システムと呼ぶ（(5) で定義する)。

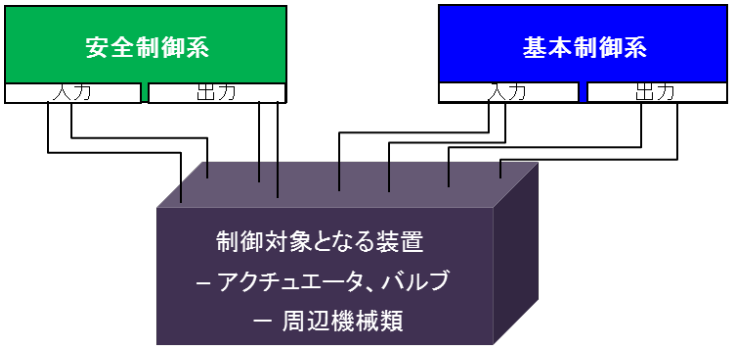


図 1-3　安全制御と基本制御の階層化

(3) 安全関連システムの機能分離

安全制御系におけるインタロック機能は、誤りを含むかもしれない機械運転指令に対して、危険側への誤りのない運転許可が運転出力を支配するという構造が基本である。運転の許可信号は機械の運転状態が安全であることを確認できたときのみ生成され、判断機能を持つ論理積要素（AND ゲート）で論理処理される。したがって、図 1-4 に示

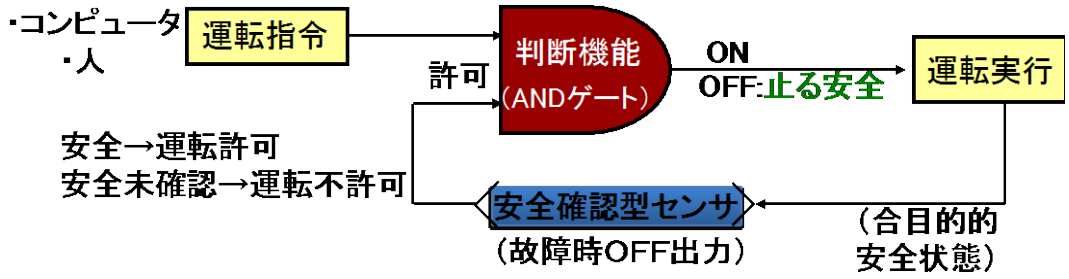


図 1-4　安全確認型インタロック構造

すように、安全確認をするセンサと AND ゲートは少なくとも危険側の誤りを許さない特性（いずれも故障時は OFF となる）が求められる。

運転許可に危険状態を検出して通報するセンサ（危険検出型センサという）を用いる場合は、その出力信号を論理反転しなければならないため、故障時 OFF 出力特性（付加する反転機能を含む）保証が困難とされてきた。すなわち、安全状態を検出して安全情報を生成する手段には故障に対する出力特性が規定され、このような物理的特性はフェールセーフと呼ばれている。図 1-5 のように、安全確認型センサであればセンサ自身の正常性確認が重畳された出力を有する。つまり、正常性が確認できなければ、たとえ安全状態を検出しても安全情報を出力しない。元々、フェールセーフは危険なエネルギー出力がないものとされ、電気的にも本質的にエネルギーが小さいことで証明されていたが、電気信号処理の分野では故障時には著しく安全側に遷移する特性(非対称誤り特性)で実現されている。

同様に、論理積（AND ゲート）演算も、両入力がないにもかかわらず運転出力してはならない特性が要求される。そのため、安全関連システムにおける安全制御の基本構成の考え方は、図 1-6 に示すように非安全関連システムと安全関連システムが独立し、両者の出力条件が揃ったときのみアクチュエータによる出力が発生することである。前述したように、安全関連システムの運転許可部分は安全確認型センサが該当し、この部分は安全確保を担う役割のため、非安全関連システムからハードウェアを分離独立する方が一般的に設計の複雑さやコスト面からも有利と言われる。ただし、同図の AND 機能は安全関連システムの一部であることに注意が必要である。したがって、安全関連の

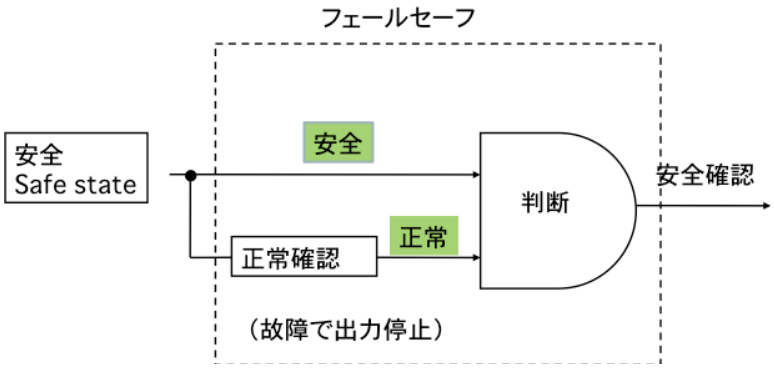


図 1-5　安全確認型センサの出力特性

制御システムには、安全機能を実行するための制御ユニット、人体検知用保護装置等の安全確認型センサ、安全コンポーネント（安全リレーなど）が含まれる。

(4) 安全関連システムへの機能安全の導入

図 1-6 に示すような機械式接点 S1、S2 を有する電磁リレーでインタロックを実現する場合、安全関連システムと非安全関連システムがハードウェアとして分離していたが、これらの接点が電子式装置に置き換わり、ソフトウェアが関与するようになって、分離・独立構造が明確に表せない場合が出てきた。これは、機能安全機器の登場に伴って制御システム全体をフレキシブル化、高機能化するという制御の大きな転換が主流となっていることを示しており、電気・電子・プログラマブル電子制御の付加により安全を確保する「機能安全」の考え方が採用される。ただし、機能安全の導入により、分離独立構造が明確にできない場合が出てきており、混在する制御系も可能となっている。その場合、非安全関連システムの不具合が、少なくとも危険側には安全関連システムに影響しないことを証明する必要がある。安全制御系の安全機能(インタロック)が電気・電子・プログラマブル電子制御の機能により実現される場合、本書の機能安全を用いる安全設計の対象となる。

機械設備の安全とは、「危害を引き起こす恐れがあると思われる危険源から守られている状態」とされる。例えば、ロボットの可動部が隙間を生成する場合、この隙間が人体寸法より狭くならない構造を実現するのが本質安全であり、そもそも挟圧の危険源が除去される。ただし、ロボットの機能を損なわない範囲でのみ実現可能である。ボイラーの場合は爆発に至るエネルギーがない状態が相当する。それに対して、挟圧状態を検出してロボット可動部出力を制御したり、圧力や温度などを基にボイラーの燃焼制御をする方法が機能安全であり、制御（ハードウェア、ソフトウェア）の信頼性によりリスクが評価される。後述するように、危険源自体の抑制ではなく、危険源の危険性の大きさ（リスク）を調節するアプローチが機能安全と言える。そのため、機能安全を用いる安全制御系の設計にはリスクアセスメントが重要な役割を担う。

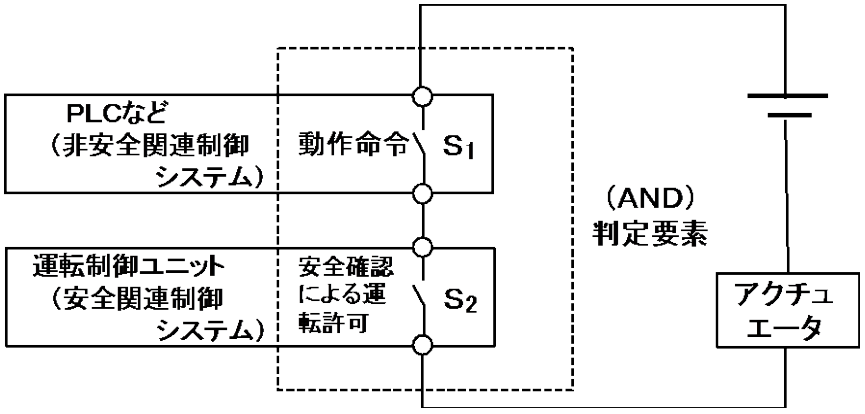


図 1-6　制御システム内の分離と独立

(5) 本書で使用する用語の定義

本書では、以降、機能安全に関する用語について、「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）に記載されている以下の用語を使用する。なお、ここに記載した用語定義と、JIS Z 8051 (ISO/IEC Guide51)および JIS C 0508-4 (IEC 61508-4)の用語定義とは相違する点があるが、本書では、下記の定義を使用する。

(1)リスク

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。

(2)機能安全

新たに機械等に電気・電子プログラマブル電子（E/E/PE）制御の機能を付加することにより、リスクを低減するための措置。

(3)製造者

機械等を製造する者。

(4)安全機能

故障がリスクの増加に直ちにつながるような機械の機能。

(5)危険事象

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。

(6)要求安全機能

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気・電子プログラマブル電子制御の機能。

(7)安全関連システム

要求安全機能を実行する電気・電子プログラマブル電子制御のシステム。
電気・電子プログラマブル電子制御システムの内、安全関連部分に該当する。

(8)安全度水準

安全関連システムの信頼性の水準であり、安全機能を実行するための能力を規定する区分レベルとして、安全度水準 SIL とパフォーマンスレベル（PL）が（JIS B 9705-1）用いられる。

(9)要求安全度水準

安全関連システムに要求される信頼性の水準。
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確率であり、その水準を表す指標として、JIS C 0508 (IEC 61508)の安全度水準又は JIS B 9705（ISO 13849）のパフォーマンスレベルが用いられる。

(10)作動要求頻度

要求安全機能の作動が求められる頻度。

(11)故障(failure)

安全関連システムやそれを構成するサブシステム(要素を含む)に要求機能を実行する能力がなくなること。

(12)ランダムハードウェア故障

ハードウェアの多様な劣化メカニズムから生じてランダムに発生する故障。

(13)決定論的原因故障(systematic failure)

認識や対策の欠如によるヒューマンエラーに至る想定外の故障または失敗。JIS C 0508-4 では systematic failure の邦訳として「決定論的原因故障」と定義しているが、 JIS B 9705-1 では「システマティック故障」としている。

(13)フォールト（fault)

安全関連システムやそれを構成するサブシステム(要素を含む)が、要求機能を実行する能力を低下する、または喪失するような異常状態 。

(14)安全側故障比率(SFF)

サブシステムの全故障の内、サブシステムが危険側故障にならない故障割合。

(15)プルーフテスト

安全関連システムやそれを構成するサブシステム内のフォールトを検出して、必要ならば新品状態に修復する為に実行するテスト 。

(16)共通原因故障(CCF)

1 つ以上の事象に起因する故障。

(17)検証

安全関連システム、サブシステム(要素を含む)が関連仕様書の要求事項に適合することを検査により確認すること。

(18)妥当性確認

安全関連システムが特定アプリケーションの機能安全要求事項を満たすことを検査により確認すること。

上記以外の用語に関しては、JIS Z 8051 (ISO/IEC Guide51)および JIS C 0508-4 (IEC 61508-4)に準じることとする。

参考文献

1)　厚生労働省「職場のあんぜんサイト」（http://anzeninfo.mhlw.go.jp/index.html）

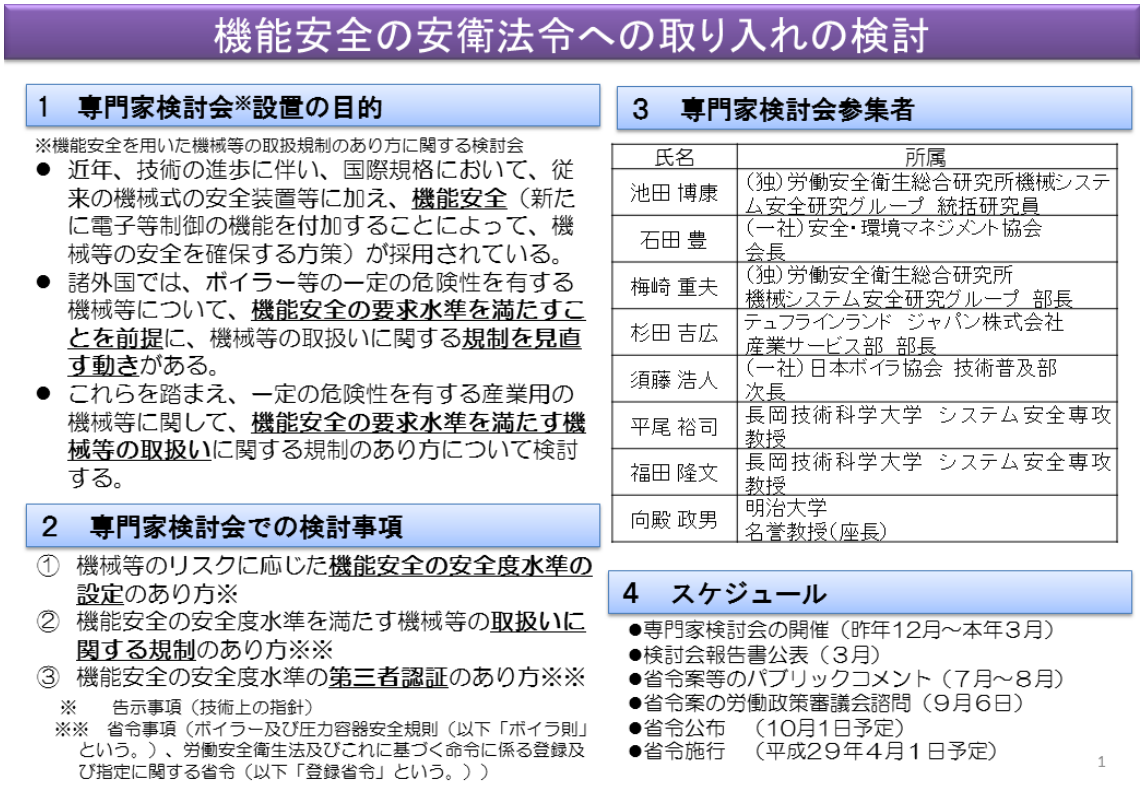
第２章　法令と規格体系

１　関係法令

（１）機能安全の安全衛生関係法令への取りいれ

従来、労働安全衛生法(以下「安衛法」という。)の機械関係の規制は、例えば、産業用ロボットについては、周囲に物理的な柵等を設けること、ボイラーでいえば、ボイラー容器の厚さや安全弁などの物理的な安全方策と、ボイラー技士などの資格者による監視といった人的な安全方策を基本としてきた。一方で、近年のコンピューター制御技術の向上により、非常に信頼性の高い制御が可能となってきており、新たに制御機能を付加することによる安全方策である「機能安全」について、国際規格が定められている。さらに、欧米では、そのような高い信頼性を持つ自動制御装置を装備した機械等に対して、機械等の取扱規制を見直す動きがある。

これらを踏まえ、我が国における、機能安全の基準によって高い信頼性を持つ自動制御装置を備える機械等に対する規制について、専門家によって検討をしていただき、平成 29 年３月に報告書をまとめた。



機能安全の安衛法令への取り入れの検討

１　専門家検討会※設置の目的

※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

- 近年、技術の進歩に伴い、国際規格において、従来の機械式の安全装置等に加え、**機能安全**（新たに電子等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）が採用されている。
- 諸外国では、ボイラー等の一定の危険性を有する機械等について、**機能安全の要求水準を満たすことを前提**に、機械等の取扱いに関する**規制を見直す動き**がある。
- これらを踏まえ、一定の危険性を有する産業用の機械等に関して、**機能安全の要求水準を満たす機械等の取扱い**に関する規制のあり方について検討する。

２　専門家検討会での検討事項

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※※

※　告示事項（技術上の指針）
※※　省令事項（ボイラー及び圧力容器安全規則（以下「ボイラ則」という。）、労働安全衛生法及びこれに基づく命令に係る登録及び指定に関する省令（以下「登録省令」という。））

３　専門家検討会参集者

氏名	所属
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)

４　スケジュール

●専門家検討会の開催（昨年12月～本年３月）
●検討会報告書公表（３月）
●省令案等のパブリックコメント（７月～８月）
●省令案の労働政策審議会諮問（９月６日）
●省令公布　（10月1日予定）
●省令施行　（平成29年４月１日予定）

1

（参考）報告書 URL　http://www.mhlw.go.jp/stf/houdou/0000118662.html

（２）ロボットへの機能安全の適用

ロボットについては、従来、労働安全衛生規則(以下「安衛則」という。)第 150 条の４の

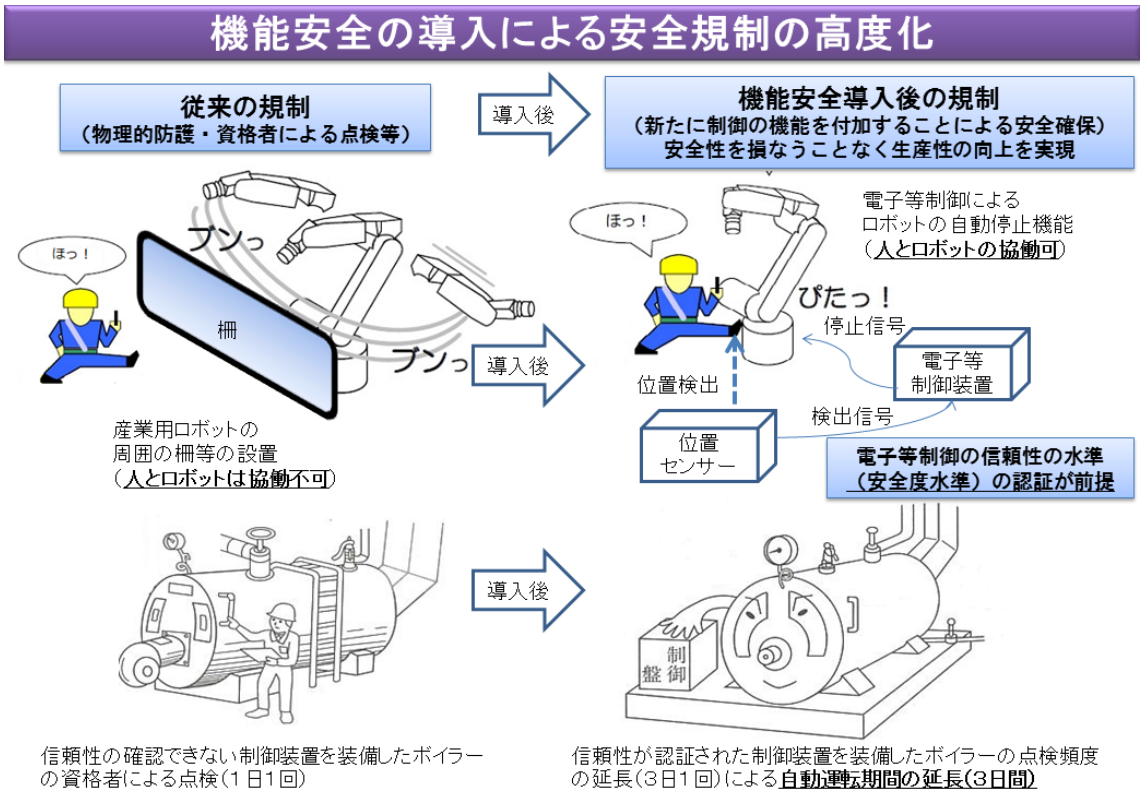
規定により、労働者に危険が生ずるおそれがあるときは、さく又は囲いを設ける等、当該危険を防止するための措置を義務付けている。一方、関係通達（昭和 58 年６月 28 日付け基発第 339 号）の改正により、「さく又は囲いを設ける等」の「等」には、ISO による産業用ロボット規格（ISO10218 シリーズ）により設計、製造及び設置された産業用ロボット（技術ファイル及び適合宣言書を作成しているものに限る。）を、その使用条件に基づき適切に使用することが含まれる、という解釈が示された。

これにより、機能安全を含む適切な安全関連システムを有していることを自己適合宣言した産業用ロボットについては、さく等を設けることなく、労働者と産業用ロボットの協働作業が可能となっている。

（３）ボイラーの取扱規制の改正の趣旨

ボイラーについては、容器の厚さや安全弁といった物理的防護に加え、ボイラー則第 25 条により、ボイラー技士による常時監視や、水面測定装置の機能の１日１回の点検を義務付けている。従来、異常があった場合に自動的にボイラーを停止する「自動停止機能」は設けられているが、その信頼性についての定めは特になく、最後の砦として、ボイラー技士が常時監視し、異常があった場合には、ボイラーを停止させることを前提としていた。

機能安全を導入すれば、自動制御の信頼性である「安全度水準」により、いざというときに自動制御が故障する確率が非常に低いことが定量的に明らかになる。このため、検討会報告書では、そのような証明がされた自動制御装置を装備したボイラーについては、ボイラー技士による常時監視を外すとともに、水面測定装置の機能の点検の頻度を３日に１回とすることが妥当であるとされた。これにより、ボイラー技士の負担軽減と生産性の向上を図ることが可能となる。報告書に基づき、厚生労働省は、ボイラー則等の改正を行った。改正ボイラ則等は、平成 29 年４月１日から施行された。



（４）機能安全指針の制定

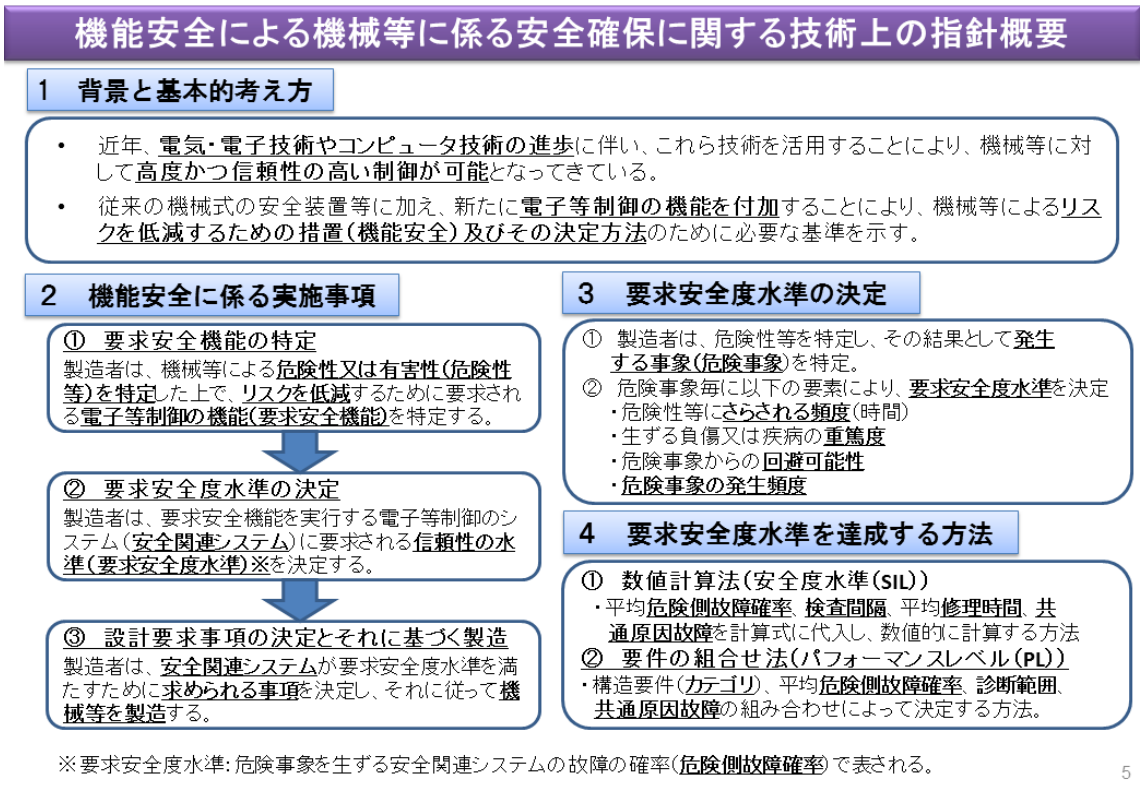
厚生労働省では、機能安全が適切に実施されているかどうかを明らかにするための基準として、「機能安全による機械等に係る安全確保に関する技術上の指針」（平成 28 年厚生労働省告示第 353 号。以下「機能安全指針」という。）を安衛法第 28 条に基づく指針として定めた。機能安全指針では、「機能安全に係る実施事項」として、３ステップが定められている。

まず、「要求安全機能の特定」で、リスクアセスメントを実施し、事故を防止するためにどのような安全機能が必要かを決定する。例えば、ボイラーの場合、空焚きが起きたときに、燃料を遮断するリミッターなどが必要となる。

次に、安全機能を実行する安全関連システムの信頼性の基準である「要求安全度水準」を決定する。指標としては、安全機能が作動に失敗する確率を使用する。

最後に、③の「設計要求事項の決定とそれに基づく製造」で、要求安全度水準のレベルに応じて、作動失敗の確率の基準を満たすことができるように、制御装置を設計し、製造する。

「要求安全水準の決定」については、①事故が起きたときの重篤度、②危険事象からの回避可能性、③危険事象の発生頻度という３点により、レベル別に決定される。「要求安全水準を達成する設計方法」は、例えば、①危険側故障率（パーツが壊れる確率）、②検査間隔、③共通原因故障（システムを多重化していても配電盤がこわれたら全てだめになってしまうような原因）を無くすことなどにより、いざというときに安全機能が作動しない確率を下げていくことになる。



（５）登録適合性証明機関

厚生労働省は、自動制御装置が機能安全指針に適合していることを証明する第三者機関として、登録省令を改正し、「登録適合性証明機関」を新設した。なお、登録証明機関は、ボイラー以外の機械等の電子等制御の機能が機能安全指針に適合していることを証明することも可能である。すでに登録された機関の連絡先については、以下の URL に掲載されている。

http://www.mhlw.go.jp/file/06-Seisakujouhou-11300000-Roudoukijunkyokuanzeneiseibu/0000165299.pdf

登録適合性証明機関の登録及び監督については、以下の規定を登録省令に規定し、厚生労働本省で行っている。

- 登録の方法：登録申請の書類等
- 登録基準：欠格条項、試験で使用する機器、実施管理者の資格、適合性証明員の資格等
- 実施義務：受託義務、適合性証明員による証明、実施方法及びそれに基づく公正な証明、証明書の交付、実施結果報告等
- 業務規程：実施方法、料金、業務時間・休日、帳簿等の保存、財務諸表の謄本請求に係る費用等
- 適合命令及び改善命令
- 登録の取消し　　等

2　規格体系

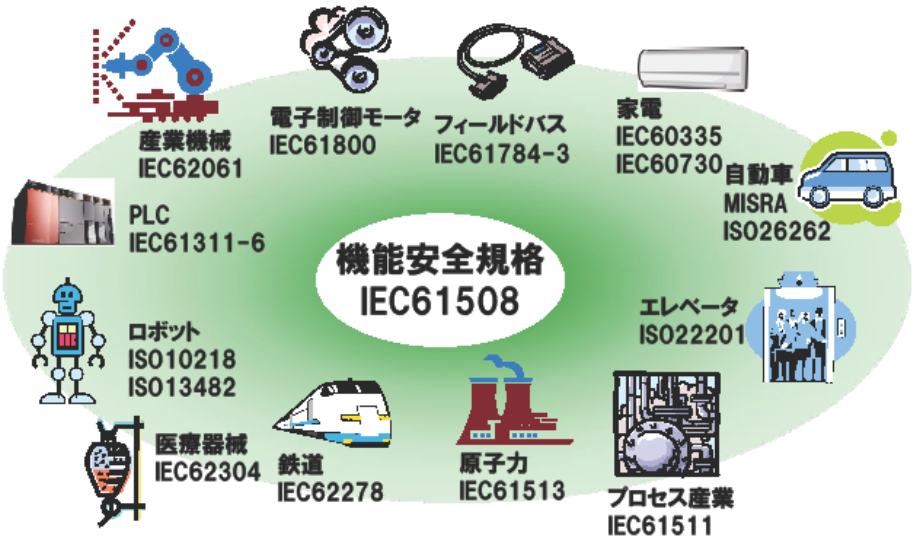


図 2-4　IEC 61508 から派生した主な機能安全規格（三菱電機作成資料）

国際規格（ISO/IEC 規格）において、ボイラー・圧力容器と産業用ロボットを含む機械類間で、それらを構成する部品類（センサーなど）を除き、共通の安全規格は存在しない。一方、機能安全においては、両者共通の規格として IEC 61508 シリーズがあり、この規格はプラント設備やプロセス制御を対象に最初に制定された機能安全規格であるが、近年ではこの規格から派生した各分野の機能安全規格が整備されてきている（図 2-4）。

(1) IEC 61508 シリーズ

IEC 61508 シリーズは、第 1 部から第 4 部までが基本規格、第 5 部以降が、それぞれ第 1 部から第 3 部の内容を補足説明している[2)]。表 2-1 に IEC 61508 シリーズの規格構成を示す。

表 2-1　IEC 61508 シリーズの構成

規格番号	規格タイトル	対応 JIS
IEC 61508-1	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：一般要求事項	JIS C 0508-1
IEC 61508-2	電気・電子・プログラマブル電子安全関連系の機能安全－第 2 部：電気・電子・プログラマブル電子安全関連系の要求事項	JIS C 0508-2
IEC 61508-3	電気・電子・プログラマブル電子安全関連系の機能安全－第 3 部：ソフトウェア要求事項	JIS C 0508-3
IEC 61508-4	電気・電子・プログラマブル電子安全関連系の機能安全－第 4 部：用語の定義及び略語	JIS C 0508-4

IEC 61508-5	電気・電子・プログラマブル電子安全関連系の機能安全－第 5 部：安全度水準の決定方法の例	JIS C 0508-5
IEC 61508-6	電気・電子・プログラマブル電子安全関連系の機能安全－第 6 部：IEC 61508-2 及び IEC 61508-3 の適用の指針	JIS C 0508-6
IEC 61508-7	電気・電子・プログラマブル電子安全関連系の機能安全－第 7 部：技法及び措置の概要	JIS C 0508-7

表 2-1 で示した JIS 規格は、対応する IEC 規格に対して、ISO/IEC GUIDE 21-1:2005 の 4.2 節に規定した最小限の編集上の変更はあるが、技術的内容において一致している。なお、JIS C 0508-5、JIS C 0508-6、及び JIS C 0508-7 は、それぞれ既に廃版となった IEC 61508-5:1998、IEC 61508-6:2000、及び IEC 61508-7:2000 に対応する規格（2016 年 11 月 7 日時点）なので、これらの JIS 参照時は注意が必要である。

IEC 61508 シリーズ各部の概要を以下に示す。

a　IEC 61508-1

・IEC 61508 シリーズの適用範囲と機能安全立証の一般的要求事項を規定する。
・機能安全管理及び機能安全査定の活動を有効に実施するための文書作成の要求事項を規定する。
・機能安全がシステムの全ライフサイクル上で達成すべき要求事項（潜在危険及びリスクの解析、妥当性確認なども含む）を示す。
・附属書で文書の構成事例を記載する。

b　IEC 61508-2

・安全要求事項仕様に適合する電気・電子・プログラマブル電子系のハードウェアを実現するために安全ライフサイクル用で必要な設計と製造上の要求事項を規定。
・附属書で決定論的原因故障、診断カバー率及び安全側故障割合なども解説する。

c　IEC 61508-3

・全安全ライフサイクルにおけるソフトウェアの開発と部分改修、ソフトウェアとハードウェアの統合に関する要求事項などを記載する。
・附属書でソフトウェア技法とその選択の手引き、IEC 61508-1 と IEC 61508-2 との関係についても解説する。

d　IEC 61508-4

・IEC 61508 シリーズで使用される主要な用語とその定義を規定する。また略語も示す。

e　IEC 61508-5

・リスクと安全度の一般概念、リスクモデル（ALARP）及び許容リスクの概念、そして安全度水準（SIL）の決定方法のそれぞれを附属書で例示する。

f　IEC 61508-6

・IEC 61508-2 と IEC 61508-3 の適用方法を附属書としてまとめている。
・ハードウェア故障率の算定例、自己診断率の計算方法と事例、ハードウェアの共通原因故障の扱い方を附属書で示す。
・ソフトウェアの安全度水準（SIL）の適用事例を附属書で示す。

g　IEC 61508-7
・IEC 61508-2 と IEC 61508-3 の要求事項に対する技法と方策をまとめている。

(2) ボイラー・圧力容器に関わる規格

ボイラーの国際規格としては、圧力容器に関する性能基準を規定する ISO 16528 のみ発行されている。各国は、それぞれ独自に発行している圧力容器に関する規格を ISO 規格化させるアプローチがなされている。しかし、ボイラー固有の規格は国際規格には存在せず、各国が独自に制定している。表 2-2 に国内外のボイラーの関係規格、表 2-3 に国内内外の圧力容器の関係規格を示す。

表 2-2　国内外のボイラー関係規格

地域	規格番号	規格のタイトル
日本	JIS B8201	陸用鋼製ボイラー構造
	JIS B8203	鋳鉄ボイラー構造
欧州	EN 12952 シリーズ	水管ボイラー
	EN 12953 シリーズ	丸ボイラー
米国	ASME B&PV Sec.1	ボイラー及び圧力容器基準 セクション 1：動力ボイラー
	ASME B&PV Sec.4	ボイラー及び圧力容器基準 セクション 4：加熱ボイラー

表 2-3　国内外の圧力容器関係規格

地域	規格番号	規格のタイトル
国際規格	ISO 16528-1	ボイラー及び圧力容器　第 1 部:性能要求事項
	ISO 16528-2	ボイラー及び圧力容器 第 2 部:ISO16528-1 の要求事項を満たすための手順
日本	JIS B 8265	圧力容器の構造－一般事項
欧州	EN 13445 シリーズ	圧力容器
米国	ASME B&PV Sec8	ボイラー及び圧力容器基準 セクション 8：圧力容器

(3) 産業用ロボットに関わる規格

機械類の安全に関する規格は、設計原則とリスクアセスメントへの要求事項を示す ISO 12100 を頂点に機械類に共通な安全要求事項を規定するグループ規格、個別製品の安全性要求事項を規定する個別規格に体系付けられている。機械類の 1 つである産業用ロボットは、ISO 12100 とともに関係するグループ規格、そして産業用ロボットの個別安全規格に適合する必要がある。関係グループ規格の体系については図 2-5 に示すが、産業用ロボットの個別規格については「機能安全活用実践マニュアル　産業用ロボットシステム編」の第 2 章で詳述する。

一方、機械類の機能安全に関しては、IEC 61508 シリーズをもとにした IEC 62061 と機械類の安全関連部の安全性を規定した ISO 13849-1 を必要に応じて適用できる（表 2-4 参照）。ISO 13849-1 の運用においては、必要に応じ ISO 13849-2 を参照する。

なお、参考までに本テキスト及びマニュアルで参照すべき規格一覧を附録の表 B-1 に示す。

【注】JIS B 9961 は、2017 年 1 月 1 日時点で、IEC 62061 が Edition 1.2 で修正された内容を反映していない。また JIS 9705-1 は既に失効した ISO 13849-1 の 2006 年版に互換の規格である。従って JIS B 9961 及び JIS B 9705-1 を参照するときは注意が必要である。

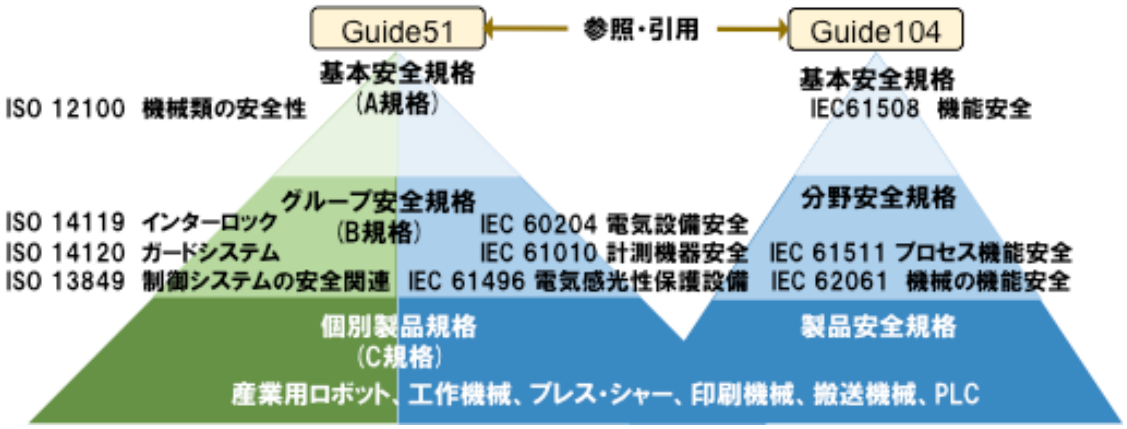


図 2-5　機械安全体系（ISO 及び IEC）

表 2-4　産業用ロボットの安全規格

規格番号	規格のタイトル	対応 JIS
ISO 10218-1	ロボット及びロボット装置－産業用ロボットの安全要求事項－第 1 部：ロボット	JIS B 8433-1
ISO 10218-2	ロボット及びロボット装置－産業用ロボットの安全要求事項－第 2 部：ロボットシステム及び統合	JIS B 8433-2

表 2-5　ロボットが参照する機能安全規格

規格番号	規格のタイトル	対応 JIS
IEC 62061	機械類の安全性－安全関連電気・電子・プログラマブル電子制御系の機能安全	JIS B 9961
ISO 13849-1	機械類の安全性－制御システムの安全関連部－第 1 部：設計のための一般原則	JIS B 9705-1
ISO 13849-2	機械類の安全性－制御システムの安全関連部－第 2 部：妥当性確認	2018 年発行予定 (JIS B 9705-2)

参照文献

１）（参考）報告書 URL　http://www.mhlw.go.jp/stf/houdou/0000118662.html

２）　井上洋一・川池襄・平尾祐司・蓬原弘一：安全の国際規格－制御システムの安全、日本規格協会

第３章　リスクアセスメントとリスク低減

１　リスクアセスメントとリスク低減の概念

(1)　　リスクアセスメントの目的と意義

リスクアセスメントを実施する目的は、機械設備のリスクを許容可能なレベルに低減した安全性の高い機械設備を世の中に提供することを求める社会的要求を背景に、機械設備に潜在する危険源を同定し、論理的な手順を踏みながら客観的にリスクを評価することにある。

またリスクアセスメントは、その結果を活用しリスク低減プロセスの出発点に位置づけられて、リスクアセスメントを出発点として論理的リスク低減プロセスを踏むことにより、残留リスクが明確になり、取扱説明書等で残された危険を機械設備製造者から機械設備使用者に伝えることにより、機械設備使用者側が実施するリスクアセスメントのベースとなり、機械設備使用者側におけるリスク低減に貢献できる。

更に、リスク低減方策を含むリスクアセスメントの記録は、欧州機械指令ではテクニカルドキュメントとして保管が義務付けられており、設計者のリスク低減に関する思考過程を明確にし、ステークホルダーに対する説明責任を果たす上で重要なものとなる。

リスクアセスメントにおいてはその実施時期が重要である。設計完了後又は試作完了後では、往々にして本質的安全設計が適用しにくく、安全防護方策などに依存せざるを得なくなり、事後処理的な対応では安全はコストがかかるという考えを生むことになる。構想設計、機能設計、詳細設計と各設計の段階でリスクアセスメントを実施することにより、適切な保護方策が可能になり、ひいてはコストミニマムでリスク低減が可能になる。

(2)　　リスクアセスメントの効果

リスクアセスメントに基づくリスク低減プロセスを実施することにより、機械設備使用者におけるメリットだけでなく機械設備製造者においても種々の恩恵が期待できる。以下にその主なものを列挙する。

ア　直接的効果

― 全ての危険源に対し漏れなく保護方策が適用できる。
― リスク対策の優先順位が決まり、選択的対応が可能になる。
― リスクの大きさに対応した合理的な保護方策が実施できる
― リスクの対象が明確になり、機械設備使用者に則した保護方策が実施できる。
― 機械安全の思考過程が明確になり、第三者の理解が容易になる。
― 国際的な機械安全と整合性が取れる

イ　間接的効果

― 安全性の高い機械設備を提供することにより企業イメージの向上が図れる。
― 安全性の差別化による競争力の向上が図れる。
― 安全に力を入れている大手企業へ、販路が広がったとの実例が報告されている。
― リスクベースの経営的判断が可能になる。
― 製造物責任予防として経営リスクの低減が図れる。
― 製造物責任防衛としてのドキュメンテーションが確立できる。
― 最適設計によるコスト低減

(3) リスクと安全

ア “安全”とは

ある辞書によれば“安全”とは“①安らかで危険がないこと、②物事が損傷したり、危害を受けたりするおそれがないこと”とされており、多くの人はこの定義に納得するであろう。果たした“安全”とはこの様な定義でよいのだろうか？

例えば、硬貨(コイン)を考えてみる。通常の使用、いわゆる買い物で使用している限りでは“危険がある、危害や損害を及ぼす”とは考え難く“安全”ということになる。しかしながら、幼児が誤飲すれば窒息の恐れもあり、金属アレルギーの人、特にニッケルアレルギーにある人にとっては 50 円硬貨や 100 円硬貨は皮膚炎などを引き起こす恐れのある有害物質にもなり得る。更に悪意を持った使い方をすれば、車の塗装を傷つける、つまり損害を与えることも可能である。

道路において信号のある横断歩道を利用する場合、“歩行者用信号が青になったので道路を渡る”という行為は、法律(青信号＝進行することができる)に基づく判断のほか、“歩行者用信号が青ということは、車両用信号は赤なので車は停止する。したがって、横断中に車にはねられることは無い”、つまり“危険がない、危害を受けるおれがない”との判断にも基づくものである。しかしながら、信号無視をする車や信号機の故障により車両用信号機と歩行者用信号機が同時に青になり車が止まらずにひかれる可能性はゼロではない。

同じく信号のある横断歩道では、歩行者用青信号が点滅していたり、青から赤に変わった直後でも横断を開始するケースを多く見かける。彼らの中には、車にひかれる可能性がある程度あることは認識しているが、“車が止まる、避ける、あるいは発進しない。または自分が走って渡れば大丈夫”、つまり“危険、危害や損害”を回避できるので“安全”であると判断している人も多いのではないだろうか。

いずれの例においても“危険はあり、危害を受けるおそれはある”にも関わらず“安全”と判断している。これは、どんな物事でも意図する／しないに関わらず使い方を誤ったり、故障したり、あるいは未知や不測の事象により危害や損害を及ぼすことがあり得る中で、“特定の条件下で危害や損害の①可能性はかなり低く無視できる、②可能性を認識していない、③可能性はあるが回避できる”のいずれかの判断をした時、“安全”としているからである。

イ 産業機械における“安全”の概念

安全側面に関する事項を規格に盛り込む場合の指針である ISO/IEC ガイド 51 では“安全”を次のように定義している。

> 安全（safety）：
> 許容不可能なリスクがないこと。（freedom from risk which is not tolerable.）

“安全”とは、“許容不可能なリスクがないこと”であり、いくらかのリスク(危害や損害を受ける可能性)は残ることを前提としている。“許容不可能なリスクがないこと”は逆に言えば、“すべて許容可能なリスクであること”となり、“許容可能なリスク”とは以下のように定義されている。

> 許容可能なリスク（tolerable risk）：
> 現在の社会の価値観に基づいて、与えられた状況下で、受け入れられるリスクのレベル
> level of risk which is accepted in a given context based on the current values of society

この定義によれば、安全とは“現在の社会の価値観に基づいて、与えられた状況下で、受け入れらないリスクがないこと”または、“現在の社会の価値観に基づいて、与えら

れた状況下で、全てが受け入れ可能なリスクであること”となる。つまり、“安全”とは絶対的なものではなく、国や地域(文化、経済)、時代(技術進歩)により異なるものである。図 3-1 に概念図を示す。

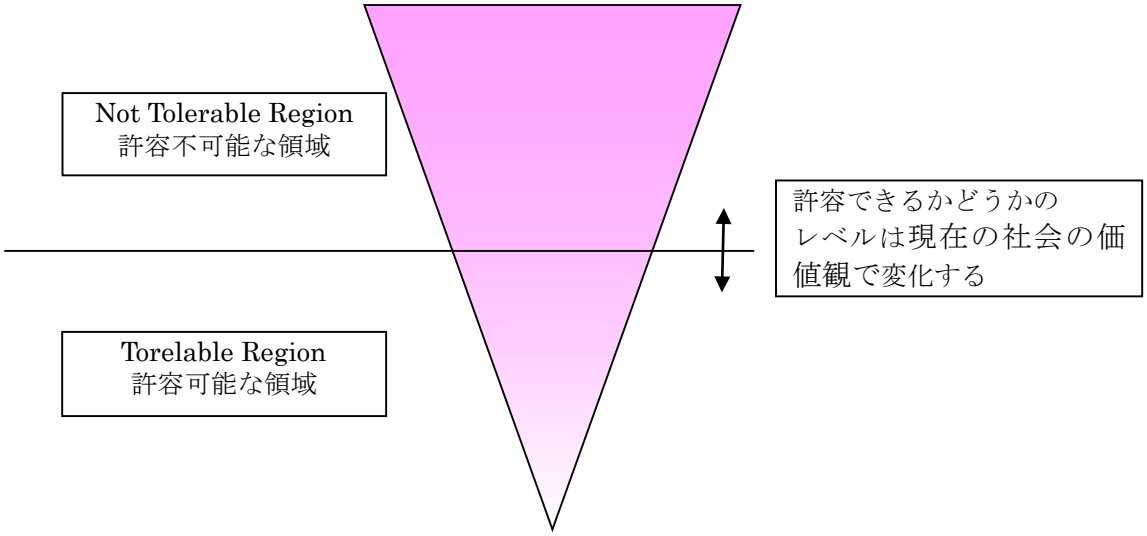


図 3－1　リスク評価の概念

ウ　現在の日本の社会における許容可能・不可能なリスクレベル

前述の概念に基づき、どこまで“許容可能”で、どこからが“許容不可能”かを考えてみる。現時点では、産業機械分野において明確に“許容(不)可能”は定義されていないが、『危険性又は有害性等の調査等に関する指針』[1)](以下「指針」という。)本文や解説、別添 4 にある“リスク見積り方法の例”を読み解くと、表 3-1 となる。

表 3-1　指針、解説及び別添 4 による評価の解釈

重篤度と可能性に組合せ	リスクへの対応	評価
僅かでも死亡災害や身体の一部に永久損傷を伴う可能性がある 休業災害の可能性が高い	直ちにリスク低減措置を講ずる必要がある。 措置を講ずるまで作業停止する必要がある。 十分な経営資源を投入する必要がある。	許容不可
休業災害の可能性がある 頻繁な不休災害の可能性がある	速やかにリスク低減措置を講ずる必要がある。 措置を講ずるまで使用しないことが望ましい。 優先的に経営資源を投入する必要がある。	許容不可
休業災害は極めて稀である 不休災害やかすり傷程度の可能性がある	必要に応じてリスク低減措置を実施する。	許容可

指針によると“休業災害は極めて稀、または不休災害やかすり傷程度の可能性がある”場合を除き、何らかの対応が必要とされており、それらは“許容不可能”であると解釈できる。

厚生労働省等の指針や JIS(ISO)は、具体的な目標や手段・方法・手順等を定めたものであるが、その内容は現時点での知見や技術力を考慮して現在社会の価値観をベースに定められているものと考えられる。つまりこれらを紐解けば現在社会の価値観に基づいた“許容(不)可能”を知ることができると考えられる。

２ リスクアセスメント

(1) リスクアセスメントの手順

リスクアセスメントは、まず、機械類の制限の決定から始まり、その制限範囲内で、機械によって引き起こされる可能性のある種々の危険源（恒久的な危険源及び予期せずに現れ得る危険源）を同定し、可能な限り要因の定量的なデータ等をもとにそれぞれの危険源についてどの位のリスクがあるかを算定し、結果としてリスクの低減が必要であるかを決定する。

図 3-2 は、JIS B 9700:2013 に示されたリスク低減方策までを含んだリスクアセスメントのフローであり、図の破線部分で囲まれたステップがリスクアセスメントである。

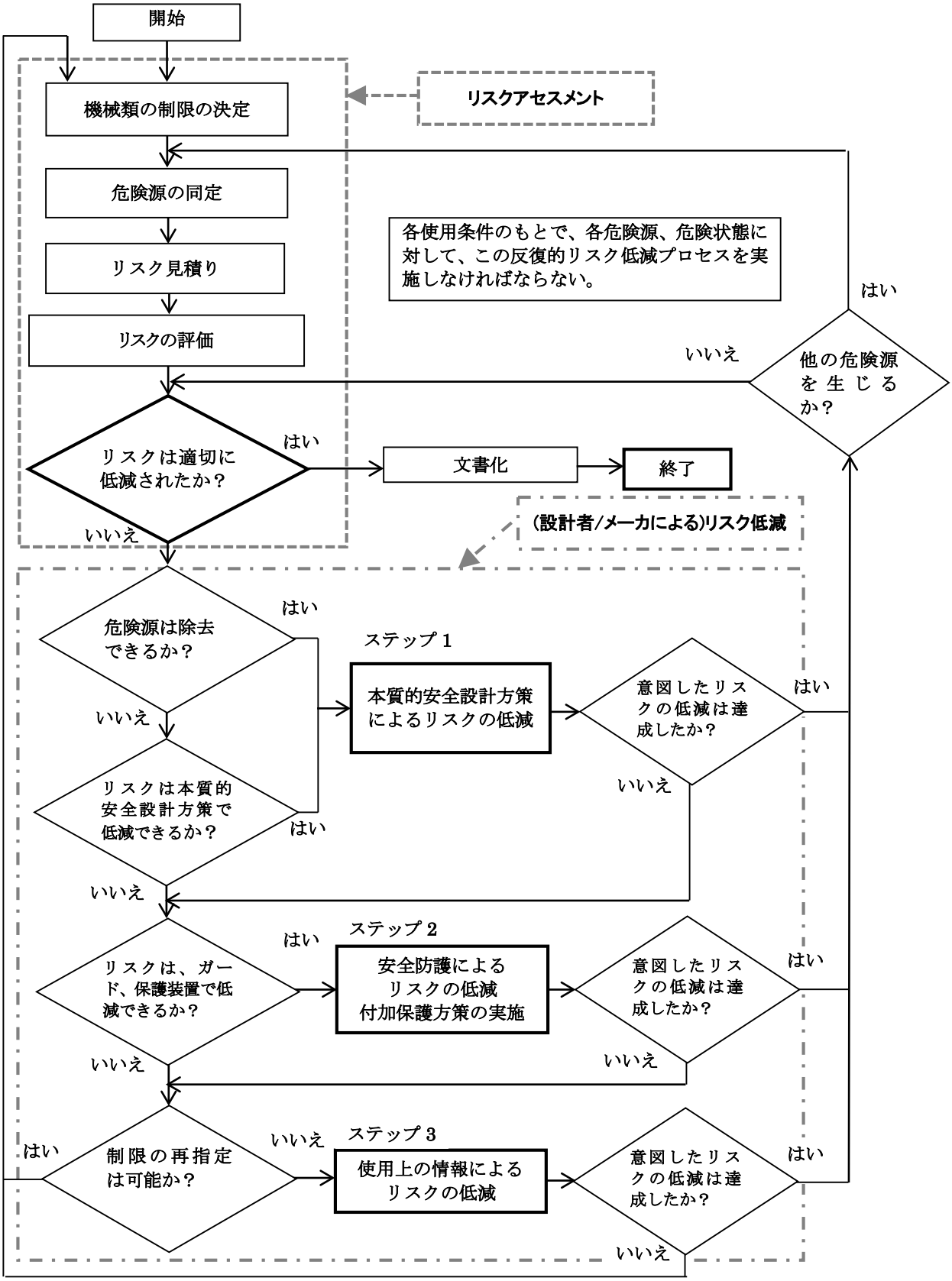


図 3-2 リスクアセスメント・リスク低減の手順

(2) 機械の制限仕様

機械類の制限は、次の 3 つの制限からなり、当該機械の仕様の範囲を決定することを意味する。

－使用上の制限：意図する使用、合理的に予見可能な誤使用を考慮
－空間上の制限：機械の可動範囲、オペレーター機械間インタフェース
－時間上の制限：機械、各コンポーネントのライフリミット

確認すべき機械類の制限仕様の例[2)]を表 3-2 に示す。

表 3-2 機械類の制限例

制限	制限要素例	
使用上の制限	意図する使用 (人との相互作用／対象設計範囲)	(a)ライフサイクル上での相互作用： 1)システム、構成、2)運搬、3)組立て及び据付、 4)コミッショニング、5)使用状態、 6)使用停止・分解
		(b)機能不良に伴う相互作用： 1) 加工品の特性、寸法・形状の変化、2) 構成部品又は機能故障、3) 衝撃、振動、電磁妨害、温度、湿度など環境変化、4) ソフトウェア上の誤りを含めて設計誤り又は設計不良、5) 動力供給異常、電源変動、6) 機械の据付やジャミングなど機械近傍の状況変化
		(c)対象とする人： 1)オペレータ、技術者、見習い/初心者、2)性別、年齢、利き手、障害者、3)機械の周辺作業者、監督者、監視役、4)第 3 者
	合理的に予見可能な誤使用 (機械の合理性の欠如)	1)オペレータによる操作不能の発生、2)機能不良、事故発生時の人の反射的な挙動、3)集中力の欠如又は不注意による機械の操作誤り、4)作業中での近道反応による被災、5)第３者の行動
	予期しない起動	1)制御システムの故障や、ノイズなど外部からの影響で生じる起動指令で生じる起動、2)センサや動力制御要素など、機械の他の部分での不適切な扱いにより生じる起動、3)動力中断後の再復帰に伴う起動、4)重力や風力、内燃機関での自己点火など、機械への外部又は内部からの影響による起動、5)機械の停止カテゴリ(IEC60204-1)
空間上の制限	機械の動作範囲	アクチュエータの可動範囲、及びその可動速度又は運動エネルギー
	オペレーター機械間インタフェース	機械の大きさに適した使用場所、操作パネルの位置、オペレータの作業範囲、保守時の点検／修理スペース、点検部位へのアクセス、 工具や加工物の放出、機械の応答時間
	機械―動力間インタフェース	機械可動部の過負荷対応、異常時のエネルギー遮断、蓄積エネルギーの消散、捕捉時の救出、
	作業環境	階段、梯子、手摺の設置、プラットホーム
時間上の制限	機械的制限	加工用の砥石やドリルなど工具の交換時期、可動部のベアリングや油空圧部品のシール寿命
	電気的制限	絶縁劣化、接点寿命、配線被覆の磨耗、接地線の外れ、有資格者の任命

(3) 危険源・危険状態・危険事象の同定

ISO/TR 14121-2:2012 では、人の存在(作業)と危険源のオーバーラップによる危険状態で、何らかのトリガーである危険事象が発生する、あるいは一定時間の暴露により危害を及ぼすとされている（図 3-3 参照)。リスクアセスメントにおいては、危険状態と

なる人の存在(作業・行動)、危険源、および危険事象を同定する。

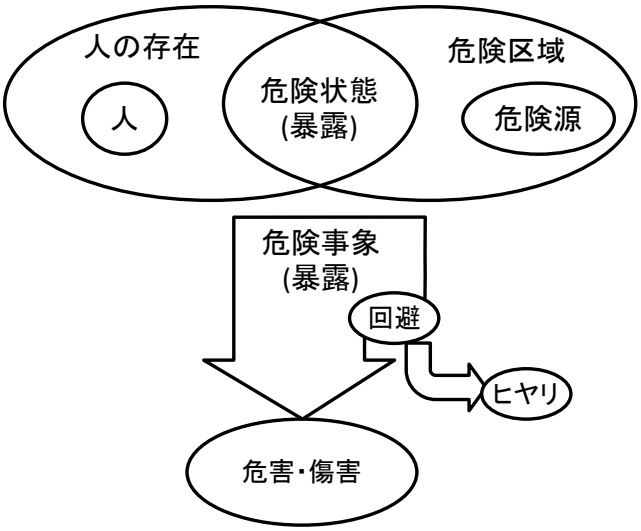


図 3-3 危険源・危険状態・危険事象と危害・傷害の関係（ISO に一部追記）

ア 危険源の同定

危険源の同定とは、機械が持つ、または機械によって引き起こされる可能性のある種々の危険源(恒久的な危険源及び予期せずに現れる危険源)を見つけ出すことであり、JIS B 9700 では、表 3-3 のような危険源が規定されている。

危険源は、同表の“発生原因”と“潜在結果”を以下のように適切な組み合わせで表される。

- ― 可動要素による押しつぶしの危険源
- ― 機械又は機械の部分の安定性の欠如による危険源
- ― 障害（不具合）条件化で充電状態になる電気部品による感電又は感電死の危険源
- ― 電気エネルギーによる機械の場合，充電部，障害（不具合）条件下で充電状態になる部分，短絡及び過負荷による感電，やけど，火災などの危険源が存在する。
- ― バランスが悪く，騒音を発する回転部分に長期／長時間暴露されることによる永久聴覚喪失の危険源
- ― 毒性物質の吸引及び接触の危険源
- ― 悪い姿勢及び反復動作による筋骨格障害の危険源

表 3-3 危険源

タイプ・グループ	危険源の例	
	発生原因	潜在結果
機械的危険源	―加速度、減速度 ―角張った部品 ―固定部分への可動要素の接近 ―切断要素 ―弾性要素 ―落下物 ―重力 ―床面からの高さ ―高圧 ―不安定 ―運動エネルギー ―機械の可動性	―ひ（轢）かれる ―投げ出される ―押しつぶし ―切傷又は切断 ―引き込み又は捕捉 ―巻き込み ―こすれ又はすりむき ―衝撃 ―噴出による人体への注入 ―せん断 ―すべり、つまずき及び墜落 ―突き刺し又は突き通し

表 3-3 危険源

タイプ・グループ	危険源の例	
	発生原因	潜在結果
	—可動要素 —回転要素 —粗い、すべり易い表面 —鋭利な角部 —蓄積エネルギー —真空	—窒息
電気的危険源	—アーク —電磁気現象 —静電現象 —充電部 —高圧下の充電部に対する距離の不足 —過負荷 —不具合（障害）条件下で充電状態になる部分 —短絡 —熱放射	—火傷 —化学的影響 —埋め込み医療機器への影響 —感電死 —落下、投げ出される —火災 —融溶物の放出 —感電
熱的危険源	—爆発 —火炎 —極端な温度の物体又は材料 —熱源からの放射	—火傷 —脱水 —不快感 —凍傷 —熱源からの放射による傷害 —熱傷
騒音による危険源	—キャビテーション —排気システム —高速でのガス漏れ —製造工程（打ち抜かれる、切断など） —可動部分 —表面のこすれ・ひっかき —バランスの悪い回転部品 —音の出る空圧装置 —劣化部品	—不快感 —認識力の喪失 —バランスの喪失 —恒久的な聴覚喪失 —ストレス —耳鳴り —疲労 —口頭伝達又は聴覚信号の妨害の結果としての他のもの（例えば、機械的、電気的）
振動による危険源	—キャビテーション —可動部分の調整ミス —移動式装置 —表面のこすれ・ひっかき —バランスの悪い回転部品 —振動する装置 —部品の劣化・摩耗	—不快感 —腰部障害 —神経疾患 —骨間接障害 —脊柱・脊髄骨の外傷 —血管障害
放射による危険源	—電離放射源 —低周波電磁放射 —光放射（赤外線、可視及び紫外線）、レーザも含まれる —無線周波数帯電磁放射	—やけど —目及び皮膚への障害 —再生機能への影響 —遺伝上の突然変異 —頭痛、不眠症など
材料及び物質による危険源	—エアロゾル —生物学的及び微生物学的（ウイルス又は細菌）な作用物質 —可燃性 —ほこり	—呼吸困難、窒息 —がん —腐食 —再生機能への影響 —爆発

表 3-3 危険源

タイプ・グループ	危険源の例	
	発生原因	潜在結果
	—爆発 —繊維 —引火性 —液体 —流体 —ヒューム —ガス —ミスト —酸性	—火災 —感染 —突然変異 —中毒 —過敏症
人間工学原則の無視による危険源	—接近 —指示器及び視覚表示ユニットの設計又は位置 —制御装置の設計、位置又は識別 —努力（身体的） —明滅、まぶしさ、影及びストロボ効果 —局部照明 —精神的過負荷／負荷不足 —姿勢 —反復動作 —視認性	—不快感 —疲労 —筋骨格障害 —ストレス —ヒューマンエラーの結果としての他のもの（例えば、機械的、電気的）
機械が使用される環境に関連する危険源	—ほこり及び霧　—雪 —電磁妨害　—温度 —雷　—水 —湿度　—風 —汚染 —酸素不足	—やけど —軽微な疾病 —滑り、転落 —窒息 —機械又は機械部分上の危険源の結果としての他のもの
危険源の組み合わせ	—例えば、反復動作＋努力（身体的）＋高温環境	—例えば、脱水症状、認識力の喪失、熱ショック

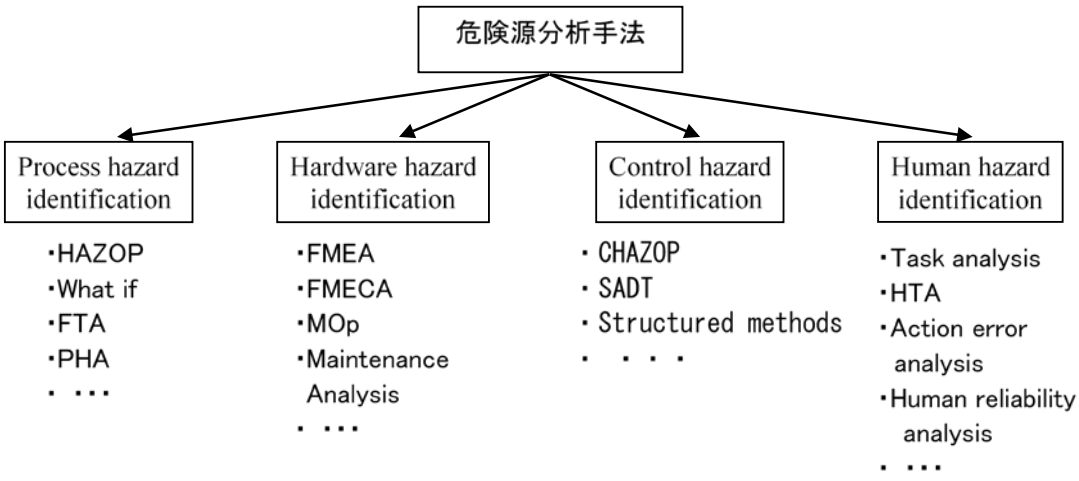
（ア）通常運転時の危険源の同定

機械の使用制限にて確認した仕様・動作等において、表 3-3 のような危険源を同定する。危険源の洗い出しでは、その危害のひどさ、接近頻度や暴露時間などは考慮せず危険源となりうるものは全て同定する。

（イ）異常時に発生する危険源の同定

設計寿命・部品寿命・消耗品寿命や設置環境などを踏まえ一般的な知見や同類の機械・機構の故障履歴などから機械の故障時や、作業ミス等人的起因にて発生する危険源と事象を同定する。危険源分析の手法については、図 3-4 のような手法があるが、このリスクアセスメントにおいてはすべての故障を洗い出すのではなく、故障や作業ミスなどにより人に対するリスクとなりうる危険源に限定する。

ここでの危険源の同定は、通常運転時には発生しないが、異常時に発生する“危険源”の同定であり、後述する“危険事象”とは異なる。たとえば、楊重機器に吊られている荷がワイヤの切断により落下する事象は、“ワイヤの切断”という異常により“荷の落下”という危険源が発生したのではなく、荷はそもそも重量物としての危険源であり、“ワイヤの切断による荷の落下”は危険事象となる。表 3-4 に異常時に発生する新たな危険源の例を示す。



HAZOP：Hazard and operability study
FTA：Fault tree analysis
PHA：Preliminary hazard analysis
FMEA：Failure mode and effect analysis
FMECA：Failure modes、 effects、 and criticality analysis

MOp：Maintenance and operability study
CHAZOP：Computer hazard and operability study
SADT：Structured analysis and design techniques
HTA：Hierarchical task analysis

表 3-4 異常時発生する危険源の例

起因	発生する危険源の例
機械的(機械の故障等)	－絶縁不良による漏電 －排気ダクト内への可燃性粉塵の堆積 －作業床面の凍結 －ポンプ汲み上げ不良による冷却水の高温化 －ウォーターハンマー現象による配管系破損 －異物等による煙道閉塞により不完全燃焼となり CO ガス滞留
人的(作業ミス等)	－配線を間違え装置カバーが充電部となる －薬品の混合を誤り有毒物質が放出される・爆発する ・混ぜてはいけないものを混ぜる。 ・混ぜる量を間違える ・混ぜる速度を間違える －空焚きによる異常高温

また、図 3-5 にマトリックスを使った危険源の網羅的な洗い出しの手法例を示す。マトリックス左列にシステムの要素部品・機構を列挙し、それぞれの要素毎に異常時に発生する危険源を含め、表 3-3 に示すタイプ・グループの危険源について同定する。

危険源 / 構成要素	機械的				電気的	熱的	騒音	振動	放射	材料		人間工学	環境
	動力（挟まれ等）	重量物	滑り・躓き・墜落	その他（切創等）						有害物質	爆発・火災		
ロボット(エンドエフェクタ含む)	●	●		●	●	●	●						
治具	●	●		●	●		●					●	
コンベア	●	●			●								
配線			●		●								
制御機器		●			●								
製品				●		●				●		●	
接着剤										●			

図 3-5 マトリックスを使った危険源の洗い出し

イ　危険状態の同定

危険状態とは、「人が少なくともひとつ以上の危険源に接近、または暴露されるような状況」のことである。危険源への接近または暴露は、機械に関するタスクを遂行する結果として生じる状態と、誤使用により生じる状態がある。（タスクとは、「機械に対して又は機械の近傍で一人以上によって遂行される特定の活動」と定義される）機械に関するタスクを遂行する結果としての危険状態は、しばしばタスク、又はタスクの実行の観点で記述される。危険状態は、危害につながる危険事象が発生可能な状態である。

（ア）機械に関する作業

機械のライフサイクルの局面毎の必要とされるタスク例を表 3-5 に示す。後述するリスク見積もりの為にも作業内容の他、係る人、頻度や接近または暴露時間についても同定する必要がある。

表 3-5 タスクの例

機械ライフサイクルの局面	タスクの例
輸送	—持ち上げ　—包装　—積み下ろし —積み上げ　—輸送　—開封
組み立て及び据付 コミッショニング	—機械及びそのコンポーネントの調整 —機械の組み立て —廃棄システムへの接続（例えば、排気システム、汚水処理） —動力源への接続（例えば、電源供給、圧縮空気） —確認（demonstration） —補助液の供給、充填、積み込み（例えば、給油、潤滑油、接着材） —囲い付け（fencing） —固定、固着 —据付のための準備（例えば、基礎作り、振動アイソレータ） —ワークなしで機械を稼動 —負荷又は最大負荷での試運転

表 3-5 タスクの例

機械ライフサイクルの局面	タスクの例
設定、 ティーチング プログラミング 及び／又は工程の切替	—保護装置及び他のコンポーネントの調整及び設定 —機械の機能パラメータの調整及び設定又は検証（例えば、速度、圧力、力、トラベル限界） —ワークピースの締付／留付 —機能試験、試運転 —工具の搭載又は交換、工具の設定 —プログラム検証 —最終製品の検証
運転	—ワークピースの締付／留付 —制御／検査 —機械の運転 —加工材料の供給、充填、積み込み —手動積み込み／積み下ろし —機械の機能パラメータの微調整及び設定（例えば、速度、圧力、力、トラベル限界） —運転中のまれな介入（例えば、汚染材料の除去、ジャムの除去、局所清掃） —手動制御器の操作 —停止／中断後の機械の再起動 —監視 —最終製品の検証
清掃 保全	—調整 —清掃、消毒 —機械の部品、コンポーネント、及び装置の取り外し —室内掃除 —遮断及びエネルギーの消散 —潤滑油補給・交換 —工具の取替え —劣化部品の取替え —再設定 —液圧レベルの回復 —機械の部品、コンポーネント、装置の検証
不具合の発見／トラブルシューティング	—調整 —機械の部品、コンポーネント、装置の取り外し —不具合の発見 —遮断及びエネルギーの消散 —制御装置及び保護装置の故障からの回復 —ジャムからの回復 —修理 —機械の部品、コンポーネント、装置の取り外し —捕捉された人の救出 —再設定 —機械の部品、コンポーネント、装置の検証
使用停止 分解	—分離及びエネルギーの消散 —分解 —持ち上げ —積み込み —包装 —輸送 —積み下ろし

（イ）想定される誤使用

合理的に予見可能な誤使用により発生する危険状態も想定する。表 3－6 に“合理的に予見可能な誤使用”と具体的な危険行為の例を示す。労働災害の多くは、意図する／しないに関わらず誤使用に起因する危険状態で発生しており、この「誤使用」を如何に同定(想定)できるかが重要となる。危険状態の同定において「誤使用」とは、危険源への接触・接近または暴露される行動・行為のうち、意図した使い方に基づくもの以外で

は全て「誤使用」とされる。したがって、危険状態の同定においては、運転者や保全者など直接機械に係る人の意図した使用に基づかない行動・行為の他、機械近傍の通行者や管理スタッフなどの第三者の行動・行為についても考慮する必要がある。

特に「協働ロボットシステム」においては、作業者とロボットが隣接しており、これらの行為が即事故につながる恐れがある。例えば、協働ロボットと隣接して作業を行うような工程において、作業遅れにより協働ロボットの動作範囲内に進入したり、ロボットが把持しようとするコンベア上の製品の姿勢を修正したりするような行為がありうることを想定しなければならない。

表 3-6 誤使用による危険行為の例

合理的に予見可能な誤使用	危険行為の例
－ 機械の使用中に、機能不良、事故又は故障が生じた時の人の反射的な行動 － 集中力の欠如又は不注意から生じる(故意の誤使用でない)誤った行動 － “近道反応”、”省略行動”等の行動 － 機械の運転を継続させようという動機から生じる不適切な行動 － 機械の製造等を行う者が意図する使用目的、用途、使用方法を正しく知らない労働者がとりがちな行動	・落下しそうになった製品を掴もうとする ・荷ブレした荷を手で止めようとする ・製品のセットミス(ズレ)を修正する ・機械内を通行する ・機械内のゴミを取り除く ・作業遅れで後工程へ進入 ・先取り作業で前工程へ進入

ウ 危険事象の同定

危険状態において危害が起こりうる事象を同定する。危険事象は、機械の故障や人の行動、あるいは機械が設置される周辺環境要素が起因となり偶発的に発生する事象と、運転中の機械内に進入したり騒音に暴露されたりするなどの危険状態から必然的に発生する事象の 2 つがある。必然的に発生する事象は、危険状態そのものが危険事象につながるが、偶発的に発生する危険事象は、何らかの原因や起因となる事象が存在する。１つの危険状態でも複数の危険事象が考えられる場合があり、原因や起因が異なれば保護方策が異なるため、原因や起因となる事象を含めた危険事象を同定する必要がある。表 3－7 に危険事象の例を示す。危険事象が次の危険事象の原因となり、事象の連鎖が起きることもある。

表 3-7 危険事象の例

分類	危険事象の例
機械	－ 運転中断中の起動条件・運転継続条件の成立による運転開始・再開 － 回路・ソフトウェアミスによる機能不良・誤動作 － 供給エネルギーの遮断・変動による機能不良・誤動作 － 供給エネルギー変動や停止後からの復旧などによる機能不良・誤動作 － 電磁ノイズによる機能不良・誤動作 － ゴム・樹脂部品の劣化による機能不良(パッキン・ホースからのガス漏れ) － 摩耗による機能不良(ブレーキ摩耗による制動不良等) － 繰り返し疲労による破壊(吊りワイヤの破断よる吊り荷の落下等) － 腐食による構造物強度低下による機能不良・破壊・倒壊
人	－ 意図した操作・動作とは違う操作・動作 － 意図せず体が操作機器に触れることによる機械の起動・動作 － 誤ったタイミングでの操作・動作(他人の誤操作・誤起動を含む) － 誤った手順・方向・回数での操作・動作(必要な手順の省略を含む) － 許容能力を超えて・設計寿命を越えての機械の使用による機能不良・誤動作・破壊 － 誤った物・量を投入する・組み合わせる

表 3-7 危険事象の例

分類	危険事象の例
自 然 現象	- 地震や強風による機械の転倒・倒壊 - 雨・結露により絶縁不良 - 雨・雪・霧等による視界不良 - 凍結による機能不良(ブレーキが効かない) ※ 津波や土石流等天災自体により危害が及ぶ事象は、機械のリスクアセスメントからは除外する。

(4) リスクの見積もり

個々の危険状態・危険事象におけるリスクは、次の要素の関数である。

a) 危害のひどさ

b) 危害の発生確率

1) 人が危険源へ暴露される

2) 危険事象の発生

3) 危害を回避又は制限するための技術的及び人的可能性

リスク見積もりとは、可能な限り要因の定量的なデータ等をもとに、それぞれの要素を算定することである。

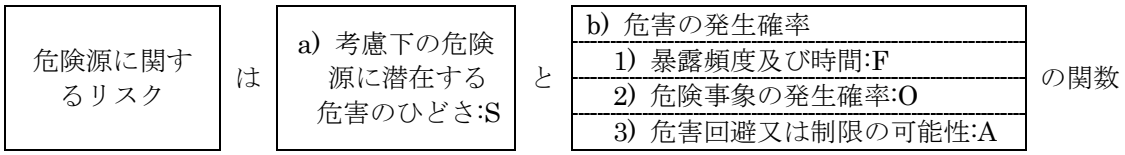


図 3-6 リスク要素

ア 各リスク要素の見積もり

(ア) 危害のひどさ:S

危害のひどさの見積もりにおいては、以下の要素を考慮する。なお、危害のひどさは最悪の場合を想定し見積もりを行う。危害のひどさの選択で迷う場合は、最もひどいが起きる可能性が低い場合と、ひどくはないが起きる可能性の高い場合を両方見積もり、リスクの高低を比較するとよい。

① 傷害又は健康障害の強度（軽い、重い、死亡）

② 危害の範囲（一人、複数）

(イ) 暴露頻度及び時間:F

暴露頻度及び時間の見積もりにおいては、以下の要素を考慮する。

① 危険区域への接近の必要性(運転、段取り、保全、異常処置)

② 接近の性質

③ 危険区域内の滞在時間

④ 接近者の人数

⑤ 接近の頻度(単位時間当たり)

(ウ) 危険事象の発生確率:O

危険事象の発生確率の見積もりにおいては、以下の要素を考慮する。

① 保護方策のレベル

② 保護方策の信頼性

JIS B 9700 や他の書物においては、危険事象の発生確率は、①信頼性及び他の統計データ、②事故履歴、③健康障害履歴、④リスク比較を考慮し見積もるとされている。しかしながら、これらを基にしても危険事象の発生確率を定量化すること、例えば作業者が操作ボタンを押し間違える等の発生確率の算出は非常に困難である。また、後述する安全防護及び付加保護方策によるリスク低減方策は、他のリスク要素でも要件とされておらず、対策実施後のリスク評価ができない。したがって、本テキストでは、「必ず機械は壊れる」あるいは「必ず人はミスをする」を前提とし、これらの事象の発生を防止できる、あるいは発生した時に危害を最小限に抑えられるかという観点から、危険事象の発生確率:O は「リスク低減方策の有効性」とする。

なお、機械の構想設計直後で、リスク低減方策が全く考慮されていない機械の場合、危険事象の発生確率:O は“高い”として見積もる。

(エ) 危害回避又は制限の可能性:A

危害回避又は制限の可能性の見積もりにおいては、以下の要素を考慮する。

① 運転者の知識・技能
② 危険事象の発生速度
③ リスクの認知
④ 危害回避又は制限の人的可能性
⑤ 実際の体験及び知識による

特にリスクの認知性と制限・回避の可能性は重要な要素である。危険事象の発生速度がゆっくりであっても後方で発生していたり、あまりにもゆっくり発生したりする事象は見ていても認知できない(例：アハ体験＝ゆっくりと部分変化する画像は集中していても気づきにくい)ことがある。また、リスクが認知できたとしても、その発生速度や人の身体能力、周辺環境を考慮して、回避の可能性を判断する必要がある。

イ　リスクの見積もり方法

リスクの見積もりは、単純にリスクを点数化したりリスクの大きさを分類したりすることが目的ではなく、後述するリスク低減の必要性判断やリスク低減後のリスク評価が正しく行えるようにすることである。具体的な見積もり方法はリスク評価の概念などを紹介した後の(5)リスク評価にて述べることとし、まずここでは、表 3－8 に示すリスク見積もりの手法 3)を紹介する。

表 3-8 リスク見積もりの手法

名称	方法	特徴
加算法	リスク評価要素毎の評価点を加算し、合計点をリスク評価点としてリスクレベルを決定。	日本では多く利用される。リスク評価要素の増減が容易。リスク低減効果が見えにくい。
積算法	リスク評価要素毎の評価点を積算し、合計点をリスク評価点としてリスクレベルを決定。	加算法の変形。リスク低減効果は加算法より反映しやすい。
マトリックス法	リスク要素を、縦・横 2 軸の評価軸の組み合わせで示されるリスク評価点でリスクレベルを決定。	リスク低減方策実施前後の比較が容易。適用できるリスク要素に限界があるが4要素までは事例がある。
リスクグラフ法	リスク評価要素毎に評価の分岐経路を定め、最終的にリスクレベルを導く。	比較・妥当性確認が容易。 リスク評価要素の評価分類は多くはできない。

（ア）加算法

加算法は、

表 3-9 及び表 3－10 のように各リスク要素を分類し点数を割り付け、リスクは全てのリスク要素の合計値として算出する方法である。

例えば、あるリスクにおいて、危害のひどさ:S＝重大、暴露頻度:F＝稀、回避性:A＝不可能とした場合、20+7=27 が、リスクレベルとなる。

表 3-9 危害の発生確率の定義と点数例

頻度:F	回避性:A	定義	点数
頻繁 (定常作業)	回避不可	可能性が極めて高	20
	回避可	可能性が比較的高い	15
稀 (非定常作業)	回避不可	可能性がある	7
	回避可	可能性がほとんどない	2

表 3-10 危害のひどさの定義例と点数例

ひどさ:S	定義	点数
致命的	死亡災害や身体の一部に永久損傷を伴うもの	30
重大	休業災害(1ヶ月以上のもの)、一度に多数の被災者を伴うもの	20
中程度	休業災害(1ヶ月未満のもの)、一度に複数の被災者を伴うもの	7
軽度	不休災害やかすり傷程度のもの	2

（イ）積算法

加算法と同様に各リスク要素を分類し点数を割付け、リスクは全てのリスク要素の積算値として算出する方法である。

例えば、表 3-9 及び表 3-10 を用いて危害のひどさ:S＝重症、暴露頻度:F＝時々とした場合(他のリスク要素は考慮せず)、20×7=140 が、リスクレベルとなる。

（ウ）マトリクス法

マトリックス法は、個々のリスク要素に点数をつけるのではなく、各リスク要素の組み合わせ結果に対して点数付けを行う方法である。表 3-11 にマトリクス法による例を示す。

表 3-11 マトリクス法によりリスク評価表の例

可能性 ＼ ひどさ			致命的	重大	中程度	軽度
頻繁	回避不可	極めて高い	5	5	4	3
	回避可	比較的高い	5	4	3	2
稀	回避不可	可能性あり	4	3	2	1
	回避可	ほとんどない	4	3	1	1

（エ）リスクグラフ法

リスクグラフ法も個々のリスク要素に点数をつけるのではなく、各リスク要素に基づきフローチャート様に分類していく手法である。

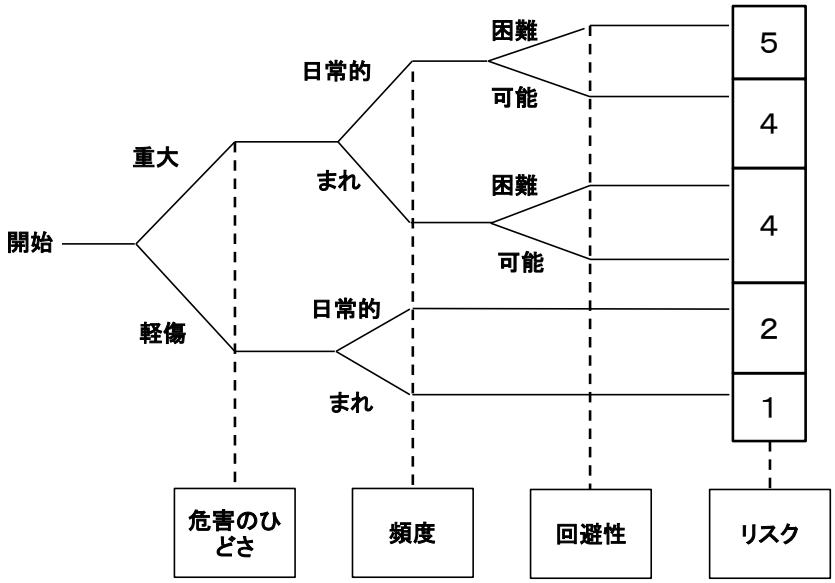


図 3-7 リスクグラフ法

(5) リスク評価

リスク評価とは、リスクの低減が必要であるかどうかを判断することである。リスク低減の必要性は、リスクが許容されるか否かである。

ア　リスク評価の具体例

表 3-12 には、指針におけるリスクの評価の解釈を示したが、同表には“可能性が極めて高い”や“可能性がある”などの表現が使われており、表のように“頻度”と“回避性”を考慮して可能性が定義されている。しかしながら、例えば“日常的に行われる作業で回避不可能な場合”や頻度の具体的な定義がされておらず、曖昧さが残る。

表 3-12 指針別添 4 における可能性の区分

可能性の用語	頻度	回避性
可能性が極めて高い	日常的に長時間行われる作業	回避困難
可能性が比較的高い	日常的に行われる作業	回避可能
可能性がある	非定常的な作業	回避可能
可能性がほとんどない	稀にしか行われない作業	回避可能

指針本文、指針に関する通達や解説などをベースに曖昧さを回避した各リスク要素の定義の例とリスク評価表を表 3-13 及び表 3-14 に示す。

表 3-13 各リスク要素の定義

リスク要素	選択肢	選択基準
危害のひどさ :S	重篤:S3	致命傷(死亡)、身体に後遺障害(欠損、機能障害)を伴うもの
	休業:S2	休業を必要とする傷害。肢の骨折や縫合を必要とする傷害、後遺障害が残らない筋骨格障害
	不休:S1	軽微な傷害（通常は回復可能)。こすり傷、裂傷、挫傷、応急処置を要する軽い傷

表 3-13 各リスク要素の定義

<table>
<tr><th>リスク要素</th><th>選択肢</th><th>選択基準</th></tr>
<tr><td>頻度・時間
:F</td><td>ライン作業:F3</td><td>ライン作業。サイクル毎に作業者が製品・部品をセットしたり取り出したりする作業</td></tr>
<tr><td></td><td>段取り作業:F2</td><td>段取り作業。定期的なツールの交換や補給品の供給・交換、清掃・消毒など</td></tr>
<tr><td></td><td>保全作業等:F1</td><td>保全作業等。機械の修理や点検、不定期の清掃・消毒など</td></tr>
<tr><td rowspan="3">回避性
:A</td><td rowspan="2">回避不可:A2</td><td colspan="2">リスクの認知性と抑制・回避行動より判断する</td></tr>
<tr><td>抑制・回避 / 認知性</td><td>可能</td><td>不可能</td></tr>
<tr><td rowspan="2">回避可:A1</td><td>認知可能</td><td>回避可:A1</td><td>回避不可:A2</td></tr>
<tr><td>認知不可能</td><td>回避不可:A2</td><td>回避不可:A2</td></tr>
<tr><td colspan="3">※適切な理由がない限り“回避不可:A2”を選択</td></tr>
</table>

表 3-14 具体的なリスク評価表

危害のひどさ:S	頻度・時間:F	回避性:A	可能性の定義	評価
重篤:S3	ライン作業:F3	回避不可:A2	可能性が極めて高い	許容不可
		回避可:A1	可能性が比較的高い	許容不可
	段取り作業:F2	回避不可:A2	可能性が比較的高い	許容不可
		回避可:A1	可能性がある	許容不可
	保全作業等 :F1	回避不可:A2	可能性がある	許容不可
		回避可:A1	可能性がほとんどない	許容不可
休業:S2	ライン作業:F3	回避不可:A2	可能性が極めて高い	許容不可
		回避可:A1	可能性が比較的高い	許容不可
	段取り作業:F2	回避不可:A2	可能性が比較的高い	許容不可
		回避可:A1	可能性がある	許容不可
	保全作業等 :F1	回避不可:A2	可能性がある	許容不可
		回避可:A1	可能性がほとんどない	許容可
不休:S1	ライン作業:F3	回避不可:A2	可能性が極めて高	許容不可
		回避可:A1	可能性が比較的高い	許容不可
	段取り作業:F2	回避不可:A2	可能性が比較的高い	許容不可
		回避可:A1	可能性がある	許容可
	保全作業等 :F1	回避不可:A2	可能性がある	許容可
		回避可:A1	可能性がほとんどない	許容可

3　リスク低減

(1)　リスク低減方策概要

ア　リスク低減の目標

リスク評価において、許容不可となったリスクについては、少なくとも法・省令・規則・指針や JIS/ISO/IEC 等の規格に定められている方策を実施し、更に費用対効果分析による評価や優良事例(good practice)を採用する等 ALARP(As Low As Reasonably Practicable：合理的に実行可能な限りできる限り低くする)の原則を適用しリスクを低減する必要がある [4]。

イ　リスク低減の検討ステップ

保護方策は、設計者よる方策と使用者よる方策とに分けられる。図 3-8 にリスク低減プロセス、図 3-9 に設計者による 3 ステップメソッドの保護方策を示す。

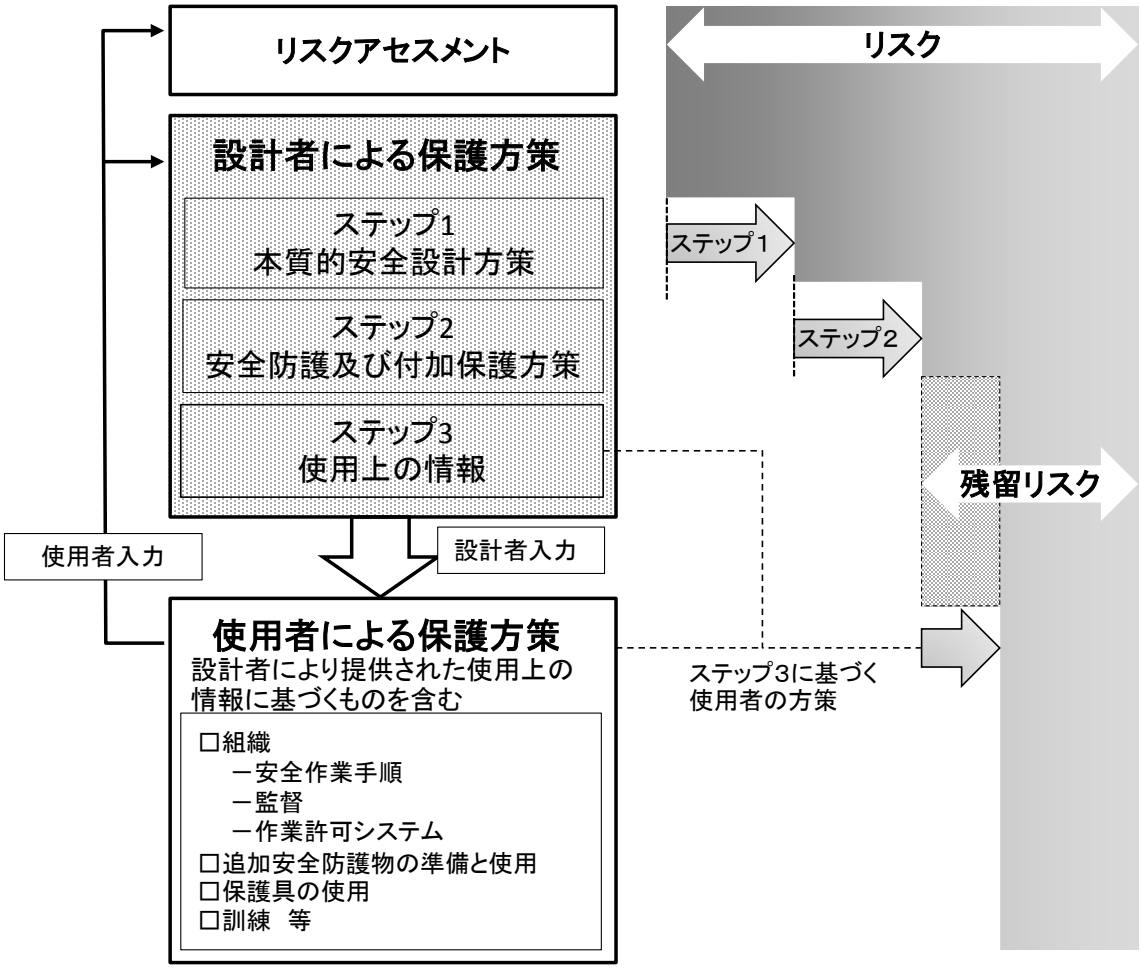


図 3-8　リスク低減プロセス

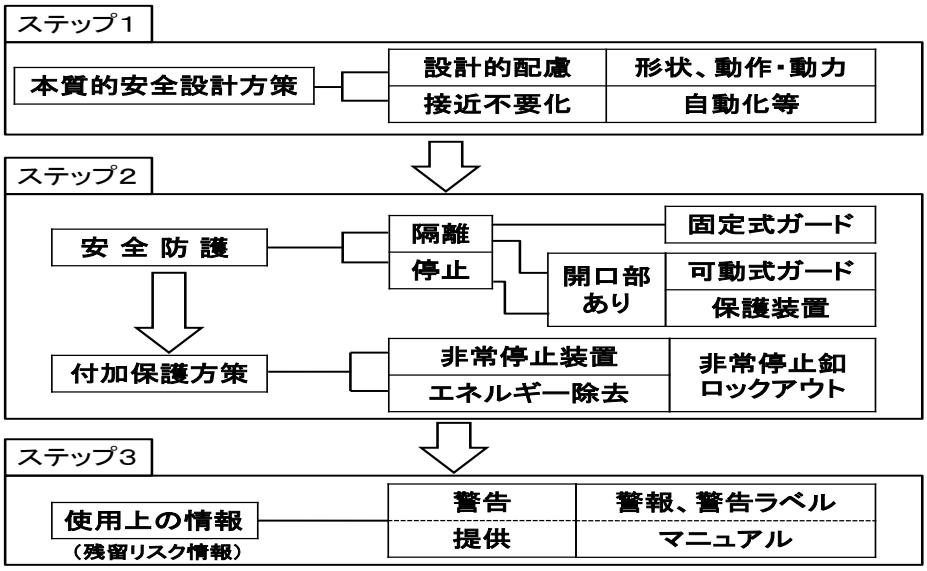


図 3-9　３ステップメソッド

(2) 本質的安全設計

本質的安全設計の基本は、危険源を除去するか、除き切れない場合に各危険源に対して、前述のように危害の程度を下げるか、または、危害の発生確率を下げることである[5]。すなわち、

1）危険源の除去、または危害のひどさの低減

2）危険状態の除去

3）異常時に生じる危険源、危険状態、および／または危険事象の発生確率の低減

の３つに分類される。

最初の２つの方策は、危険源や危険状態そのものに対する方策であり、これが本質安全である。３番目の危険源などの発生確率の低減は、機械の適切な設計や信頼性を高めることにより故障などによって生じる危険源やその発生確率を下げたり、修理等のために人が危険源に近づく必要性を無くしたり、あるいは危険事象の発生確率を下げたりすることである。

1)危険源の除去、危害のエネルギーの低減や 2)危険状態の除去は、危険源や危険状態そのものに対する方策であり、これが本質安全である。3)異常時に生じる危険源等の発生確率の低減は、機械の適切な設計や信頼性の向上により故障などによって生じる危険源の発生確率を下げたり、修理等のために人が危険源に近づく必要性を減らしたりすることである。本質安全は設計する機械の構造からくる確定論であり、危険源などの発生確率の低減は機械や機械のコンポーネント、あるいは人の行動に基づく信頼性等の確率論である。

また、(3)異常時に生じる危険源等の発生確率の低減のうち、制御の信頼性向上により実現される方策は、３ステップメソッドのうちステップ２である安全防護や付加保護方策で採用する安全装置等の他の装置を用いて安全を確保する方策と同様に機能安全により達成される方策である。

ア 危険源の除去・低減

設計的配慮により危険源が持つ危害のひどさを除去する、あるいは危害を与えない程度にエネルギーを低減する方策である。表 3-15 に危険源の種類毎の本質安全化の方策例を示す。

表 3-15 本質安全設計の例

危険源の種類		本質安全化方策
機械	動力	無動力での機構、駆動源の低推力化
	重量物	軽量化
	墜落・滑り	作業床面と同レベル化
	その他(鋭利等)	バリ取り、面取り、挟まれ箇所の排除
電気		保護特別低電圧（PELV）の採用
熱		高温・低温での加工を常温でできる生産技術の採用
音・振動		大きな音や振動を発生させない加工方法の採用
人間工学		無理な姿勢とならないレイアウト
物質		危険有害性のない物質の採用、物質が発散・放出しない材料・加工方法の採用

イ 危険状態の排除

機械の可動範囲外から製品や材料を供給する工程とするなど危険区域外で作業を行うことにより、危険状態を作らないことによるリスク低減方策である。例えば、手動式スライド機構を持つ製品受け台にロボットの可動範囲外で製品をセットし、ロボットの

可動範囲内に押し込むといった方策がある。

ウ　発生確率の低減

異常時の危険源、危険状態、および／または危険事象の発生確率の低減する方策の例を表 3－16 示す。なお、JIS B 9700(ISO 12100)には、上記のア　危険源の除去・低減や危険状態の排除を含めて方策が列挙されているが、ここでは発生確率の低減に関する事項だけを取り上げる。

表 3-16 発生確率の低減方策例

幾何学的要因	視認性の向上、作業位置の適正化、操作位置への接近性の向上
機械設計一般的知識の考慮	機械的応力、材料及びその特性を考慮した設計
適切な技術の選択	防爆機器の採用等
機械的結合の安全原則	構成品間のポジティブな機械的作用の原理の採用
安定性	指定された使用条件下での安定性の確保
保全性	接近性・作業性を考慮した設計
人間工学原則の遵守	人間特性（適切な人―機械インタフェースの設計)、エルゴノミクスを考慮した設計
電気的危険源の防止	JIS B 9960-1 に基づく設計
油気圧装置の安全設計	内圧変動・外乱を考慮した設計
制御システム	安全原則(安定高エネルギー＝安全、安全確認型)の採用 動力の中断・再開に対する考慮、自動監視の使用、適切な PLC 利用、手動制御装置の適切な設計、運転モードの適切な設計、電磁両立性の達成、診断システムの組み込み
安全機能の故障の確率の最小化	信頼性のある部品の採用、非対称故障モード部品の採用、2 重化又は冗長化の採用、
危険源への暴露機会の制限	機械全体・部品の信頼性向上による介入機会の排除

(3)　安全防護及び付加保護方策

本質的安全設計により低減できないリスクについては、安全防護及び付加保護方策にてリスク低減を図ることになる。保護方策は次の順で検討する。

1）安全防護
2）付加保護方策

安全防護とは、ガードと保護装置（安全装置）による方策で、危険な箇所への接近防止策として、ガードで囲う又は保護装置は機械の危険な動きを停止させる方策である。保護装置については、ライト（光）カーテンや圧力検知マットなどの人の侵入・存在検知装置や、両手操作制御装置、イネーブル装置、ホールド・トゥ・ラン制御装置などの人の意思とは関係なく、またはあえて使用を意図なくても有効となる制御システムと連携する保護装置である。

付加保護方策は、非常停止、機械類へ安全に接近するためのはしごやプラットホーム、人の救出手段などである。

なお、1 つのリスクに対する安全防護方策を検討するとき、他の必要とする作業を妨げたり、他のリスクへの保護方策と矛盾したりしない方策を考慮する必要がある。例えば、不注意によりロボットシステム内を通行することに対して、ロボットシステムの全周を固定ガードにて囲う方法が保護方策として考えられるが、この方策を採用した場合、ロボットシステムへの製品のセットや修理のためのロボットシステムへのアクセスができなくなってしまう。

ア　安全防護

低減の必要があるリスクのうち人と危険源と人を隔離することが可能な場合、物理的または時間的に人とロボットシステムを隔離し、リスクの低減を図る方策である。

表 3-17 に安全防護の例を示す。

表 3-17 安全防護の例

安全防護物	具体例	適用個所
固定式ガード	固定柵、固定カバー	必要とされる作業を考慮し、機械内へのアクセスをする必要がない個所。
可動式ガード	安全扉 (インターロック付)	修理など低頻度で機械内にアクセスする必要のある個所。
検知保護装置	ライトカーテン、 レーザスキャナ	製品のセットなど高頻繁で機械内にアクセスする必要のある個所。
		協働システムにおいて、協働時と非協働時で機械側の動作等を制御する場合。

イ　付加保護方策

本質的安全設計方策及び安全防護を補完して、人の能動的行為等で機能を有効にすることによりリスクを低減できる方策がある。これらはハード手段であるが人が正しく使用してはじめて有効になる方策である。付加保護方策の例を表 3-18 に示す。

表 3-18 付加保護方策の例

手段	説明
動力供給遮断手段	機械への動力供給を遮断し、供給される動力により発生する危険源を消滅させる手段。例えば、機械のメインブレーカや圧縮空気の元弁などがこれに当たる。
非常停止手段	人の行動または予期しない危険事象により発生した差し迫った危険状態を回避するための手段。例えば、非常停止ボタンや非常停止ワイヤなどがこれに当たる。
残留エネルギー解放･抑制手段	動力の供給を遮断しても残留するエネルギーの開放または抑制手段。例えば、落下防止ピンや気圧回路の残圧抜き弁がこれに当たる。
接近手段	作業床面以外の場所にアクセスする手段。例えば、階段やはしご、作業用足場などがこれに当たる。
捕捉時の脱出・救助手段	機械内に閉じ込められた時に機械外への脱出手段。例えば、脱出路、手動操作手段、逆転手段、下降手段、通報手段などがこれに当たる。
重量品の安全な扱い手段	重量品を安全に扱うための手段。例えば、フック、アイボルト、吊り上げ／掴み取り用具などがこれに当たる。
第 3 者起動防止手段	第 3 者が誤って起動させないための手段。例えば、キースイッチやパドロック(南京錠)による操作機器類の固定がこれに当たる。

(4)　使用上の情報

機械の状態変化や異常状態を知らせるための信号及び警報装置、機械を正しく使用するために必要な表示、標識（絵文字）及び警告文、機械の運転や保全等のために必要とされる取扱説明書となる。この方策は、使用者が意味を理解し、適切な対応を取ることでリスク低減が行う方策であり、基本的には機械自体のリスクを低減することはできない。

使用上の情報伝達の手段には、以下の方法がある。

ア　信号及び警報装置

危険事象の警告のために使用される視覚信号（例えば，表示灯）及び聴覚信号（例えば，警報サイレン）

イ　表示，標識（絵文字），警告文

機械本体や表示部・操作部に表示

ウ　附属文書

取扱説明書（設置／運転／保全／修理マニュアル等）

(5)　リスク低減後のリスク見積り・評価

ア　リスク低減方策とリスク算定要素の関係

本質的安全設計や安全保護などを実施後、目的とするリスクの低減ができたかの確認を行う。具体的には表 3-19 の通りリスク低減方策の内容によりリスク要素のパラメータを選択し直し、リスクの評価につなげる。

安全防護等の保護方策を実施した場合、保護方策のレベルや信頼性を考慮したリスクの評価を行う。本テキストでは、保護方策のレベルや信頼性を“発生確率:O”として、また、構想設計後のリスク低減方策が考慮されていない状態でのリスクアセスメントとリスク低減方策前後の評価を 1 つのマトリクス評価表で行えるよう“発生確率:O”の“頻繁:O3”の選択基準に“保護方策未実施”を加え、表 3-20 に示すような定義例に基づきリスクの見積もりを行う。評価されたリスクレベルの定義を表 3-21 に、具体的なリスク評価例を表 3-22 に示す。尚、JIS B 9700 では「注意表示や保護具の使用により機械のリスクは下がらない」とされているが、「何もしないのと同じであれば、わざわざ何かする必要はない」または「許容されない機械リスクがある機械は出荷できない／受け入れられない」とならないためにも「保護具や表示」による方策でもパラメータが変化するようにしている。

表 3-19 リスク低減方策とリスク要素の関係

リスク要素	リスク低減方策の効果
危害のひどさ	本質安全化により、危険源の大きさそのものを小さくしした場合。 なお、モータにトルク制御装置や速度制御装置を付加したり、油空圧回路に圧力調整弁を付加する等により出力を制限する場合、又はガードの設置では“危害のひどさが低減される”としてはならない。これらの装置や機能の付加による制限は、後述する“発生確率:O”の選択時に考慮すべき事項とする。 危険源そのものを除去できた場合、当該リスクは存在しないものとしてよい。
暴露頻度	基本設計により、人が危険源に接近・暴露する頻度・時間を低減した場合。 例えば、サイクル毎の材料投入を 1 回／日とした場合。 ある危険源に接近・暴露する作業を無くした場合、当該リスクは存在しないものとしてよい。
回避の可能性	機械的駆動部の動作速度を遅くし、抑制・回避手段を設けるなどの方策により、リスクの認知性及び／または抑制・回避性を向上し回避可能とした場合

表 3-20 発生確率の定義例

リスク要素	選択基準	
発生確率:O	頻繁 :O3	機械として保護方策を実施していない＝頻繁に危険事象等が発生する ― 構想設計後の最初に行うリスクアセスメントにおける見積もりにて選択される
	時々 :O2	人への依存がある保護方策(“付加保護方策”や“使用上の情報”での方策)、または信頼性を確認していない保護方策を実施している＝時々危険事象等などが発生する ― 非常停止ボタンやロックアウト対応器具の設置、手動の残留エネルギーの開放・抑制手段など使う人に操作などを要求する保護方策。 ― 注意ラベル、保護具の使用、作業手順の遵守等の使用上の情報提供による保護方策
	稀 :O1	人への依存度がほとんど無い信頼性のある保護方策を実施している＝危険事象等が発生することは、稀である。 ― 関係する法・省令・規則・指針や JIS/ISO/IEC に従った安全防護 ― 機械系は適切な強度計算等により信頼性が確認したもの ― 制御系の機能安全は、要求される信頼性(PLr)に合致している。

表 3-21 リスクレベルの定義

リスクレベル	定義
4	許容不可なリスク。リスク低減が必要
3	ALARP 原則が適用されていなければ許容不可のリスク。
2	許容可能なリスク
1	無条件で許容可能なリスク

表 3-22 具体的なリスク評価表の例

危害のひどさ:S	頻度・時間:F	回避性:A	発生確率:O		
			頻繁:O3	時々:O2	稀:O1
重篤:S3	ライン作業:F3	回避不可:A2	4	3	2
		回避可:A1	4	3	2
	段取り作業:F2	回避不可:A2	4	3	2
		回避可:A1	4	3	2
	保全作業等:F1	回避不可:A2	4	3	2
		回避可:A1	4	3	2
休業:S2	ライン作業:F3	回避不可:A2	4	3	2
		回避可:A1	4	3	2
	段取り作業:F2	回避不可:A2	4	3	2
		回避可:A1	4	3	2
	保全作業等:F1	回避不可:A2	4	3	2
		回避可:A1	2	2	1
不休:S1	ライン作業:F3	回避不可:A2	4	3	2
		回避可:A1	4	3	2
	段取り作業:F2	回避不可:A2	4	3	2
		回避可:A1	2	2	1
	保全作業等:F1	回避不可:A2	1	1	1

表 3-22 具体的なリスク評価表の例

危害のひどさ:S	頻度・時間:F	回避性:A	発生確率:O		
			頻繁:O3	時々:O2	稀:O1
		回避可:A1	1	1	1

イ　リスク低減方策の評価

リスク低減方策の評価においては、リスク低減目標の達成度合いの他、リスク低減方策が新たな危険源を生じたり、1 つの機械に採用される様々なリスク低減方策が矛盾したりしないかなどの妥当性も確認する必要がある。表 3-23 に JIS B 9700(ISO 12100)に基づく確認すべき項目を示す。

表 3-23　リスク低減方策の評価項目

リスク低減方策の妥当性評価内容	確認
リスクは合理的に実現可能な程度まで低減できているか？	
すべての運転条件及びすべての作業で成立するか？	
新たに生じた危険源は同定・評価され、必要な場合は方策が講じられているか？	
残留リスクについては使用者に十分に通知し、かつ警告しているか？	
作業性を阻害したり、機械の使い勝手を悪くしたりしていないか？	
他の保護方策の支障にならないか？	
機械の能力を過度に低減しないか？	

参考文献

(1) 基発第 0310001 号　危険性又は有害性等の調査等に関する指針.
(2) 社団法人日本機械工業連合会, メーカのための機械工業界リスクアセスメントガイドライン.
(3) 中央労働災害防止協会, 機械設備のリスクアセスメントマニュアル機械設備製造者用.
(4)イギリス HSE, "*Principles and guidelines to assist HSE in its judgements that duty-holders have reduced risk as low as reasonably practicable*". from http://www.hse.gov.uk/risk/theory/alarp1.htm
(5) 向殿政男. (2013). 安全確保における本質安全の役割について. *検査技術 , 18* (6), 26-31,2013.

第４章　機械安全における機能安全の適用

１ 概要

第３章で説明したリスク低減の本質的安全設計方策として制御システムを適用することができる。本章では、その際の安全関連システムに対する要求事項について解説し、さらに本質的な安全部分として、または安全防護物若しくは保護装置の制御部分として、プログラマブル電子装置（例えば、プログラマブルロジックコントローラ：PLC）による機能安全を適用する概略について述べる。

２ 制御システムへの本質的安全設計方策の適用

(1) 危険な機械の挙動と安全機能

危険な機械の挙動およびその原因としては、例えば以下が考えられる。

- 予期しない機械の起動
- 無制御状態の速度変化
- 運動部分の停止不能
- 機械の部分または機械によってクランプされたワークピースの落下または放出
- 保護装置の不作動（無効化または故障）によって生じる機械の挙動
- 制御ロジックの不適切な設計または修正（偶発的または故意）
- 制御システムのコンポーネントの一時的あるいは恒久的な障害・故障
- 制御システムの動力供給の変動または故障
- 制御装置の不適切な選択、設計および配置

これらの危険な機械の挙動を防止し安全機能を達成するために、制御システムの安全機能・性能が十分リスクを低減できるように方策を選択する。機械制御システムの正しい設計によって、予測できない潜在的に危険な機械の挙動を回避することができる。

(2) 一般要求

制御システムは、オペレータが機械と安全かつ容易に相互に作用し合えるよう設計しなければならない。具体的には、以下のいずれかを備えなければならない。

- 起動および停止条件の体システム的分析
- 特定の運転モードの提供。例えば、正常停止後の起動、サイクル中断後または非常停止後の再起動、機械に装荷されたワークピースの排出、機械要素に故障が生じた場合の機械の一部分の運転など
- 障害の明確な表示
- 危険な機械の挙動を引き起こすような予期しない起動指令の偶発的な発生を防止する手段。例えば、覆いをつけた起動装置など
- 危険な機械の挙動を引き起こす再起動を防止するために維持された停止指令。例えば、インタロック。

制御装置や保護装置は、機械のどの区域に属するのかを明らかにしなければならない。区域間のインタフェースの設計は、一つの区域の機能によって、介入のため停止している他方の区域に危険源を生じないようにしなければならない。

(3) 詳細要求

制御システムに本質的安全方策を適用する際に考慮する項目について列挙する。詳細は、JIS B 9700（ISO 12100）6.2.11 を参照のこと。

ア　内部動力源の起動または外部動力供給の接続

内部動力源の起動または外部動力供給の接続によって危険状態が生じてはならない。

イ　機構の起動または停止

機構運動の起動または加速の最初の動作は、電圧や流体圧力の加圧・増加によることが望ましい。逆に、停止または減速の最初の動作は、電圧や流体圧力の除去または低減によることが望ましい。常時減速の制御をオペレータが維持するためにこの原則を守れない場合、機械には主ブレーキシステムが故障したときに減速し、停止する手段を備えなければならない。

ウ　動力中断後の再起動

動力の中断後に再起動されると機械が自動的に再起動して、それが危険源となるおそれがある場合は、その再起動を防止しなければならない。例えば、自己保持のリレー、電磁接触器(コンタクタ)またはバルブの使用による。

エ　動力供給の中断

機械類は、動力供給の中断または過度な変動によって生じる危険状態を防止するように設計しなければならない。少なくとも次の要求事項に合致しなければならない。

- 機械類の停止機能を維持しなければならない。
- 安全性のために常時運転を必要とする全ての装置は、安全を維持するために効果的な方法で作動しなければならない。
- 位置エネルギの結果として、機械類の部分または動きやすい機械類によって保持されたワークや負荷は、それらを安全に低い位置に移すために必要な時間、保持されなければならない。

オ　自動監視の使用

自動監視は、保護方策によって実行される単独または複数の安全機能を実行するコンポーネントや要素を対象とする。それらの能力が低下、工程条件が危険源を発生する側に変化した場合に、その安全機能が確実に実行されることを意図している。安全機能が次に動作要求される前に障害を検出するために、自動監視は障害を直ちに検出するか、または周期的にチェックを行う。

カ　手動制御に関する原則

a) 手動制御器は、関連する人間工学原則に従って設計し、配置しなければならない。

b) 停止制御器は、各々の起動制御器の近傍に配置しなければならない。起動または停止の機能をホールド・ツゥ・ラン制御によって行う場合で、操作を止めたときにホールド・ツゥ・ラン制御装置が停止指令の伝達を失敗することによってリスクが生じるおそれがある場合には、別途停止用の制御器を設けなければならない。

c) 例えば、非常停止または教示ペンダントのように必要上やむを得ず危険区域内に配置する制御器の場合を除いて、手動制御器は危険区域から届かない所に配置しなければならない。

d) 制御器および制御位置は、可能な場合はオペレータが作業区域または危険区域を視認できるように配置しなければならない。

e) 同一の危険要素を複数の制御器を用いて起動できる場合、一つの制御器だけが有効に作動するように制御回路を設計しなければならない。

f)制御アクチュエータは、リスクがあるところでは意図的な操作を行わない限り操作できないように設計し、またはガードを設けなければならない。
g)オペレータによる直接制御によって安全な運転が確保される機械の機能に対しては、例えば、制御装置の設計および配置によってオペレータが制御位置にいることを確実にするための方策を採用しなければならない。
h)ケーブルレスでの制御に対し、通信が不通になることを含め、制御信号が受信されないときは自動的に停止しなければならない。

キ　設定（段取りなど)、ティーチング、工程の切替え、障害の発見、清掃または保全の各作業に対する制御モード

機械類の設定、段取り、ティーチング、工程の切替え、障害の発見、清掃または保全作業のためにガードを移動若しくは取り外さなければならない場合および／または保護装置を無効にしなければならない場合で、かつ、これらの作業の目的で機械類または機械類の一部を運転する必要がある場合は、次の機能を全て満たす特定の制御モードによって、オペレータの安全を確保しなければならない。

a)全ての他の制御モードを不作動にする。
b)機械の危険な要素の運転は、イネーブル装置、両手操作制御装置またはホールド・ツゥ・ラン制御装置の操作を続けることによってだけ許可する。
c)機械の危険な要素の運転は、リスクが低減した状態下においてだけ許可する。例えば、減速、低減した動力または力、段階的操作による。
d)機械のセンサに対する故意または無意識の行為で危険な機能が実行されることを防止する。

ク　制御モードおよび運転モードの選択

調整、設定、保全、点検などを許可するために異なる保護方策および／または作業手順を必要とする幾つかの制御モードまたは運転モードを使用できるように機械を設計し製作する場合、当該機械には各々のモード位置に固定（ロック）できるようなモード切替装置を備えなければならない。モード切替装置の各々の位置は、一つの制御モードまたは運転モードのいずれか一つを選択するようにしなければならない。

モード切替装置は、機械のある特定機能の使用について特定のカテゴリのオペレータに限定するような他の切替手段（例えば、ある種の数値制御機能に対するアクセスコード）で置き換えてもよい。

ケ　電磁両立性を達成するための方策の適用

電磁両立性に関しては、JIS B 9960-1(IEC 60204-1)およびIEC 61000-6を参照のこと。

コ　障害の発見を支援する診断システムの規定

保護方策を無効にする必要性をなくすため、制御システムに障害の発見を支援する診断システムを組み込むことが望ましい。

3　プログラマブル電子制御システムによって実行される安全機能

(1) 一般

プログラマブル電子装置を含む制御システムは、適切な場合、機械類の安全機能を実

行するために使用することができる。プログラマブル電子制御システムを使用しているところでは、安全機能に関係する性能要求事項を考慮する必要がある。

プログラマブル電子制御システムの設計は、ランダムハードウェア故障の確率および安全関連システムの性能に対して悪影響を及ぼし得る決定論的原因故障の可能性が十分に低いものでなければならない。決定論的原因故障とは、設計および評価試験などの開発プロセス中に発生するバグやミスなどの障害を指す。

プログラマブル電子制御システムで監視機能を行う場合、障害の検出についてのシステムの挙動を考慮しなければならない。詳細は、本書 5 章を参照のこと。

プログラマブル電子制御システムは、各々の安全機能に対して指定された性能（SIL または PL）が達成されることを確実にするために妥当性確認を行い、取り付けるのが望ましい。妥当性確認は、全ての部品が安全機能を実行するために正しく相互作用していることを示すための、および意図しない機能が生じないことを示すための試験および分析を含んでいる。

(2) ハードウェアの側面

ハードウェア（例えば、センサ、アクチュエータ、論理回路を含む。）は、実行する安全機能の機能的要求事項および性能要求事項の両者に適合するように選択、設計、取付けをしなければならない。特に、次の手段による。

- アーキテクチャの制約。例えば、システムの構成、障害を許容するシステムの能力、障害の検出におけるシステムの挙動がある。
- 危険なランダムハードウェア故障の確率が適切である装置の選択および／または設計
- 決定論的原因故障および制御のシステム障害を回避する方策並びに技術のハードウェアへの取り込み。

(3) ソフトウェアの側面

組込みオペレーティングソフトウェア（またはシステムソフトウェア）およびアプリケーションソフトウェアなどのソフトウェアは、安全機能に対する性能仕様を満たすように設計しなければならない。

アプリケーションソフトウェアは、使用者が再プログラムできないようにするのが望ましい。アプリケーションに対して使用者による再プログラムを必要とする場合、安全機能を取り扱っているソフトウェアへのアクセスを制限するのが望ましい。例えば、ロック、または権限のある人へのパスワードによる。現在、市販の安全プログラマブルロジックコントローラの多くは、後者のアクセス制限機能を持っている。

4 安全関連システムの構成と安全度水準

(1) 概要

安全機能を提供するために割り当てられる機械の制御システムの部分（安全関連システム）はハードウェアおよびソフトウェアで構成することができ、かつ、これらは機械の制御システムから分離または統合することができる。安全関連システムの要求事項は、JIS B 9705-1(ISO 13849-1)または JIS B 9961(IEC 62061)に記載されている。本章では、JIS B 9705-1「機械類の安全性–制御システムの安全関連部–第 1 部：設計のための一般原則」に基づいて安全関連システムの構成と安全度水準について説明する。

JIS B 9705-1 は、ソフトウェアの設計を含み、安全関連システムの設計および統合のための原則に関する安全要求事項および指針について規定している。安全関連システ

ムに対して、この規格は、安全機能を実行するために要求される性能レベル（パフォーマンスレベル：PL）を含む特性を規定する。JIS C 0508(IEC 61508)では、この性能レベルを安全度水準（SIL）と呼んでいる。安全関連システムの一部である製品の例は、リレー、ソレノイドバルブ、位置スイッチ、PLC、モータコントロールユニット、両手操作制御装置、圧力検知装置である。

(2) 設計上での考慮事項

ア　設計における安全性の目標

安全関連システムは、JIS B 9700(ISO 12100)のリスクアセスメント及びリスク低減の原則に従って、設計および製作しなければならない。全ての意図する使用および合理的に予見可能な誤使用を考慮しなければならない。

機械におけるリスク低減の方法論は、本書第 3 章に説明している。機械の危険源分析およびリスク低減プロセスは、次の階層的方策によって危険源を除去または低減することを要求している。

- 設計による危険源除去またはリスク低減
- 安全防護方策および付加保護方策によるリスク低減
- 残留リスクに関する使用上の情報の準備によるリスク低減

イ　リスク低減に対する制御システムの寄与

機械の全般的設計手順に従うことの目的は、安全性の目標を達成することである。要求のリスク低減を提供する 安全関連システムの設計は、機械の全般的設計手順に組み込まれた一部である。設計の本質的な安全部分として、または安全防護物若しくは保護装置の制御部分として安全機能を提供する際、安全関連システムの設計はリスク低減の方法論の一部である。これは、反復的プロセスであり、図 4-1 で示される。

機械におけるリスクアセスメントから、設計者は、安全関連システムによって実行

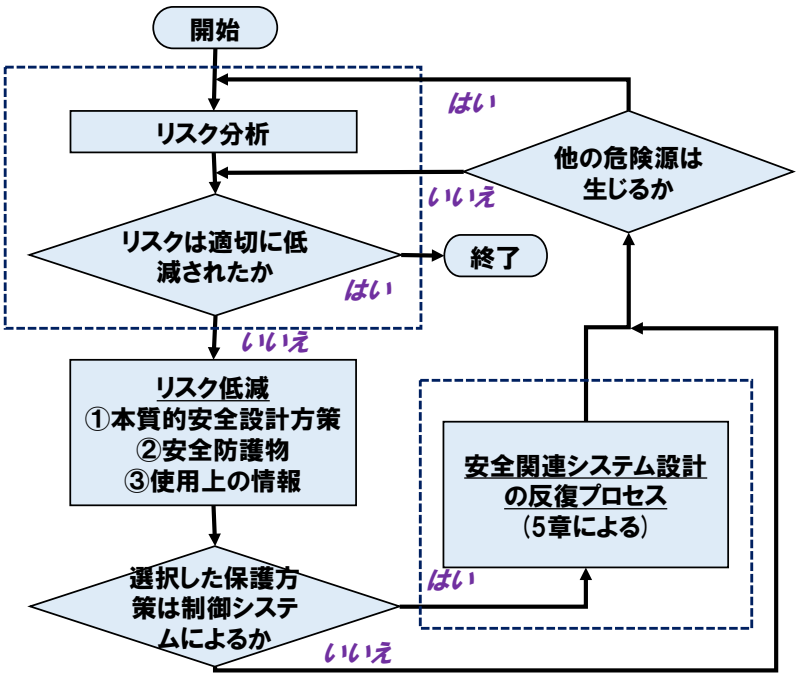


図 4-1 リスクアセスメント／リスク低減の概要

される、関連のあるそれぞれの安全機能によるリスク低減への寄与を決定しなければならない。この寄与は、制御下の機械類の全体にわたるリスクを網羅してはいない。しかし特別な安全機能の適用によって部分的リスクは低減される。そのような機能の例は、プレスの電気的検知保護装置の使用によって開始される停止機能、または洗濯機のドアロック機能である。

リスク低減は、種々の保護方策（安全関連システムおよび非安全関連システム共に）を適用することによって、所定の安全条件達成の最終結果として実現できる。

ウ　要求安全度水準(PLr/SIL)の決定

安全関連システムによって実行される選択したそれぞれの安全機能に対して、リスクアセスメントの結果に従い、要求安全度水準を決定しなければならない。要求安全度水準は、要求パフォーマンスレベル(PLr)あるいは安全度水準（Safety Integrity Level: SIL)として5段階あるいは4段階で示される。要求安全度水準は高くなるほど、安全関連システムによって提供されるリスク低減量は大きくなければならない。

エ　安全関連システムの設計

リスク低減プロセスの一部は、機械の安全機能を決定することである。これは制御システムの安全機能、例えば、予期しない起動の防止を含む。

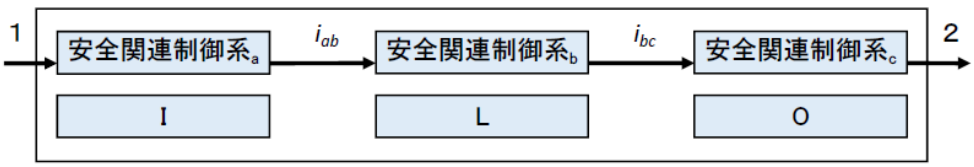
一つの安全機能は、一つ以上の 安全関連システムによって実行される場合があり、かつ、複数の幾つかの安全機能は一つ以上の安全関連システムのサブシステムに分割される場合がある。一つの 安全関連システムが安全機能および通常の制御機能を実行することが可能である。設計者は、有効な技術方式のいずれかを単独または組み合せて用いることが望ましい。また、安全関連システムは操作機能を提供する場合もある。

代表的な安全機能は、図4-2のダイアグラムで表現され、制御機能を持つ安全システムは次の組合せによる。

- 入力（安全関連システムa）
- 論理／処理（安全関連システムb）
- 出力／動力制御要素（安全関連システムc）
- 相互接続手段（i_{ab}、i_{bc}）

同一の機械類内で、種々の安全機能とそれらに関連する安全関連システムが実行する特定の安全機能を区別することは重要である。制御システムの安全機能を同定する場合、設計者は 安全関連システム（図4-1参照）を特定しなければならない。また、必要な場合、入力、論理および出力に 安全関連システムを割り当て、また、冗長システムの場合には、個々のチャネルに対して 安全関連システムを割り当て、その後、安全度水準を評価しなければならない。

なお、本章5節において、安全機能の分解の事例を示す。



I 入力　　L 論理処理　　O 出力
1 開始事象(例えば、押しボタンの手動操作、ガード開、ライトカーテンのビーム遮断)
2 機械アクチュエータ(例えば、モーターブレーキ)

図4-2　安全関連システムの組合せに関するダイアグラム

オ 安全関連システムの能力と達成手段

JIS B 9705-1 においては、安全制御が安全機能を遂行する能力は、パフォーマンスレベル(PL)の決定によって表される。安全機能を遂行するために選択した 安全関連システムの各々および／または 安全関連システムの組合せに対して、PL の見積りを実施しなければならない。

JIS C 0508 および JIS B 9961 規格では、安全関連システムが安全機能を遂行する能力は、安全度水準(SIL) として示される。表 4-1 は、PL および SIL の対応関係を示している。PLa は SIL のスケールとは合わず、主に軽微なリスク、通常は回復可能な傷害を低減するために使用される。一方、多数の致命的被害に及ぶ SIL4 は、機械のリスクとして評価されることはない。すなわち、SIL3 に対応する PLe は最も高いレベルとして定義される。

安全関連システムが、PL 及び SIL を達成するための手段としては、主として、次によらなければならない。

- コンポーネントレベルでの障害発生確率の低減
  この目的は、安全機能に影響を与える障害発生確率または故障の発生確率を低減することである。これは、コンポーネントの信頼性を向上させること、例えば、重要な障害または故障を、低減または除去するために、“十分吟味されたコンポーネント”の選択によっておよび／または“十分吟味された安全原則”を適用することによって達成可能である。
- 安全関連システムの構造を改良
  この目的は、障害の危険な影響を回避することである。幾つかの障害は検知される場合があり、かつ、冗長および／または監視構造が必要となる。

両方策は、個別にまたは組み合わせて使用することができる。技術方式によって、リスク低減は信頼性のあるコンポーネントの選択によって、および障害の除外によって達成することができる。しかし、他の技術方式では、リスク低減は、冗長および／または監視システムを必要とする場合がある。

表 4-1　PL と SIL との関係

PL	SIL(高/継続運転モード)
a	―
b	1
c	1
d	2
e	3

５ 安全関連システムの安全機能

(1)　安全機能仕様

この箇条は、安全関連システムによって提供できる安全機能の詳細を規定する。設計者は、特定の用途の制御システムで要請される安全方策を達成するために必要な安全機能を組み込まなければならない。例えば、安全関連停止機能、予期しない起動の防止、手動リセット機能、ミューティング機能、ホールド・ツゥ・ラン機能などである。

表 4-2 は、代表的な安全機能であり、そのそれぞれの特性および安全関連パラメータをリスト化してあり、さらに他の JIS および国際規格での安全機能に関する要求事項を参照している。設計者は、表 4-2 に掲げてある関連する安全機能に対して、すべての適用可能な要求事項を確実に満たさなければならない。安全機能の特性によっては、追加の方策が必要であり、本節で述べる。

安全機能を同定し、かつ、指定する場合、少なくとも次を考慮しなければならない。
a)個々の危険源または危険状態に対するリスクアセスメントの結果
b)機械の運転特性、以下を含む
- 機械の意図する使用（合理的に予見可能な誤使用を含む。）
- 運転モード［例えば、ローカルモード、自動モード、機械の一部分に関連するモード］
- サイクルタイム
- 応答時間
c)非常操作
d)異なる作業プロセスおよび手動作業（修理、調整、清掃、トラブルシューティングなど）での相互作用に関する記述
e)安全機能で達成するまたは回避する機械の挙動
f)機械が作動可能または不可能となる条件（運転モードなど）
g)運転頻度
h)ある機能が同時に作動した場合の優先順位

表 4-2　典型的な機械の安全機能およびその特性に適用可能な規格
注）表中の数字は、該当規格の章番号を表す

安全機能/特性	JIS B9705-1 (ISO 13849-1)	JIS B 9700 (ISO12100)	追加の情報
安全防護物によって始動する安全関連停止機能	5.2.1	3.28.8, 6.2.11.3	JIS B 9960-1 9.2.2, 9.2.5.3, 9.2.5.5 JIS B 9710 (ISO 14119) JIS B 9715(ISO 13855)
手動リセット機能	5.2.2	-	JIS B 9960-1 9.2.5.3, 9.2.5.4
起動/再起動機能	5.2.3	6.2.11.3, 6.2.11.4	JIS B 9960-1 9.2.1, 9.2.5.1, 9.2.5.2, 9.2.6
ローカル制御機能	5.2.4	6.2.11.8, 6.2.11.10	JIS B 9960-1 10.1.5
ミューティング機能	5.2.5	-	IEC/TS 62046 5.6
ホールド・トゥ・ラン機能	-	6.2.11.8 b)	JIS B 9960-1 9.2.6.1
イネーブル装置機能	-	-	JIS B 9960-1 9.2.6.3, 10.9
予期しない起動の防止	-	6.2.11.4	JIS B 9714(ISO 14118) 5.4
捕捉された人の脱出および救助	-	6.3.5.4	-
遮断およびエネルギの消散	-	6.3.5.4	JIS B 9714(ISO 14118) 5.3, 6.3.1
制御モードおよびモード選択	-	6.2.11.8, 6.2.11.10	JIS B 9960-1 9.2.3, 9.2.4
異なる制御システムの安全関連部間の相互作用	-	6.2.11.1 (最後の文)	JIS B 9714(ISO 14118) 9.3.4
安全関連入力値のパラメータ化の監視	4.6.4	-	-
非常停止機能	-	6.3.5.2	JIS B 9703 (ISO 13850) JIS B 9960-1 9.2.5.4

(2) 安全機能の詳細

ア 安全関連停止機能

表 4-2 の要求事項に加えて、次を適用する。

安全関連停止機能（例えば、安全防護物によって始動する）は、作動後必要に応じて速やかに機械を安全状態に移行しなければならない。このような停止は、通常運転の停止に対し、優先的でなければならない。一連の機械がある管制下で共に動作する場合、上述の停止条件にあることを監視制御および／またはその他の機械に対して情報伝達のための処置を講じなければならない。

安全関連停止機能の無効化の試みを低減するために、実際の運転を完了させるための中止操作を先行させ、また停止位置から容易で、かつ、迅速な再起動手段を準備することがある（例えば、生産に対する損害を与えることなく）。この一つの解決法は、サイクルが容易な再起動を可能にする規定の位置に到達した場合、ガード施錠が開放されるような施錠式インタロック装置の使用である。

イ 手動リセット機能

表 4-2 の要求事項に加えて、次を適用する。

停止命令が安全防護物によって始動した後、再起動のための安全条件が存在するまで、その停止条件を維持しなければならない。

安全防護物をリセットすることによって安全機能を再設定することは、停止命令を消去することである。リスクアセスメントによって示される場合、この停止命令の消去は、手動で、独立して、かつ、故意の動作（手動リセット）で確認されなければならない。

手動リセットの機能は、次でなければならない。

- 安全関連システム内で個別に、かつ、手動で操作される機器を介して提供される。
- 全ての安全機能および安全防護物が動作可能であるときだけ実行される。
- リセット自体で機械の始動または危険状態の始まりとならない。
- 故意の動作による。
- 個別の起動命令を受け入れるための制御システムを備える。
- アクチュエータの励起（オン）位置からの解除動作だけによって受け入れる。

手動リセット機能を備える安全関連システムのパフォーマンスレベルは、手動リセット機能を備えることによって関連の安全機能で要求される安全性を低下させないように選択しなければならない。

リセットアクチュエータは、危険区域の外で、危険区域内の人の不在を目視によってチェックしやすいような安全な位置に配置しなければならない。

ウ 起動／再起動機能

表 4-2 の要求事項に加えて、次を適用する。

再起動は危険状態が存在しない場合にだけ自動的に行われなければならない。起動および再起動に対するこれらの要求事項は、遠隔制御が可能な機械にも適用しなければならない。

制御システムへのセンサからのフィードバック信号は、自動的な再起動を始動することができる。例えば、機械の自動運転では、制御システムへのセンサのフィードバック信号は、プロセスフローを制御するために、しばしば使用される。加工物が加工位置からずれた場合、プロセスフローは停止する。インタロック付きの安全防護物の監視が自動的プロセス制御に優先しない場合、オペレータが加工物を再調整する間、機械を再起動する危険が生じる可能性がある。したがって、遠隔制御による再起動は、安全防護物が再び閉じて、保全員が危険区域を離れるまで、許可されてはならない。

制御システムによる予期しない起動の防止への寄与度は、リスクアセスメントの結果に依存する。

エ　ローカル（局所）制御機能

表 4-2 の要求事項に加えて、次を適用する。

機械が、例えば、携行式制御装置またはペンダントによってローカルに（局所で）制御される場合、次を適用しなければならない。

- ローカル制御を選択するための手段は、危険区域外に配置しなければならない。
- リスクアセスメントで定めた区域におけるローカル制御器によってだけ、危険条件を始動可能としなければならない。
- ローカル（局所）制御と主制御間の切替えで、危険状態を生じてはならない。

オ　ミューティング機能

表 4-2 の要求事項に加えて、次を適用する。

ミューティングとは、ある条件下において安全機能を一時無効化することである。

ミューティングによっていかなる人も危険状態にさらされることがあってはならない。ミューティング中は、他の手段によって安全条件が提供されなければならない。ミューティングの終了では安全関連システムの全ての安全機能が復旧しなければならない。

ミューティング機能を備える安全関連システムのパフォーマンスレベルは、ミューティング機能を含むことによって、関連する安全機能で要求される安全性を損なうことがないように選択しなければならない。

カ　応答時間

表 4-2 の要求事項に加えて、次を適用する。

リスクアセスメントで要請される場合、安全関連システムの応答時間を決定しなければならない。応答時間は、機械の安全距離やインタロックに影響する。

ここで注意が必要なのは、制御システムの応答時間は、その機械全体の応答時間の一部であることである。その機械で必要な全体の応答時間は、安全関連部の設計、例えばブレーキシステムを備えることの必要性、に影響することになる。

キ　安全関連パラメータ

表 4-2 の要求事項に加えて、次を適用する。

安全関連パラメータ、例えば、位置、速度、温度、または圧力が現在の制限から逸脱する場合、制御システムは適切な方策、例えば停止動作、警告信号、アラームを始動させなければならない。

プログラマブル電子システムの安全関連データに関する手動入力エラーによって危険状態を生じるおそれがある場合、安全関連システム内に、例えば限界値、フォーマットおよび／または論理入力値に関するデータチェックの手段を備えなければならない。

ク　動力源の変動、喪失および復旧

表 4-2 の要求事項に加えて、次を適用する。

エネルギー供給の喪失を含めて、設計上の動作範囲を超えるエネルギレベルの変動が生じた場合、安全関連システムは、機械システムの他の部分において安全状態を維持できるように出力信号を生成し続ける、または始動させなければならない。

(3) 妥当性確認

安全関連システムの設計では、妥当性確認を実施しなければならない。妥当性確認は、各安全機能を提供する安全関連システムの組合せが、この規格に関する全ての要求事項を満たすということを立証しなければならない。

妥当性確認は、第 6 章にて説明する。

(4) 保全

予防保全または事後保全は、安全関連部の特定の性能を維持するために必要である。時間の経過とともに指定の性能からの逸脱は、安全性の低下、または危険状態にもなり得る。安全関連システムの使用上の情報には、安全関連システムの保全指示書を含めなければならない（定期検査を含む）。

安全関連システムの保全性に関する規定は、JIS B 9700 の 6.2.7 に示す原則に従わなければならない。

(5) 技術文書

安全関連システムを設計する場合、設計者は、少なくとも安全関連システムに関連する次の情報を文書化しなければならない。なお、これらの文書類は、製造業者内部での使用を目的としており、機械のユーザに配布するものは「使用上の情報」である。

- 安全関連システムによって提供される安全機能
- 各安全機能の特性
- 安全関連部の正確な起点および終了点
- 環境条件
- パフォーマンスレベル PL
- 選択したカテゴリ又は複数のカテゴリ
- 信頼性に関連するパラメータ（MTTFd、DC、CCF および使命時間）
- 決定論的原因故障に対する方策
- 使用した技術方式または複数の場合、各技術方式
- 考慮した全ての安全関連障害
- 障害の除外に関する正当化の根拠
- 設計の論理的根拠（例えば、考慮した障害、除外した障害）
- ソフトウェア関連文書
- 合理的に予見可能な誤使用に対する方策

(6) 使用上の情報

JIS B 9700 のおよび他の関連文書の適用可能な箇条を適用しなければならない。特に、安全関連システムの安全な使用に際しての重要な情報は、ユーザに示されなければならない。これは次を含むが、この限りではない。具体的な情報については、ボイラーおよびロボットのマニュアルにおいて説明する。

- 選定したカテゴリに対する安全関連部の制限および障害の除外の全て
- 安全関連システムの制限および障害除外の全て。選定したカテゴリおよび安全性能の維持のために必須である場合、その障害の除外を継続的に正当化するために、適切な情報を示すことが望ましい。
- 安全機能における指定性能からの逸脱の影響
- 安全関連システムおよび保護装置へのインタフェースの明瞭な記述
- 応答時間
- 運転制限（環境条件を含む）

- 指示および警告
- 安全機能のミューティングおよび中断
- 制御モード
- 保全
- 保全チェックリスト
- 内部部品へのアクセスおよび交換の容易性
- 容易かつ安全なトラブルシューティングの手段
- 参照カテゴリに関する適用上の情報
- 関連する場合、試験間隔のチェック

安全関連システムのカテゴリ（または複数のカテゴリ）およびパフォーマンスレベルに関して、次のような特定の情報を提供しなければならない。

- この規格の参照および発行年号（すなわち、“JIS B 9705-1:2011”）
- カテゴリ B、1、2、3 または 4
- パフォーマンスレベル、a、b、c、d または e

6 JIS B 9705-1 と JIS B 9961 の関係

JIS B 9705-1(ISO 13849-1)および JIS B 9961(IEC 62061) は、いずれも機械類の安全関連システムの設計および実装のための要求事項を規定する。これらの規格は、その適用範囲に従っていずれを使用しても関連の必須安全要求事項を満たすということが想定される。ただし、安全度水準の表記と扱う技術範囲が異なっている。表 4-3 は、この規格 JIS B 9705-1 および JIS B 9961 の範囲を要約したものである。(この表は、ISO 13849-1：2015 の発行に伴い消去されたが参考のために示す)

JIS B 9705-1 と JIS B 9961 は同じ目的の規格であるが、適用範囲が異なる。関連規格を含めた規格の関係を図 4-3 に示す。

表 4-3 JIS B 9705-1 と JIS B 9961 の適用のための推奨情報

	安全関連制御機能実装の技術方式	JIS B 9705-1 (ISO 13849-1)	JIS B 9961 (IEC 62061)
A	非電気式、例えば液圧式	他規格による	適用できない
B	電気機械式、例えば、リレー及び/又は非複雑電子システム	PLe まで	SIL3 まで
C	高複雑度電子システム、例えばプログラム式	PLd まで	同上
D	A と B の複合	PLe まで	他規格による
E	C と B の複合	PLd まで	SIL3 まで
F	C と A、または C と A 及び B との複合	他規格による	他規格による

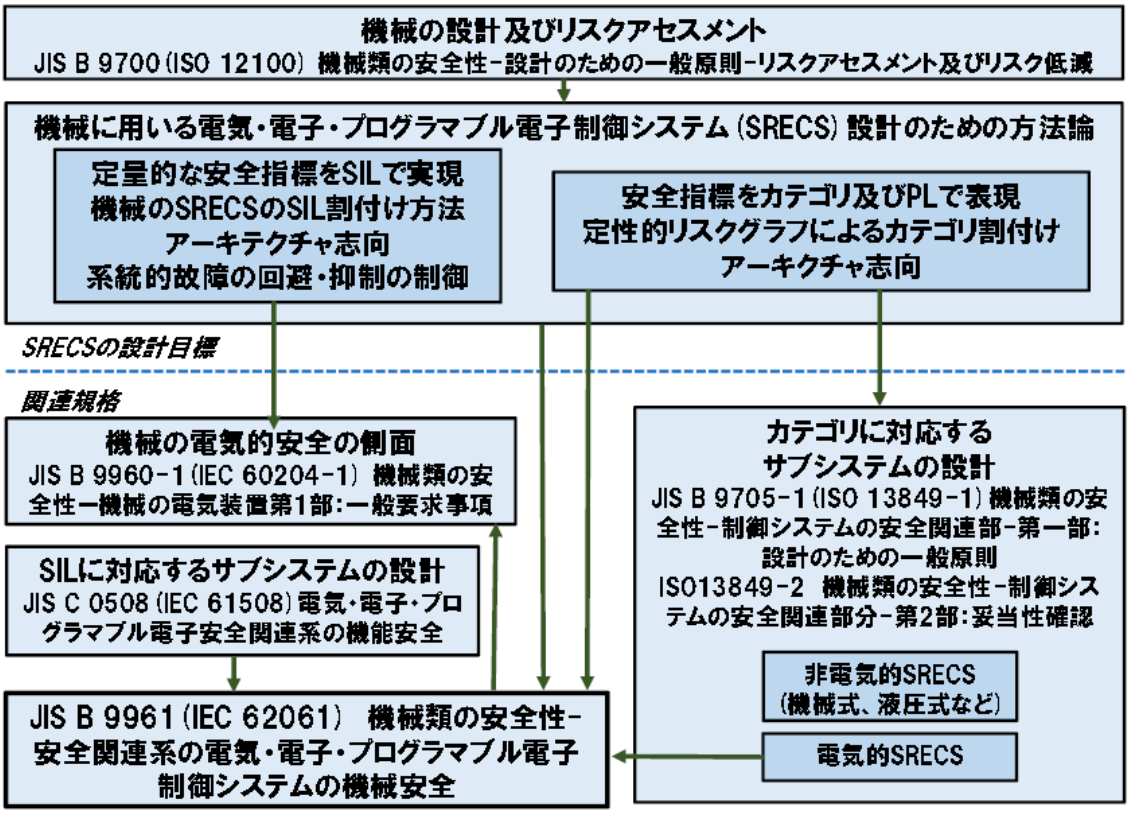


図 4-3 JIS B 9705-1 と JIS B 9961 との関係

第 5 章　機能安全による安全関連システムの設計

1　機能安全の概要

欧米では，危険が隔離されていることが，安全であると認識されている．そして、その考え方は「すべての危険を除くことは難しく，高価になる．安全とは，怪我や物的損害の危険性が低く，管理可能であること.」である．

このことから，「我慢(許容)できる危険は残る」と言うことになる．もし，隔離が不十分であれば，不十分部分を通り抜けた危険が人に危害を与えることになる．

このことから安全は技術で解決するものという概念が生まれた。

1980 年代から，電気，電子応用製品，機器類がコンピュータにより高機能化が進み，複雑になるに従い，故障がソフトウェア起因や予期しない外乱により起こるようになり，良いものを作れば，壊れないという「品質中心」の考え方から，壊れても危険にならない(人に危害を与えない)という「機能安全」の考えに変化してきた。

本章では主に JIS C 0508（IEC 61508）の内容に沿って説明する。

2　リスクアセスメントと機能安全

機能安全は、リスクアセスメントの結果行われるリスク低減のための３ステップメソッドのステップ２の安全防護及び付加保護方策において電気･電子制御を用いた方策が該当する。この方策の一部は、安全機能と呼ばれる。

電気・電子制御では電気・電子部品やソフトウェアが使用される。電気・電子部品は機械部品と異なり、使用中に偶発的故障が起きる。この故障により電気・電子制御で安全が維持される安全防護及び付加の保護方策が機能しなくなり、危険状態になる可能性がある。それを回避するため、電気・電子制御部の故障発生、フォールト状態でも安全を維持できるようにしなければならない。故障発生、フォールト状態でも安全を維持する考え方が機能安全である（図 5-1 参照)。

ソフトウェアは、多くの制御に使用される。ソフトウェアは、人が開発するものであり、ソフトウェアの中には考え違いやうっかりミスのような人に起因する故障原因（バグともいわれる）を潜在的に含むことがある。この故障原因が、安全機能実行時、何らかの条件で発現した時、安全機能が実行できず、電気・電子制御による安全防護及び負荷の保護方策が機能しなくなり、危険状態になる可能性がある。機能安全の考

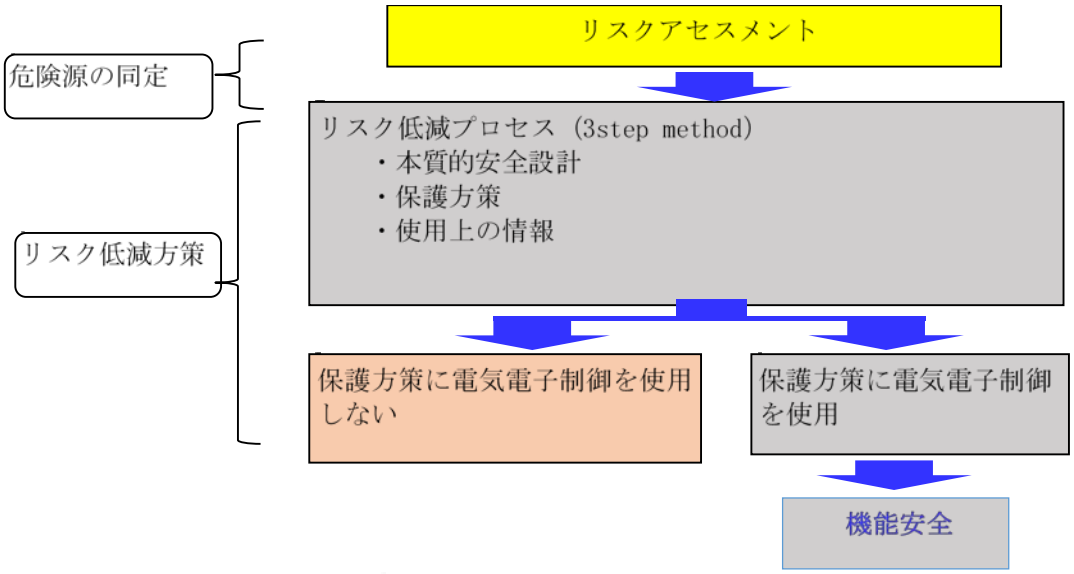


図 5-1　機能安全の概念

え方の中には、主にソフトウェアに潜在的に含まれる危険源を決定論的原因故障(systematic failure)と呼び、これを出来るだけ除去するため、決定論的原因故障の回避のための技法や手段が推奨されている。

結局、機能安全は、ハードウェア面では、部品故障が、又ソフトウェア面では決定論的原因故障が、装置やシステムの安全機能の正常な働き妨げ、それらを操作する人、又周辺の人に危害が及ばないように安全機能の故障を監視し、故障を検出した場合は、予め決めた安全状態に移行し、人や財産への危害を防ぐことである。そして、IEC 61508 の要件を満たすことで、機能安全を証明できることになる.

3 全安全ライフサイクル中の安全度水準の割当て

全安全ライフサイクルは、安全関連システムの機能安全に必要な業務をフェーズ(工程)別に分類し、流れ(フローチャート)図（図 5-2）表現したものである。

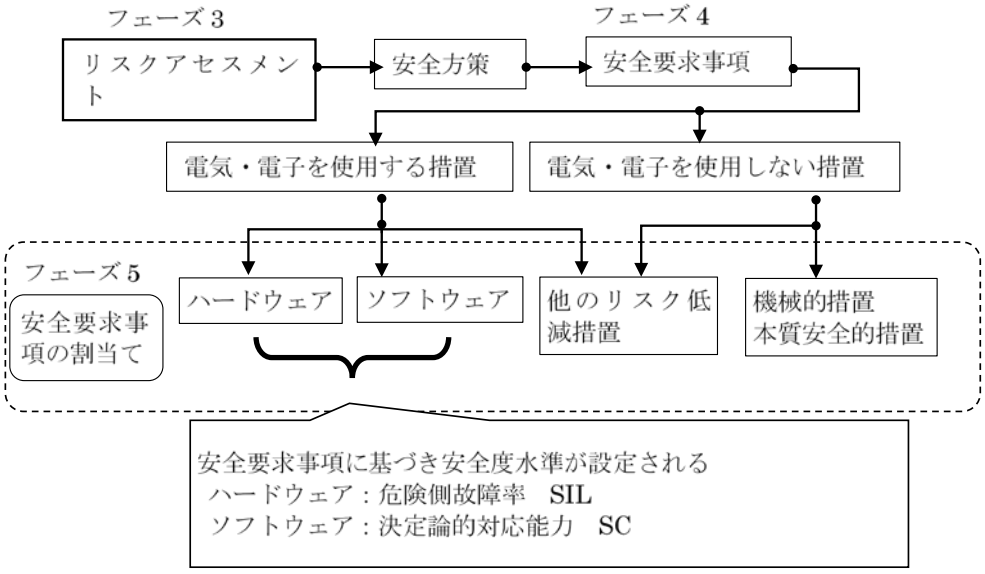


図 5-2　安全度水準の割当て

(1) 安全度水準の割当て

割り当てられた安全機能は、安全機能に割当てる目標機能失敗尺度である安全度水準(SIL)を決める.

各安全機能に対する安全度水準は，次のいずれかを割り付ける.

ⅰ. 低頻度作動要求モード

安全機能の作動要求における機能失敗時間平均確率.(PFDavg)

ⅱ. 高頻度作動要求又は連続モード

安全機能の危険側失敗の平均頻度(PFH)［1/h］

(2) 目標機能失敗尺度

この尺度は、安全機能に作動要求が出た時、安全機能がその作動要求に対し、正常に動作できず失敗する確率を表す（表 5-1)。安全度水準により、失敗尺度の上限範囲が決まっている。この目標機能失敗尺度は、後述の FMEDA によって求めることがで

きる。

表 5-1 目標失敗尺度

安全度水準 (SIL)	低頻度作動要求モード運用 PFD(Probability of Failure on Demand) 作動要求当たりの設計上の機能失敗平均確率(PFDavg)	高頻度作動要求又は連続運転モード運用 PFH(probability of failure per hour) 安全機能の危険側失敗の平均頻度 (PFH) [1/h]
1	10^{-2} 以上 10^{-1} 未満	10^{-6} 以上 10^{-5} 未満
2	10^{-3} 以上 10^{-2} 未満	10^{-7} 以上 10^{-6} 未満
3	10^{-4} 以上 10^{-3} 未満	10^{-8} 以上 10^{-7} 未満
4	10^{-5} 以上 10^{-4} 未満	10^{-9} 以上 10^{-8} 未満

(3) 安全度水準と共通原因故障

安全度水準は、FMEDA(ハードウェア (7))で求める危険側故障確率(PFD、PFH)と共通原因故障確率の合計で判定する。

共通原因故障は、冗長システムにて安全機能と安全度水準の割当てを行う場合、冗長システムチャンネルの複数チャンネルが同じ故障原因により故障となり、故障状態となることである。

共通原因故障は、EUC(非制御機器)制御システム，電気・電子・プログラマブル電子 (以降、電子等制御と呼ぶ) 安全関連システム及び他技術安全関連システム及び他リスク低減措置の間で十分な独立性が明示できない場合，これらのシステム間には、共通原因故障による危険側機能失敗の可能性があるものとする.

独立性の確認には、安全関連システムのサブシステム，エレメントを構成する 2 つ以上のチャンネル間の空間的，距離的分離、電気的な分離、そして、使用部品の制約条件の確認も必要である。

十分な独立が認められる場合は，共通原因故障の考慮が不要であるが、IEC 61508 では共通原因故障の程度を、チェックシートの点数によって評価する。

安全度水準は、ハードウェアの構成(HFT : Hardware Fault Torelance : 5 項参照)の制約により上限が決まっている。求める安全度水準は、「安全度水準 = 危険側故障確率＋共通原因故障確率」となる。

安全度水準の判定には、共通原因故障確率が大きく影響するので、設計仕様作成の段階から共通原因故障の要因を取り除くことが重要である。

4 ハードウェアの設計

(1) ハードウェアの要求事項

機能安全を実行する電子、電気、プログラマブル電子機器、装置、又は、これらを使用している設備機械、システムにおいて、安全機能を達成するために、安全信号を入力し、それらの信号を論理的な処理をし、出力信号を介して、アクチュエータを制御する。信号を入力し、出力を制御するためには、これらの信号処理を行う論理処理ハードウェ

ア(マイコンとそのソフトウェアを含む)が必要となる。

ア　信頼性ブロック図

要求された安全機能を実行するハードウェアは、次の 3 つの部分に分けて考える（図 5-3)。3 つの部分は、それぞれサブシステムと呼ばれる。

ⅰ．入力部(Sensors：センサ)サブシステム
ⅱ．　論理部(Logic：ロジック)サブシステム
ⅲ．出力部(Final elements (actuators)：最終要素)サブシステム

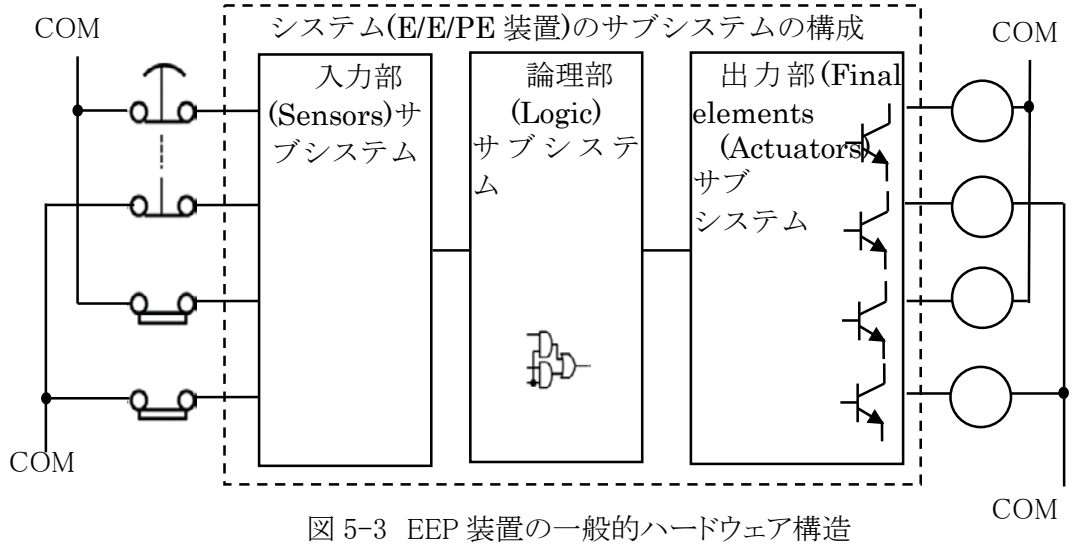


図 5-3　EEP 装置の一般的ハードウェア構造

各サブシステムは、１つ以上の要素(Element)で構成される。

SIL 値はサブシステムごとに求め、それを合計してシステム全体の SIL 値とするので、ハードウェア要求仕様は、サブシステム単位で記述することが必要である。(ハードウェア（8）参照)

また、ハードウェアの構成は、予め、これら 3 つのブロックを意識して作成する。

この、システムを 3 つのサブシステムに分け、そのサブシステムの機能を要素とするブロック図は、「信頼性ブロック図」と呼ばれる。この信頼性ブロック図は、安全装置の信頼性、安全度を考察する上で重要な図である。

イ　信頼性ブロック図の信頼性割合

安全関連システムに必要とされる安全度水準を達成するため、市場で故障が多く発生する部分に達成割合を多く設定する。一般的には図 5-4 に示す割合である。

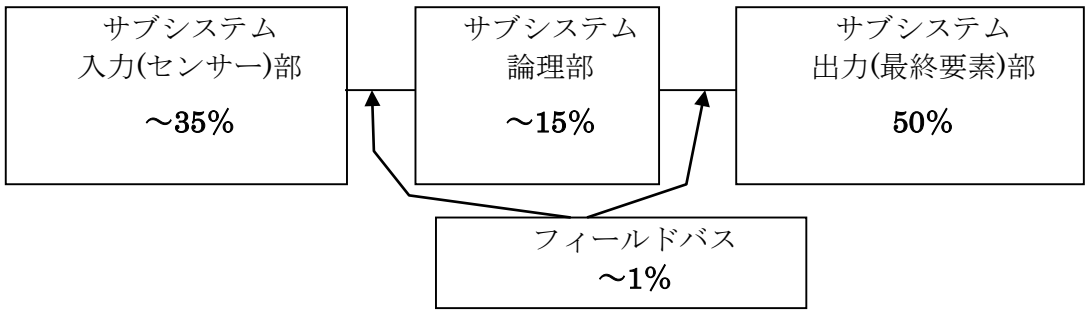


図 5-4　信頼性ブロックの信頼性割り付け

ウ　安全部と非安全部の分離

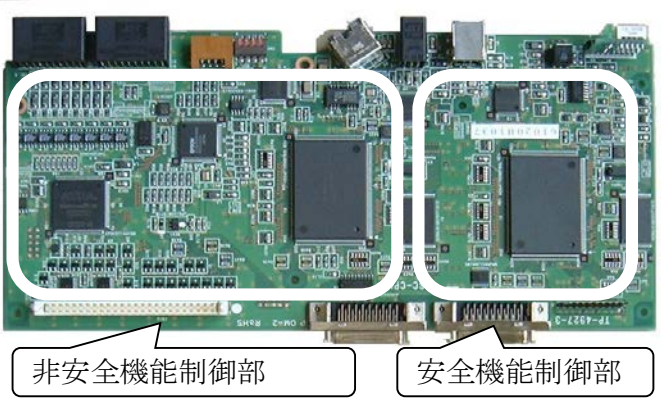
安全機能の設計仕様書の作成上で特に注意を要することは、安全機能と非安全機能を分離することである。一緒にした場合、非安全部分を安全部分と見なすことが必要になる場合が多い。そのため、安全関連システムの全ライフサイクルが両者に適用となり、機能安全対象の安全機能としての適用部分が多くなり、複雑性、困難性が高くなることを承知しておかなければならない。

（ア）安全と非安全の独立性

安全関連システムで安全機能と非安全機能の両方が実装されている場合、非安全側の故障が、安全側の危険側故障の起因とならないように、安全機能と非安全機能との独立性が、十分保証されていることが必要である（図 5-5）。
このことが証明されない限り、非安全機能を含むハードウェア/ソフトウェアは安全関連システムとして扱う。

十分に保証された独立とは、非安全部と安全部との間で発生する相手側に影響する従属故障の確率が安全部の最も高い安全度水準に要求される故障確率より十分低いことを証明することである。

非安全機能と安全機能を同じ安全関連システムで実行することは、IEC 61508 の規格では禁止とは言っていないが、もし、非安全機能の独立性を証明できない場合、非安全機能を安全機能と同じ安全ライフサイクルの工程で実施することが必要となる。その結果、その安全機能の設計・開発がより煩雑となり、設計、開発の困難さが増す。



独立である証明の例
- 電源は別か？
- 信号は電気的に分離ができているか？
- 非安全マイコンの暴走が、安全側に影響ないソフトか？
- 非安全側のノイズが安全側に影響しないか？
- ――――
- etc

図 5-5　安全部と非安全部

なぜなら、一般に安全機能部より非安全機能部の方が圧倒的に設計、開発規模が大きいからである。一般論的には、設計の初期段階で少々回路が増えても安全機能と非安全機能は分離する方が良い。

エ　電子等制御システム設計要求仕様の項目

電子等制御システム設計要求仕様は，要求された安全機能を実行するために必要なハードウェア及びソフトウェアの詳細、及び安全機能と安全度に関する設計要求事項を含まなければならない。

（ア）設計仕様に関する主な項目

ⅰ．システムを構成する各要素の要求事項。
ⅱ．各要素を結合、統合するための要求事項
　・主にモジュール化、構造化、インタフェース仕様等
ⅲ．応答時間と処理能力。

ⅳ．正確で安定的な制御動作
・遅延のない応答、危険事象の正確な判定等)
ⅴ．オペレータとのインタフェース
・誤操作しにくいボタン配置、色配置、保守時の危険源の隔離方法等
ⅵ．安全関連システムや他のシステム間とのインタフェース
ⅶ．異常時を含んだ全ての動作モード
・故障（例えば，アラーム，自動停止、非常停止）時の動作や応答時間
ⅷ．ハードウェアとソフトウェア間の約束事、仕様
ⅸ．各要素間の制約事項及び条件
・インタフェース信号タイミング，共通原因故障の可能性など。
ⅹ．起動及び再起動の手順、それに関連した特定の要求事項
・異常解除後の再起動手順、不意の起動の防止、起動前準備の有無等

（イ） 安全度に関する主な項目
ハードウェアとソフトウェアの安全度水準に影響する以下の項目について、安全要求仕様作成時考慮する。
ⅰ．安全度水準達成のための各サブシステムのハードウェア・アーキテクチャ
・HFT(：Hardware Fault Torelance)と SFF(Safe Failure Fraction：安全側故障割合)の制約に従ったハードウェアの冗長化と診断率の達成
ⅱ．安全度水準達成のために設定したプルーフ試験間隔などのパラメータ
・プルーフ試験間隔を縮めれば高い安全度水準が得やすくなる。
ⅲ．診断によって危険側故障が検出されたとき、すべき動作
・一般的には、予め決めた安全状態(動力遮断など)へ移行する制御を行う。
ⅳ．プルーフ試験ができるようにするための要求事項，制約，機能及び施設
・分解できない樹脂モールドされたマイコン組み込み装置など動作確認する方法、高温で動作する装置を常温で試験する方法など、予め試験用プログラムの組み込み、特殊な設備が必要になることがある。
ⅴ．安全ライフサイクルの中で、使用を想定した環境条件(温度，湿度，機械的環境，電気的環境など)の極端な状態で使用される試験機器、測定器の能力確保
ⅵ．電磁イミュニティレベルの設定（IEC/TS 61000-1-2:2008 参照)。
・特定の場所，又はより過酷条件での使用が想定される場合、製品規格が規定する値よりも高いレベル又は追加のレベルが要求される。
ⅶ．安全管理に必要な品質保証／品質管理の体制、技法又は手段

オ 電子等制御システムの設計と開発
電子等制御システムの設計と開発は、電子等制御システム安全要求設計仕様書に基づき安全機能を設計、開発することである。
妥当性確認計画のフェーズと並行して進めていく。妥当性確認計画は、設計・開発の進展に伴い、追加変更が行われるので、変更が加えられるので常に最新版管理を行う必要がある。

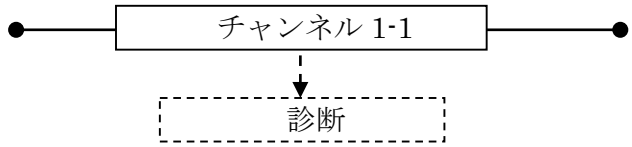
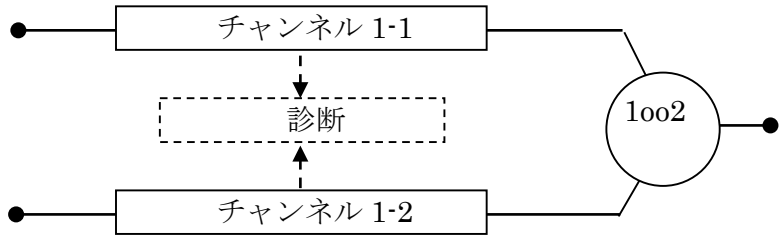
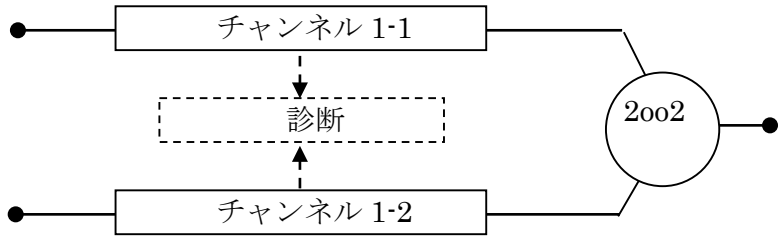
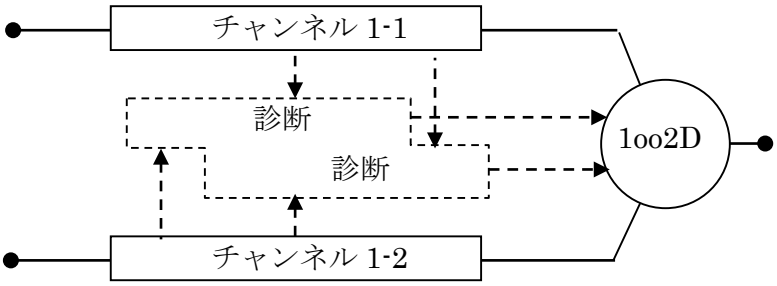
（ア） 設計、開発への要求事項
ハードウェア設計に際し、以下を検討する。
ⅰ ハードウェアに要求された安全度水準に対応した要求事項の検討
・ハードウェア・アーキテクチャに関する HFT の制約
・ランダム故障の定量化の要求事項(危険側故障率の算定)

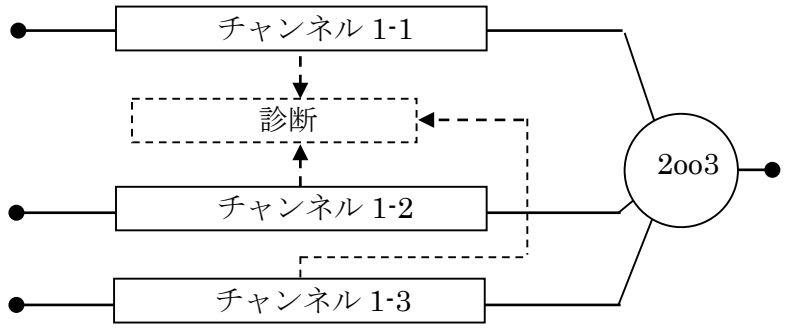
（イ） ハードウェアのアーキテクチャ（構造）
リスクアセスメントによるリスク低減方策としての安全機能を電子等制御システ

ムで達成しようとする場合、要求される安全度水準に応じ、表 5-2 の基本的ハードウェア構造の 1 つが選択される。

以下のハードウェア構造の No.1 から No.5 は安全度水準の低いものから高いものへ概ね適応順である。

表 5-2　ハードウェア構造

No. 1	1oo1 タイプ	HFT 0
	1 チャンネルで構成されたハードウェア構造である。	
		
No. 2	1oo2 タイプ	HFT 1
	2 つのチャンネルで構成されたハードウェア構造である。2 つのチャンネルの処理結果を比較し、不一致の場合に安全状態への移行の要求(デマンド)を発生する。	
		
No. 3	2oo2 タイプ	HFT 0
	2 つのチャンネルが直列で構成されたハードウェア構造である。2 つのチャンネルの処理結果が一致の場合のみ安全状態を維持できる構造である	
		
No. 4	1oo2D タイプ	HFT 1
	2 つのチャンネルで構成されたハードウェア切り替え構造である。 最初、どちらか一方のチャンネルで運転され、診断部で異常が検出されると他方のチャンネルへ切り替わって安全状態を維持する。	
		
No. 5	2oo3 タイプ	HFT 1
	3 つのチャンネルで構成された「3:2」の多数決ハードウェア構造である。3 つのチャンネルの処理結果を比較し、2 つ以上一致の場合、安全状態を維持でき	

	る構造である。 

これらのハードウェア構造は、ハードウェアフォールトトレランス(HFT: Hardware Fault Tolerance)と安全側故障割合と、要求される安全度水準の関係により選択される。
注：表中の“oo”は、out of のこと。2oo3 は、2 対 3 の意味。

（ウ） 決定論的故障の排除

決定論的故障は、ランダム故障以外の故障の総称である。決定論的故障は、ハードウェア・ソフトウェアに関わり、その原因の多くは人に関わる。その主なものは、仕様間違い(知見・経験不足による設計仕様不足、思い込みによる仕様の誤解、コミュニケーション不足による仕様の欠落、試験不足による潜在的欠陥の存在等)、EMC による誤動作、温度・湿度による誤動作、振動・衝撃による誤動作など、また、オペレータの誤操作の誘発などである。

決定論的原因故障を排除するためには、３つのルートの内１つ以上を選択し、そのルートで要求される技法又は手段を選択実施する。(ハードウェア（9）参照)

ルート 1S：決定論的原因故障を回避するため機能安全規格の要求事項を遵守した方法
ルート 2S：使用実績で決定論的原因故障が無いことを証拠だてる方法
ルート 3S：機能安全規格に従わない方法で開発された既存のソフトウェアが、決定論的原因故障が無いことを証明する方法。事実上ルート 3S は現実的方法ではない。
(S は、決定論的安全度を意味する。)

(2) ハードウェアの安全構造の制約

安全機能として要求できる最も高い安全度水準は、２つのルート(以下のルート 1H、2H)の内の１つを選択するで求めることが出来る。

ルート 1H；	ハードウェアフォールトトレランス(HFT: Hardware Fault Tolerance)と安全側故障割合を算出する方法
ルート 2H；	規定された安全度水準に対して、更に高い信頼性水準とハードウェアーフォルトトレランス(HFT)に関するエンドユーザからフィードバックされたコンポーネントの信頼性データに基づく方法

ア ルート 1H

設計・開発の安全機能において、ハードウェア・アーキテクチャと安全側診断率故障割合(SFF)により、安全度水準の最大値の制限がある。

ハードウェア・アーキテクチャは、冗長化の形式から HFT の値で表される故障に対する許容度で表す。

HFT と SFF による制約は、安全機能を実行するハードウェアがタイプ A、タイプ B の 2 通りがある。

イ タイプ A,B

（ア） タイプ A

要求される安全機能を達成するためのコンポーネントに対し、要素が以下の条件であれば、タイプ A とする。

ⅰ．コンポーネントのすべての故障モードが正しく定義されている。

ⅱ．フォールト状態での要素の挙動が、完全に決まっている。

ⅲ．「検出された」と「検出されない」危険側故障が要求される故障確率を満たしていることを示す十分な信頼できる故障データがある。

タイプ A の電気、電子コンポーネントは、リレー、抵抗、コンデンサ、コイル、トランジスタやダイオードなどのディスクリート部品が主に相当する。

（イ） タイプ B

要求される安全機能を達成するためのコンポーネントに対し、要素が以下の条件であれば、タイプ B とする。

ⅰ． １つ以上の構成要素のコンポーネントの故障モードが正しく定義されていない

ⅱ．フォールト条件の下での要素の挙動を完全に決められない

ⅲ．「検出された」と「検出されない」危険側故障が要求される故障率の根拠となる信頼性データが不十分である。

タイプ B のコンポーネントは、タイプ A 以外のコンポーネントである。主に、IC や LSI などが該当する。

ある要素内のコンポーネントの少なくとも 1 つがタイプ B 要素の条件(故障モードの定義が不十分)に適合している時、その要素は、タイプ B とである。

具体的には、プリント板で構成される要素に 1 つでも IC が使用されていれば、そのプリント板は、タイプ B である。

ウ SFF と HFT の関係表

表 5-3 タイプ A　安全関連要素やサブシステムで許される安全度水準の最大値

要素の SFF	HFT(ハードウェアフォールトトレランス)		
	0	1	2
< 60 %	SIL 1	SIL 2	SIL 3
≥ 60 % – < 90 %	SIL 2	SIL 3	SIL 4
≥ 90 % – < 99 %	SIL 3	SIL 4	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

表 5-4 タイプ B　　安全関連要素やサブシステムで許される安全度水準の最大値

要素の SFF	HFT		
	0	1	2
<60 %	不可	SIL 1	SIL 2
≥ 60 % – <90 %	SIL 1	SIL 2	SIL 3
≥ 90 % – <99 %	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

（ア） ハードウェアフォールトトレランス（HFT）

(以後、HFT：Hardware Fault Tolerance(ハードウェアの故障状態の許容度のこと))

に関する要求事項

HFT は、0 以上の数値で表される。HFT N は、「N+1」個以上のチャンネルで構成された冗長化構成を表している。

「N+1」個以上のチャンネルで安全機能の喪失となるフォールトが起きた時、正常な動作を維持できるチャンネル数の最小値が N 個ということである。

逆に言えば、N+1 チャンネルの冗長化構造の安全機能の内 1 つのチャンネルが、機能喪失すると N 個のチャンネルとなり、まだ、正常動作できるが、更に機能喪失チャンネルが発生し、N-1 個のチャンネルになった時、正常動作できなくなるなら、正常動作できるチャンネル数は N 個であるので、HFT N になる。

このような冗長化チャンネル構成を M oo N 構成(m out of n)と呼ぶ。

一般的には HFT は、'n-m'で求められ、HFT n-m となる。

設計工程によっては、HFT を考慮しないでハードウェア安全度を決めることがある。その場合、故障診断、自己診断のようなハードウェアフォールトの影響を制御できる方法が必要である。言い換えれば、フォールト状態を診断で検出し、危険状態を回避し、安全側へ移行する手段が必要ということである。

故障の中には、ある 1 つの故障が起きるとそれが引き金で次々と故障や不具合が将棋倒し的に発生することがある。このような場合は、因果関係がはっきりしていれば最初の故障を単一故障とし、将棋倒し的に発生した故障はカウントしない。

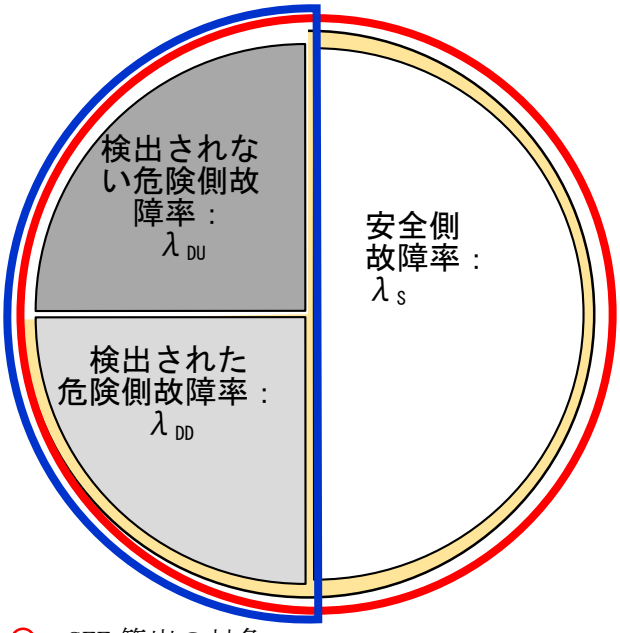


図 5－6　故障の分類

（イ） SFF(Safe Failure Fraction：安全側故障割合)

要素やサブシステムの故障は、故障解析によって、安全側故障率、自己診断によって検出された危険側故障率、検出されない危険側故障率に分類できる（図 5-6)。

検出された危険側故障率は、検出後、要素やサブシステムの安全機能に対し、発動を要求(デマンド)すれば、予め決めた安全状態に移行することができる。このため、SFF の計算では、安全側故障と同じ扱いをする。

一方、検出されない危険側故障率は、安全状態に移行できず、危険状態となる。

故に、SFF は、電子等制御安全関連システムの故障の内、検出されない危険側故障率を除いた故障率の割合となる。

$SFF=(\Sigma \lambda_{DD}+\Sigma \lambda_{S})/(\Sigma \lambda_{DU}+\Sigma \lambda_{DD}+\Sigma \lambda_{S})$

λ	*D：検出された	*U:検出されない	故障率の統合	
S*：安全	λ_{SD}	λ_{SU}	λ_{S}	安全側故障
D*：危険	λ_{DD}	λ_{DU}	λ_{D}	危険側故障

λ_{DU} の D は、「危険」の意味、U は、「検出されない」の意味。

λ_{DD} の先頭の D は、「危険」の意味、D は、「検出された」の意味：「検出できる」ではない。

λ_S の S は、「安全」の意味。

安全側故障は、自己診断で検出された故障と検出されない故障があるので、

$\lambda_S = \lambda_{SD} + \lambda_{SU}$

と表すことができる。しかし、λ_{SU} であっても危険側故障にならないので、2 つ合わせて λ_S と記述するのが一般的である。同じように危険側故障は、検出された危険側故障と検出されない危険側故障を統合したものであるので、

$\lambda_D = \lambda_{DD} + \lambda_{DU}$

と表すことができる。

（ウ） DC:診断カバー率(Diagnostic Coverage)

DC は、診断カバー率であり、危険側故障の内、検出可能な危険側故障の割合である。

$DC = \Sigma \lambda_{DD} / (\Sigma \lambda_{DD} + \Sigma \lambda_{DU}) = \Sigma \lambda_{DD} / (\Sigma \lambda_D)$

となる。ここに、$(1\text{-}DC) = \lambda_{DU} / \lambda_D$ である。

自己診断で行われる診断には、表 5-5 の項目が一般的に挙げられるが、診断内容はアプリケーションに依存する。

表 5-5 診断試験の項目の主なもの

No.1	冗長システムの相互信号比較、相互監視のような比較チェック、
No.2	メモリチェックサムのような診断
No.3	I/O 信号へのチェックパルスによる導通試験
No.4	アナログ信号の連続監視。規定の信号範囲にあるかのモニタによる範囲外故障検出
No.5	電源投入時のステータスチェック、電源電圧チェック、ウォッチドグの動作確認、論理部試験、I/O 部動作確認、メモリチェック、アプリケーション特有な仕組みのチェック

（エ） ＳＦＦの信頼性の確認

ハードウェアフォールトトレランス(HFT)が 0 のサブシステムにおいて、安全機能又は安全機能の一部を高頻度作動要求モード又は連続モードで動作する要素(サブシステムを構成するある機能のグループ)の安全側故障割合が、下記のどちらかの場合、その要素のＳＦＦは、信頼できない可能性がある。

ⅰ．診断テスト間隔と作動要求(デマンド)より安全機能が動作し、安全機能を達成するまでのプロセス合計時間がプロセスセーフティタイムより長い場合。

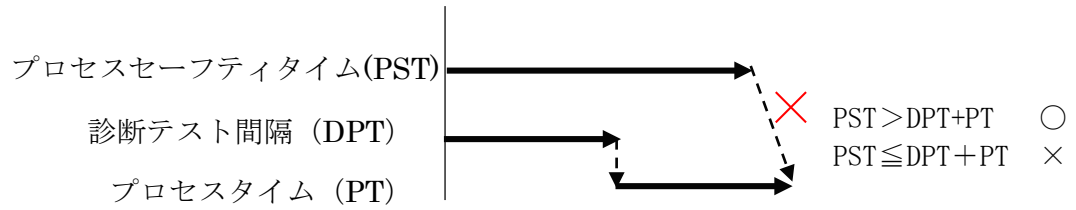


図 5-7　プロセスセーフティタイムとプロセス合計時間

プロセスセーフティタイムは、安全機能発動のデマンド発生から安全状態になるまでの時間である。これは、安全要求仕様で決定する。

診断テスト直後に故障が生じた場合、次の診断テストまで故障が検出できないので、最悪値の診断テスト時間で評価する。

ⅱ．高頻度作動要求モードである時、作動要求(デマンド)率に対する診断テスト率の比

が 100 以上である場合。
（作動要求率は，作動要求が発生するまでの時間の逆数。診断テスト率は，診断テスト平均間隔の逆数。）。
作動要求間隔：DT　診断テスト間隔を DPT とする。
作動要求率：1/DT　診断テスト率：1/DPT　(1/DT)/(1/DPT)=DPT/DT＞100%は×。
このことは、ある時間内のデマンド回数と診断テスト回数を比べた時、デマンド回数より診断テスト回数が多くなければならないことである。

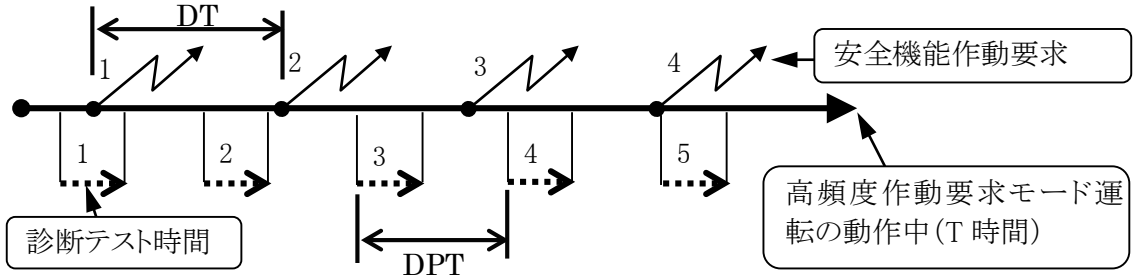


図 5-8　作業要求回数と診断テスト回数

(3) SIL の簡易決定

ア　サブシステムの直列接続

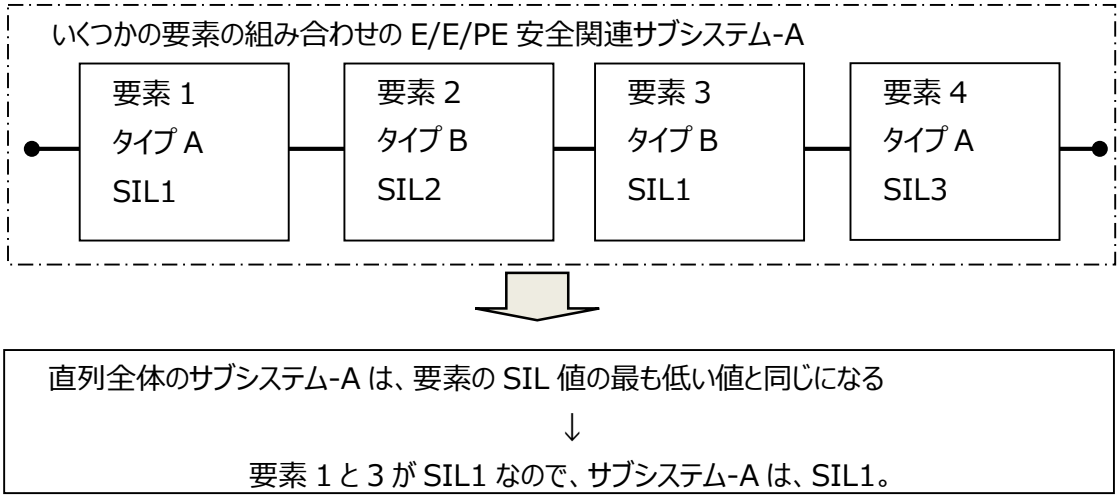
安全関連システムのサブシステムにおいて、サブシステムの中でいくつかの要素が直列的に組み合わさっている場合、そのサブシステムの SIL 値は、もっとも低い SIL 値と同じになる。
以下、表 5-6 及び図 5-7 を例に説明する。

（ア） 直列接続の接続例

表 5-6

例	要素 1、2、3、4 で構成された単チャンネルのサブシステムで実行されている安全機能があるとする。これらの要素は、HFT の制約を満足しているとする。
	要素 1：タイプ A、HFT 0 で SFF は<60%　⇒　SIL1
	要素 2：タイプ B、HFT 0 で SFF は 90%～99%未満　⇒　SIL2
	要素 3：タイプ B、HFT 0 で SFF は 60%～90%未満　⇒　SIL1
	要素 4：タイプ A、HFT 0 で SFF は 90%～99%未満　⇒　SIL3

a．直列接続の計算による求め方



SIL 値を簡易方法で求めず、計算で求める場合は、図 5-9 に示すようになる。

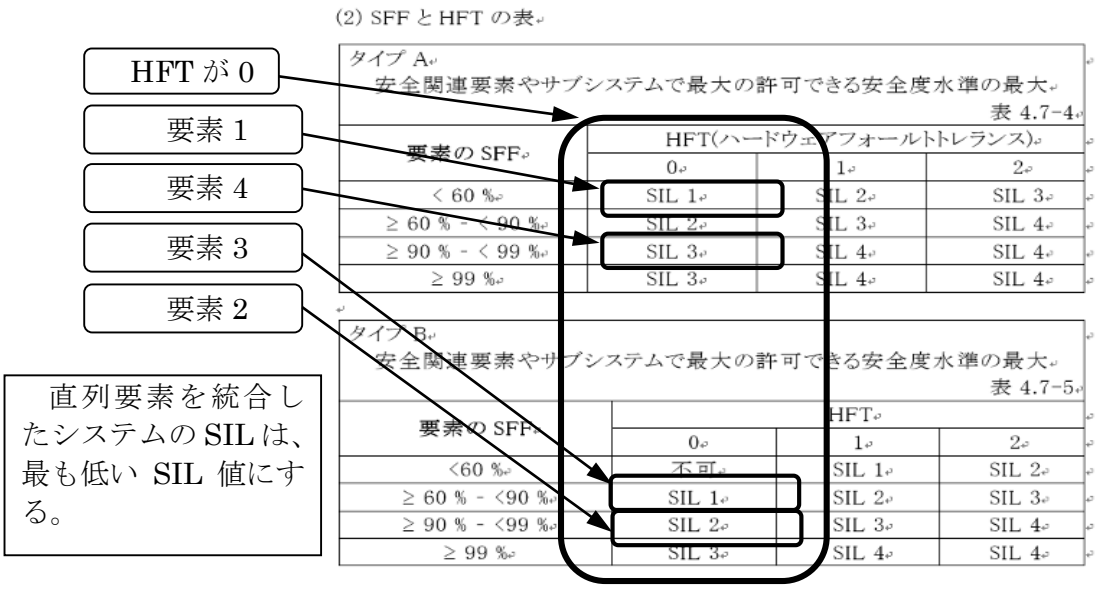


図 5-9　直列要素の SIL 決定の補足図

（イ） 複数のサブシステムの組み合わせの SIL の決定について

並列の要素で組み合わされた安全機能の安全関連システムのサブシステムにおいて、安全度水準は、以下の手順によって決定できる。

並列の要素は冗長化された要素とする。

ⅰ．並列の要素の中の最も高い SIL 値の要素を選択する。

ⅱ．並列の要素を合わせたサブシステムの HFT の値 N を出す。

ⅲ. 最も高い SIL 値に HFT の N 値を加える。これが求める SIL 値となる。ただし、SIL 値は 4 が上限である。

a．複数のサブシステム組み合わせの SIL の決定の例

並列組み合わせを含むグループ化の解析例を図示で説明する。

この組み合わせは、特定の安全機能を 2 つのサブシステム X,Y で実行していると想定する。

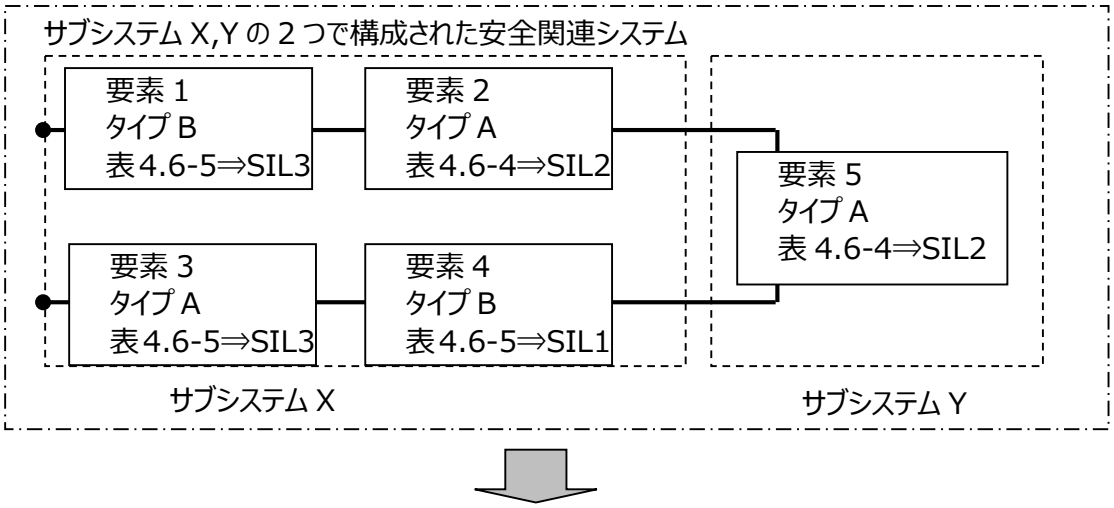
X は、要素 1、2、3 と 4 を含んだサブシステム、Y は単一の要素 5 のサブシステムとする。サブシステム X の中の並列のチャンネルは、サブシステ X の安全機能の一部を実

行し、要素 3、4 とは独立している。一方、要素 3、4 も同様である（表 5-7）。
安全機能は、以下のように実行されている。

b．要素の並列接続の例

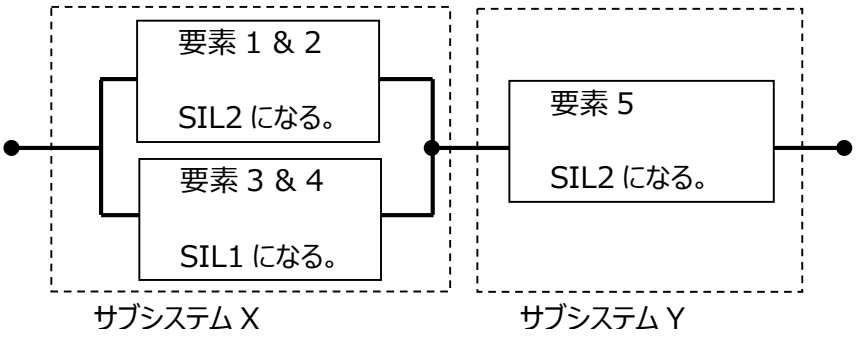
表 5-7 SIL 計算の手順

前 提 条件	1	要素 1、要素 2 のどちらかがフォールトを起こすとする(要素 3 と 4 の組み合わせが安全機能を実行する)
	2	要素 3、要素 4 のどちらかがフォールトを起こすとする(要素 1 と 2 の組み合わせが安全機能を実行する)
想 定 条件	1	要素 1：タイプ B、HFT 0 で SFF は≧99% ⇒ SIL3
	2	要素 2：タイプ A、HFT 0 で SFF は 60%～90%未満 ⇒ SIL2
	3	要素 3：タイプ A、HFT 0 で SFF は 90%～99%未満 ⇒ SIL3
	4	要素 4：タイプ B、HFT 0 で SFF は 60%～90%未満 ⇒ SIL1
	5	要素 5：タイプ A、HFT 0 で SFF は 60%～90%未満 ⇒ SIL2



c．要素 1，2 の統合：

要素 1，2 は、それぞれ SIL3、SIL2 の要求事項を満足している。よって、要素 1 & 2 は、SIL2 となる。



d．要素 3，4 の統合：

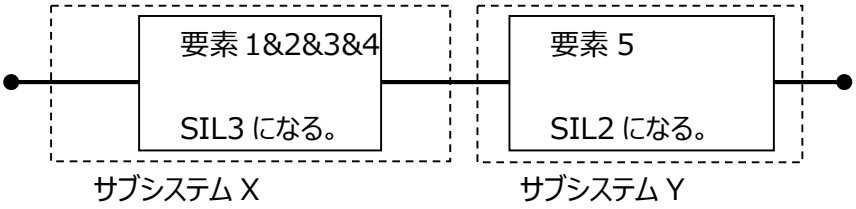
要素 3，4 は、それぞれ SIL3、SIL1 の要求事項を満足している。よって、要素 3 & 4 は、SIL1 となる。

さらに、構造をまとめて

e. 要素 1 & 2 と要素 3 & 4 の統合：

並列の要素の安全機能で要求可能な安全度水準の最も高い安全度水準のチャンネルを選ぶ。

その後、並列チャンネルの要素の新しい HFT の値 N を求め、並列チャンネル内の要素の安全度水準の最高値に N を加える。



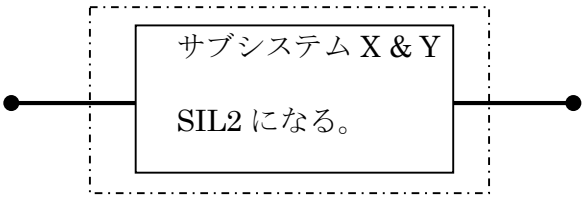
f．最も高い安全度水準のチャンネル：要素 1 & 2 ⇒ SIL2

HFT の値 N ：サブシステム X は、2 つの冗長化された並列チャンネル(1oo2)の組み合わせなるので HFT 1 となる。故に N=1 である。

サブシステム X の安全度水準は、SIL(2+N)=SIL(2+1)=SIL3 となる。

サブシステム X と Y は、直列でそれぞれ SIL3 と SIL2 である。

結局、直列要素サブシステム X,Y を統合した構造となる。



g．安全関連システムとして、安全度水準の最大値は、その安全機能に対して、SIL2 が得られる。

h．SFF・HFT 表と接続の関係（図 5-10）

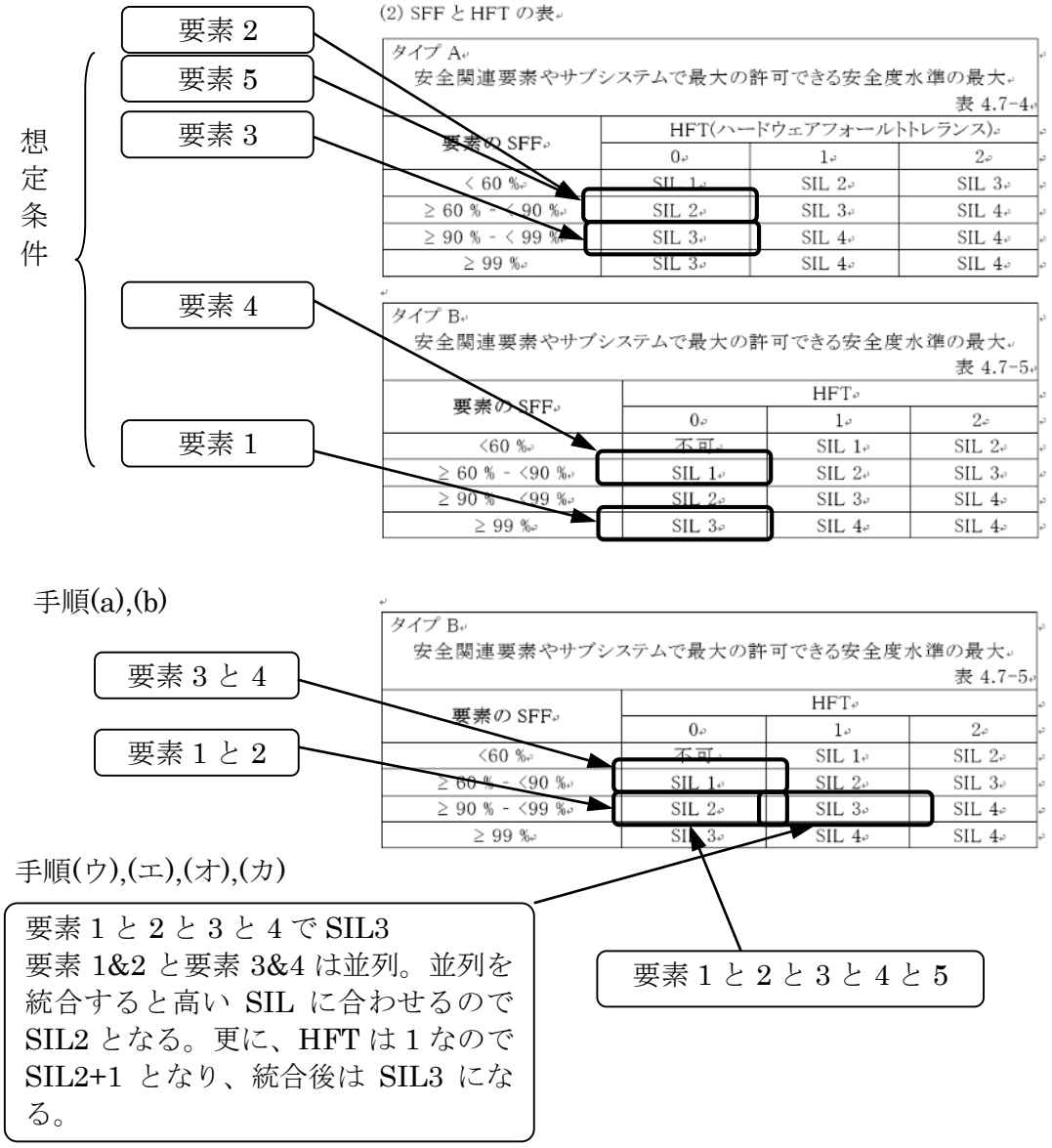


図 5-10　要素の SIL 決定の補足図(SIL の変遷)

この SIL の簡易決定法は、PFD 又は PFH を求めて計算する時と結果が異なる場合がある。その時は計算で求めた結果を優先する。この方法は、あくまで簡易的方法である。

(4) ルート 2H

ルート 2H は、フィードバックされた信頼性データに基づく方法である。

ア　統計的制約条件

ルート 2H を選択した場合、ハードウェアのランダム故障の影響を定量化することが必要である。その時、使用される信頼性データは、以下の条件である。

ｉ．　類似のアプリケーションや類似の環境で使用されている要素のフィールドフィードバックを基にする。

ⅱ．国際規格(例えば、IEC 60300-3-2(JIS C 5750-3-2)や ISO 14224)に従って収集したデータを基にする。

・JIS C 5750-3-2：ディペンダビリティ管理－第３－２部：適用の指針－フィールドからのディペンダビリティデータの収集

ⅲ． 以下についても見極め、信頼性を評価する
・フィールドフィードバックデータの量
・専門家の判定の結果
・信頼性確認試験の実施
計算に使用するそれぞれの信頼性変数(e.g.故障率)の平均値や不確定性レベルについては、90%信頼区間での評価が最低条件である。

（ア） 統計法使用の注事項
ⅰ．出版された規格に記載されている関連の構成要素の信頼性データの使用が推奨される。
ⅱ．故障率λの 90%信頼区間が望ましい。
ルート 2H の選択では、目標機能失敗尺度（PFDavg または PFH）の計算は、信頼性データの不確実性を考慮する。目標機能失敗尺度の信頼区間が 90%より大きくなるまで改善される必要がある。

(5) ハードウェアランダム故障の影響の定量化

安全関連システムにおいて、各安全機能の安全度は、機能失敗尺度で評価され、それはランダムハードウェア故障(ソフトエラー(注)を含む)とデータ転送プロセス要求事項の達成で推定される。それは、安全関連システムの安全要求仕様で要求された目標機能失敗尺度と同等であるかより小さくあるべきである。

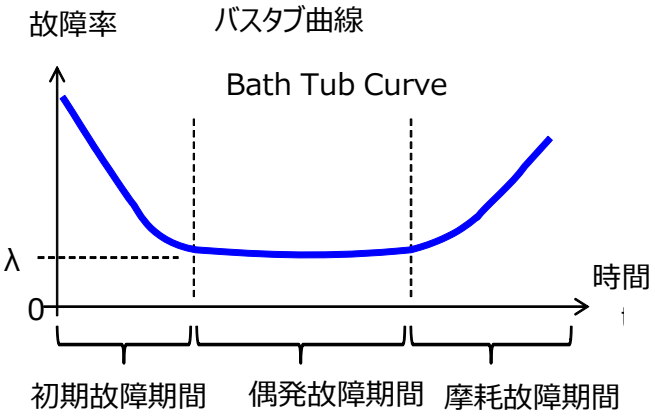


図 5-11　故障率曲線

このことが達成されたことを証明するため、安全機能の信頼性予測で PFD、PFH を求め、当初の目標機能失敗尺度と比較する。
注：ソフトエラーは、ソフトウェアの不具合ではなく、宇宙線や放射線(多くは封止樹脂の炭素同位元素による)の影響で半導体内のメモリやロジックの情報が一時的に反転する不具合で、再実行で正常に戻るような一時的故障として取り扱う。

ア　ランダム故障について

(ア)故障率曲線
故障率曲線は、機器や装置の時間経過 t に伴う故障率 y (t) の変化を表した曲線である。
曲線の形が洋式の風呂に似ていることからバスタブ曲線と呼ばる。バスタブ曲線は時間の経過による故障率の変化から初期故障期間、偶発故障期間、摩耗故障期間に分けられる（図 5-11)。

a．初期故障期間：
さまざまな要因があるが、設計、製造工程が未習熟のまま初期工程で作りこまれてしまった欠陥により、使用開始とともに劣化、故障が発現する期間。
この領域では故障率は時間の経過とともに低下し、やがて安定した状態に移っていく。

b．偶発故障期間：
不良品が初期故障期で十分取り除かれてしまった後、故障がごく稀にしか発生しない

安定した期間のこと。
この時期の領域では故障率は時間の経過に関係なく、ほぼ一定（=λ）とみなされる。

c．摩耗故障期：
部品などに摩耗や劣化が蓄積してきて故障が増加してくる期間である。この時期は、それまでの使用状況によって変化する。部品の使用限界に近い使い方では、摩耗故障の期間に早く到達することになる。

イ　目標機能失敗尺度（target failure measure）

目標機能失敗尺度（target failure measure）は、安全要求事項により安全機能が達成すべき故障時の危険側機能失敗目標確率である。安全機能の運用モードにより 2 種類の危険側機能失敗目標確率がある。

ｉ．低頻度作動要求モード運用の場合
作動要求当たりの，安全機能の危険側機能失敗の平均確率 --------PFD
単位は回数　MTBF/T に相当。

ⅱ．高頻度作動要求モード運用又は連続モード運用の場合
時間当たり[1/h]の危険側機能失敗の平均頻度----------PFH
1/MTTFd に相当。

(ア)PFD の概要

PFD は、低頻度作動要求モードにおける安全関連システムの安全度水準を評価する指標値である。安全関連システムに安全機能作動要求が発生した時、要求された安全機能が作動しない確率を表している。

ｉ．PFD(Probability of Failure on Demand): 安全機能作動要求時の危険側機能失敗確率

ⅱ．PFDavg(Average probability of a dangerous failure on demand of the safety function): 安全機能作動要求時の危険側機能失敗確率の平均確率。

PFDavg の単位は回数である。プルーフ試験間隔の間で何回故障するかを表す。プルーフ試験間隔が２０年なら２０年の間の故障回数である。単純には(プルーフ試験間隔)T/MTBF(システムの修理をしながら運転する平均故障時間)と考えられる。

安全度水準を評価する指標は、PFDavg の算定である。
安全関連システムの故障率には、故障時危険状態にならない安全側故障率(λ_S)と危険状態になる危険側故障率(λ_D)がある。

危険側故障率(λ_D)は、診断試験によって検出される故障(DD 故障)率(λ_{DD})と検出されない故障(DU 故障)率(λ_{DU})で構成される。

PFD は、EUC 又は EUC 制御システムから作動要求が発生した時、安全関連システムの規定の安全機能が実行されない確率、安全が有効とならないアンアベイラビリティ(不可動率)である。

アベイラビリティは、故障の平均間隔と故障したときの平均修復時間を用いて次のように表すことができる。

A= MTBF (平均故障間隔)/ (MTTR (平均修復時間)+ MTBF)

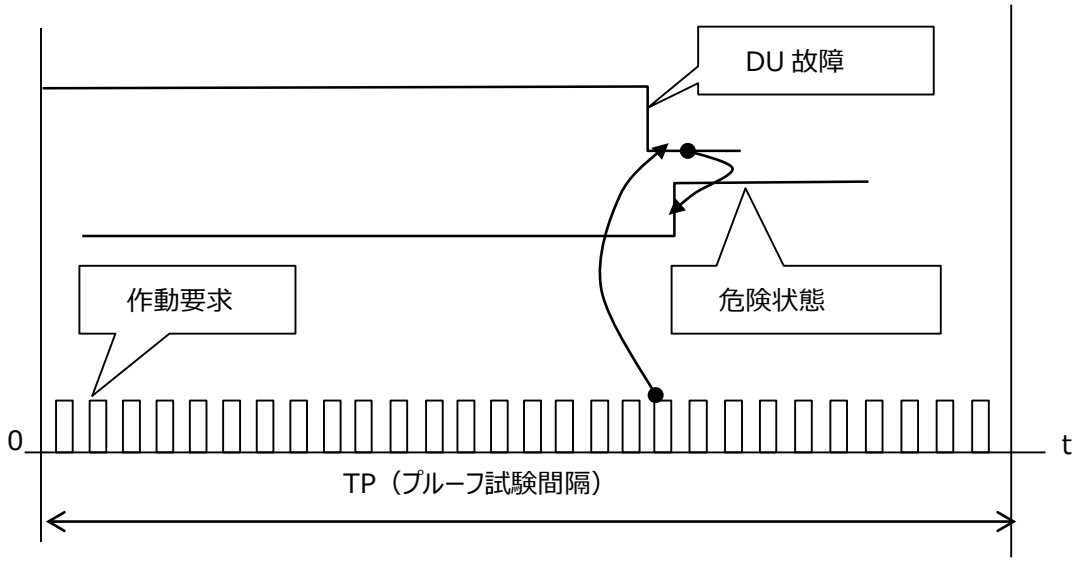
アベイラビリティとアンアベイラビリティの関係は以下のようになる。

U＝１－A

(イ)PFH について

PFH(Probability of Failure per Hour)は、安全機能の 1 時間当たりの危険側故障率のことである。安全機能が動作を開始してプルーフ試験までに安全機能が故障して危険側故障になるまでの平均故障時間 MTTF(Mean Time To Failure)、又は平均故障間隔 MTBF(Mean Time Between Failure)の逆数である（図 5-11）。

PFH は、作動要求が 1 回/年より多いか、連続的に発生する。この条件で、「プルーフ



PFH の故障発生

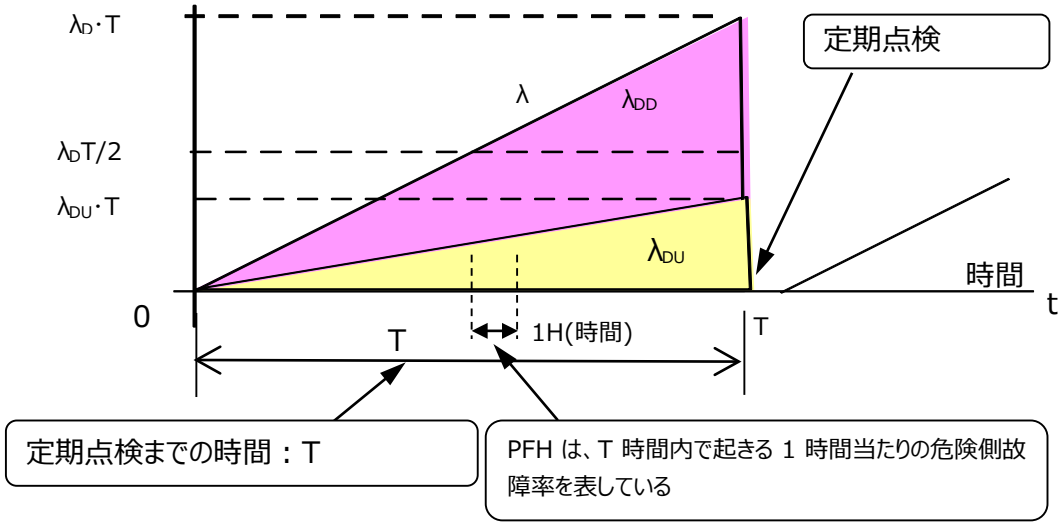


図 5-12　故障率の時間変化

試験間隔の間に DU(検出されない)故障が起きる確率」を表す（図 5-12)。

PFH は作動要求頻度が多いので、DU 故障発生で短時間に危険側故障になるとする。

PFH は、プルーフ試験までの期間中の故障頻度の平均値で表す。

$PFH(TP) = \int_0^T f(t)dt/TP$

f(t)は、不信頼度 F(t)を微分した関数である。

$f(t) = dF(t)/dt = d\{1-\exp^{(-\lambda t)}\}/dt = \lambda \exp^{(-\lambda t)}$

故に、次のようになる。

$PFH(T) = \int_0^T f(t)dt/T = F(T)/T = (1-e^{-\lambda T})/T$

$\lambda T<<1$ なら近似的に　$F(t) = 1-e^{-\lambda t} \fallingdotseq \lambda t$

$PFH(T) = (1-e^{-\lambda T})/T \fallingdotseq \lambda \cdot T/T$

$PFH(T) = \lambda$

λは、一般的に次のように表せる。

$\lambda = 1/MTBF$　又は、1/MTTF

MTBF：平均故障間隔　又は、MTTF：故障までの平均時間

PFH は、簡単に言えば、安全システムの危険側故障率である。(危険側故障になる平均

故障時間 MTTFd)/T(プルーフ試験間隔)で表せる。

(ウ)共通原因故障

a．1oo2 の共通原因故障

2 チャンネル以上の多重チャンネルの場合、共通原因故障を考慮して安全関連システムの危険側故障率、PFD、PFH を求める。

共通原因故障は 1 つの故障原因で複数のチャンネルがほぼ同時に故障になり、安全状態への移行ができず、危険状態になる故障のことを言う。

共通原因故障と安全機能を実行している 2 つのチャンネルの信頼性ブロック図(RBD)は、図 5-13 のようになる。

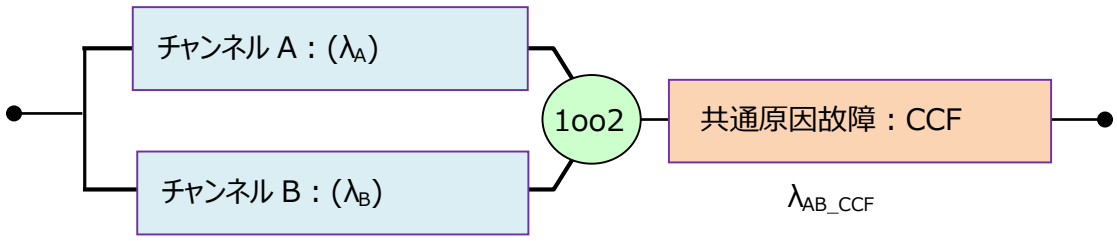


図 5-13　共通原因故障のブロック図

b．共通原因故障を加味した故障率

共通原因故障は、冗長化されたチャンネル A の故障とチャンネル B の故障の同時故障なのでチャンネル A とチャンネル B ともに同率と考えられる。この率を β で表す。図 5-14 の集合図から、共通原因故障率は、β(λA+λB)/2 である。

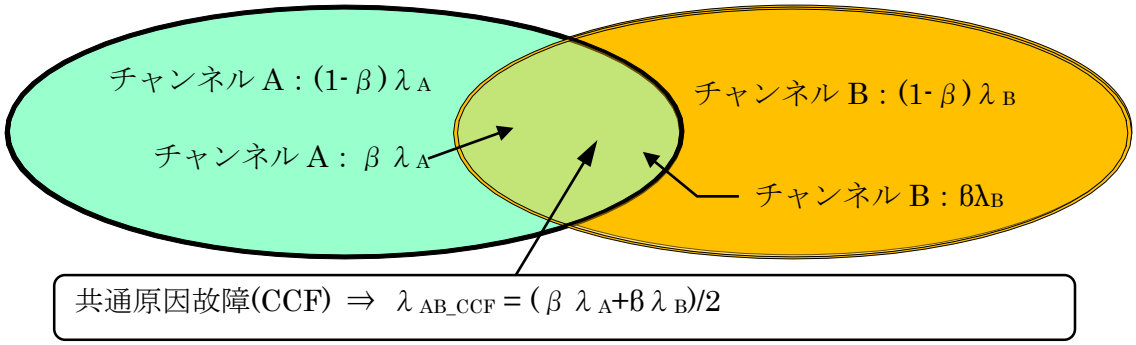


図 5-14　共通原因故障の集合図

チャンネル A　故障率:(1-β)λA＋βλA ＝λA

チャンネル B　故障率:(1-β)λB＋βλB ＝λB

共通原因故障 CCF の故障率は、β(λA+λB)/2　となる。この場合の信頼性ブロックの論理は図 5-15 のようになる。 ¥

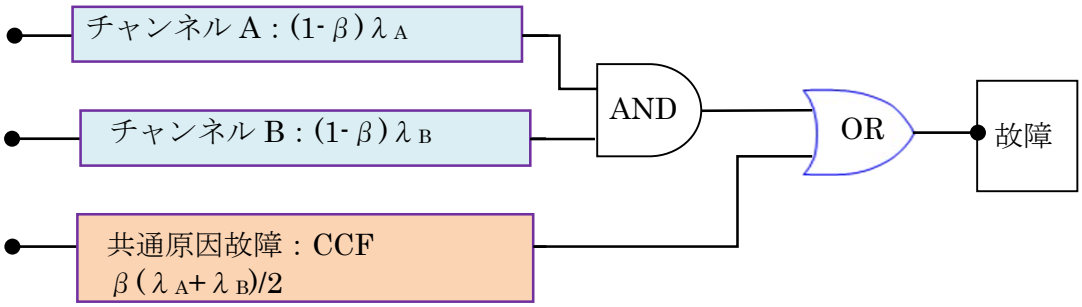


図 5-15　共通原因故障率を入れた RBD の論理図

(6) 共通原因故障のβ、β_Dの定量化

共通原因故障は、1つ以上の事象により、多重チャンネル及び冗長システムチャンネルシステムの中で2つ以上の分離されたチャンネルが同時故障になり、それがシステムの故障につながるものである。

ア　共通原因故障の検討

（ア）　共通原因故障要因の検討

設計段階、又は安全機器導入段階で以下の項目に従って共通原因故障の要因を考慮する。

ⅰ．共通原因故障の因子β、β_D値の目標値を決める。

ⅱ．一般的に、共通原因故障の発生がランダム故障だけとは限らない。決定論的原因故障による故障が含まれるので決定論的原因故障対策を行う。

（イ）　故障の種類

ⅰ．ランダム故障

ランダム故障は、構成要素(部品、コンポーネント)に対して、時間的にランダムに発生する故障である。冗長システム、多重システムチャンネルの故障につながる。

ⅱ．決定論的原因故障

決定論的原因故障は、多くは設計段階の仕様不足、知見不足、試験不足により潜在的に組み込まれる。例えば、設計や仕様の誤り、ソフトウェアのバグ、ハードウェアの初期故障をもたらす外部ストレス、例えば、過度な温湿度、EMC、サージ、電源変動などがある。

潜在的に決定論的原因故障の要因を持っていると作動中に発生条件が揃うとその故障が発現する。

ⅲ．従属故障

ランダム故障に対する従属故障を評価する。ある部品が故障したらどんな機能故障になるか、FMEA等で評価する。

ⅳ．共通モード故障（CMF）

多数の設備項目が同じモードで故障するようなCCFの特殊な場合。

ⅴ．カスケード故障

故障を増殖させるもの。

1つの故障により次々に故障が連鎖して増えていくもの。最初の故障がわからなくなることが多い。（将棋倒し的故障）

イ　共通原因故障の抑制策

共通原因故障の抑制策の主方法は以下である。

ⅰ．危険側故障となるDU故障を減らすこと。即ち診断率を上げること。

ⅱ．信頼性を上げ、共通原因故障の影響を少なくする。

抑制策の例

ⅰ．診断カバー率(DC)を大きくし、検出されない故障(λDU)割合を低減する。

ⅱ．診断にクロスモニター(相互監視)を使用する。
冗長・多重チャンネルにおいて、一方のチャンネルの故障を他方のチャンネルで検出するクロスモニターを行う。クロスモニターにより、診断率が向上する。

ⅲ．診断試験の頻度を多くし、作動要求の前に共通原因故障を検出する。

ⅳ．信頼性が使用実績で明らかになったものを使用する。

使用実績としては、信頼性が認証されているもの、市場で多く受け入れられているもの、長期間危険側故障の発生していない実績のあるもの等が相当する。

ⅴ．冗長・多重チャンネルの相互間の独立性を高め、共通源故障の影響を少なくする。

（ア）　β因子

冗長・多重化チャンネルシステムにおいて、各チャンネルで診断試験を行っている場合、β因子を使って共通原因故障の影響を推定する。

危険側故障λ_Dは　$\lambda_D=\lambda_{DD}+\lambda_{DU}$である。

共通原因危険側故障率は次のようになる。

β因子として危険側故障率のλ_{DU}にβ、λ_{DD}にはβ_Dを与える。

共通原因故障率：$\beta\ \lambda_{DU}+\beta_D\lambda_{DD}$

ウ　β、β_Dの推定

β、β_Dは、IEC 61508-6 の表 D1(Table D.1 – Scoring programmable electronics or sensors/final elements)を利用して推定する。

（ア）　β、β_Dを求める手順

IEC 61508-6 付属書 D1 表の項目チェックにより論理サブシステム(LS)とセンサ・最終要素サブシステム(SF)のスコアを別々に求める。

ⅰ．スコアの集計

サブシステムごとに集計したスコア値は、βとβ_Dの初期値になる。(IEC 61508-6 付属書 D)

βの初期値β_{INT}は、S=X+Y より

β_Dの初期値$\beta_{D\,INT}$は、 $S_D=(Z+1)X+Y$ の式より合計を計算する。

X:共通原因故障が直接コンポーネントに及ぶものの係数

Y:決定論的原因故障に関係する係数

ⅱ．診断試験頻度による補正

Z 値は、D2、D3 表のマトリックスより求める。

D2 表は、論理サブシステムに該当する DC と診断試験間隔表である。

論理サブシステムの DC が高く、診断試験間隔が 1 分未満なら高い SD 値が得られる。

Z 値が"0”なら診断試験が不十分であることになる。

D3 表は、センサ・最終要素サブシステムの DC と診断試験間隔表である。

これによって、各サブシステムの S、S_D値が求まる。

ⅲ．スコア値によるβ_{INT}、$\beta_{D\,INT}$の推定

次に D4 表のマトリックスにより、S、SD 値によってβINT、βD INT 値が得られる。

ⅳ．ハードウェア・アーキテクチャ補正

共通原因故障は、ハードウェア・アーキテクチャにより影響度が異なることからハードウェア・アーキテクチャ MooN の換算表 D5 表によって、β_{INT}、$\beta_{D\,INT}$の係数が与えられ、最終的なβ、β_Dが求まる。

換算値によると、1oo2 であれば、$\beta_{INT}=\beta$、$\beta_{D\,INT}=\beta_D$、2oo3 では、$\beta_{INT}=1.5\beta$、$\beta_{D\,INT}=1.5\beta_D$である。

共通原因故障の発生確率を最小にするため、安全関連システムに予め、このチェックシートにある適切な手段を講じておけば、共通原因故障の故障率を減らすことができる。

IEC 61508-6 のスコア表の項目を表 5-8 に示す。

このスコア項目は設計開始段階から対応を行う。

β、β_Dの算出の詳細は、ボイラーマニュアルの第 3 章 PFDavg の項を参照するとよい。

(7) FMEDA

FMEDA((Failure Modes Effects and Diagnostic Analysis)は、安全システムにおける故障原因とその影響を詳細に解析する方法である。また、この解析は設計・開発の初期段階で行うことで、安全システムの弱い処を特定するのに効果的である。

表 5-8　IEC 61508-6　Table D.1 のスコア表の項目
I/O 部は、I：入力部　O:出力部

	評価項目	サブシステム		コメント	スコアの配点		
		論理部得点	I/O 部得点		設計方法	装置関連	運用関連
1	分離/隔離	10	10	配線分離/制御盤収納		10	
2	多様性/冗長性	20	20	設計の方式、試験方法、保守方法、制御方式の 2 重化、多重化	16		4
3	複雑さ/設計/運用/成熟度/経験	10	10	安全情報の分離、使用実績、安全機器の単純性、定格の余裕度	4		6
4	評価データの解析とフィードバック	10	10	故障情報の再利用度、再発防止の仕組み			10
5	手順ヒューマンインターフェース	10	10	故障検出の仕組みの完全度、保守手順の完成度、ポカよけの程度、診断率の程度			10
6	適正/訓練/セーフティカルチャー	10	10	設計者、保守者の訓練、理解度向上			10
7	環境制御	10	10	要員の機密管理、環境試験と実環境の差、信号配線の独立性		3	7
8	環境試験	20	20	EMC,EMI、ESD のレベルの適正		10	

ア　FMEDA の例

FMEDA の例として、入力部の入力回路の一部（図 5-16）で説明する。

回路条件

条件 1：1oo2 構成の片側チャンネルの安全回路とする。

条件 2：信頼性ブロック図の内、入力部（センサ部：太枠）とする。

条件 3：故障率(λ)は、抵抗：10FIT、コンデンサ：40FIT、ホトカプラ：100FIT、IC：50FIT　とする。

条件 4：%FM は、故障モードであって、市場での発生割合のこと

この回路は、DC24V レベルの安全信号を入力し、ホトカプラを介して、DC24V 信号を論理部の DC3.3V 信号に変換する回路である。

%FM は、ある部品の故障モード(状態)の故障全体を 100%とした時、ある故障モード(例えば、短絡、開放、ドリフトなど)が市場でどのような発生割合かを表したものである（表 5-9)。

尚、故障モードは、以下を参照するとよい。

IEC 62061 Edition 1.0 2005(Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems) Table D.1 – Examples of the failure mode ratios for electrical/electronic components
JIS B 9960 付表 D

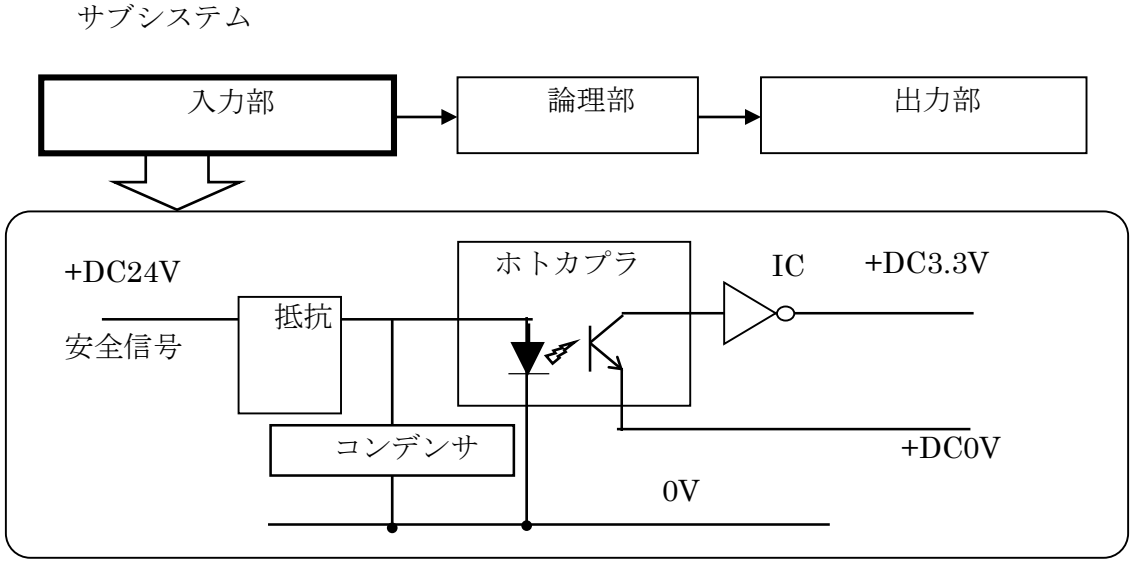


図 5-16　FMEDA 回路例

イ　FMEDA 表の記号

表 5-9　FMEDA で用いる記号

No.	記号		説明
1	λ		部品の故障率。単位は、FIT (フィット)。 FIT→(1/(10^9･h(時間))　10^{-9} ・1/h
2	DC		診断カバー率又は診断率。 回路内の部品の診断ができている割合。
3	故障 モード		部品の故障状態。 故障状態には PIN 間ショートやオープン、内部回路破損、ドリフト、発振などがある。
4	%FM		故障モードの市場発生割合。 例) : 抵抗の故障モード、短絡(ｼｮｰﾄ)、開放(ｵｰﾌﾟﾝ)の市場での発生割合(%データ)。 発生割合不明の場合は安全側故障/危険側故障の発生割合を 50%/50%とする。
5	安全/危険		該当の部品故障が発生した時、設計・開発の装置、機器が安全状態になるのか、危険状態になるのかの判定。
6	λ_{SD}、λ_{SU}、λ_{DD}、λ_{DU} は、以下の計算で求める。		
	1	λ_{SD}	安全側故障で検出された故障率。 λ×DC×%FM×(安全=1,危険=0)
	2	λ_{SU}	安全側故障で検出されない故障率。 λ×(1-DC)×%FM×(安全=1,危険=0)
	3	λ_{DD}	危険側故障で検出された故障率。 λ×DC)×%FM×(安全=0,危険=1)
	4	λ_{DU}	危険側故障で検出されない故障率。 λ×(1-DC)×%FM×(安全=0,危険=1)

ウ FMEDA表

表 5-10　FMEDA 表の例　(図 5-16 の回路例による)

部品	λ	DC	故障モード	%FM	安全/危険	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}
抵抗	10	60%	短絡(ｼｮｰﾄ)	50%	危険 *1	0	0	3	2
			開放(ｵｰﾌﾟﾝ)	50%	安全	3	2	0	0
コンデンサ	40	90%	短絡(ｼｮｰﾄ)	50%	安全	18	2	0	0
			開放(ｵｰﾌﾟﾝ)	50%	安全	18	2	0	0
ホトカプラ	100	60%	トランジスタ開放	25%	安全	15	10	0	0
			トランジスタ短絡	25%	危険 *2	0	0	15	10
			ﾀﾞｲｵｰﾄﾞｼｮｰﾄ	25%	安全	15	10	0	0
			ﾀﾞｲｵｰﾄﾞ開放	25%	安全	15	10	0	0
IC	50	60%	開放(ｵｰﾌﾟﾝ)	20%	安全	6	4	0	0
			短絡	20%	危険 *3	0	0	6	4
			常時 0 になる (ｽﾀｯｸｱｯﾄ 0)*5	20%	危険 *4	0	0	6	4
			常時 1 になる (ｽﾀｯｸｱｯﾄ 1)	20%	安全	6	4	0	0
			出力変動	20%	安全	6	4	0	0
合計（集計）						102	48	30	20

表 5-10 の値を集計の結果、SFF、DC は次のようになる。

$SFF=(\lambda_{SD}+\lambda_{SU}+\lambda_{DD})/(\lambda_{SD}+\lambda_{SU}+\lambda_{DD}+\lambda_{DU})$

$=(102+48+30)/(102+48+30+20)=180/200=90\%$

$DC=\lambda_{DD}/(\lambda_{DD}+\lambda_{DU})=30/(30+20)=30/50=60\%$

PFDavg、PFH は、⑨、⑪の式に $\lambda_{DD}=30$、$\lambda_{DU}=20$ を代入して求める。

注 : この表中の数値は、計算を分かり易くするため、実際のものとは異なる数値となっている。

*1:抵抗短絡により入力信号回路の漏れ電流が流れ､ホトカプラのホトダイオードが ON する。ホトカプラの ON により、信号 OFF でも ON 信号と読み違い、出力 ON 処理をする可能性がある。

*2:トランジスタ ON 故障により､入力信号 OFF でも ON 信号と読み違い､出力 ON 処理をする可能性がある。

*3,4:IC 出力 ON 故障により、入力信号 OFF でも ON 信号と読み違い、出力 ON 処理をする可能性がある。

*5 : スタックアット 0 とは､故障状態も含め何らかの原因で出力が 0V や"0"信号に引っ張られて"0"になっている状態のことである｡規格や解説書によっては､｢縮退又は固着｣と訳されているが､"0"に強制的になっている状態､" 0" に張り付けられている状態であると理解するとよい。スタックアット 1 はその逆。

スタックアット状態は、内部要因の場合もあるし、外部要因の場合もある。

(8) PFD、PFH の算出

ア　計算の手順

電子等制御安全関連システムの安全機能の低動作要求時の平均故障率は、安全機能を一緒に実行する全サブシステムの低動作要求時の平均故障率を算出し、加算して決定する。

ここで扱う確率は"1 "に比べ充分小さいので、これは次式で表現することができる（図 5-17 参照）。

$$PFD_{SYS} = PFD_S + PFD_L + PFD_{FE}$$

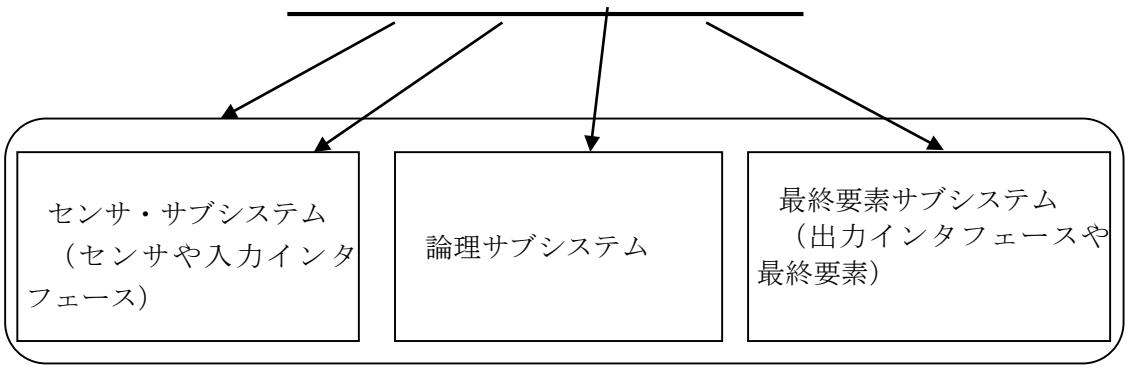


図 5-17　信頼性ブロックと PFD の関係

イ　使用する用語とその範囲（表 5-11）

表 5-11　用語の定義

略語	用語（単位）
TP	プルーフテスト（定期点検）間隔（時間）
MTTR	修復までの平均時間（時間）
MRT	平均修理時間（時間）。プルーフテストで見つかる DU 故障の修理時間
DC	診断カバー率。診断試験で検出できる部品故障の比率
β	検出されない故障率の内、共通原因故障とされる比率 β= 2×βD と仮定 (%)
β_D	検出された故障率の内、共通原因故障とされる比率(%) β= 2×βD と仮定
λ_{DU}	検出されない危険側故障率（1/時間）
PFD_G	センサ、論理、又は最終要素サブシステムの内の 1 つのサブシステムグループの低頻度作動モードの機能失敗時間平均確率
PFH_G	センサ、論理、又は最終要素サブシステムの内の 1 つのサブシステムグループの高頻度・連続モードの安全機能危険側失敗平均頻度（1/時間）
PFD_{SYS}	センサ、論理、最終要素サブシステム合計の低頻度作動モードの機能失敗時間平均確率
PFH_{SYS}	センサ、論理、最終要素サブシステム合計の高頻度・連続モードの安全機能危険側失敗平均頻度（1/時間）
λ	サブシステム 1 チャンネルの全故障率（1/時間）
λ_D	サブシステムの 1 チャンネル当たりの危険側故障率（1/時間）
λ_{DD}	サブシステムの 1 チャンネル当たりの検出された危険側故障率（1/時間）

λ_{DU}	サブシステムの 1 チャンネル当たり検出されない危険側故障率（1/時間）
t_{CE}	1oo1, 1oo2 アーキテクチャのチャンネルの平均不可動時間（時間）
t_{GE}	1oo2 アーキテクチャの選択されたグループの平均動作不能時間（時間）

ウ PFD, PFH 規格推奨式

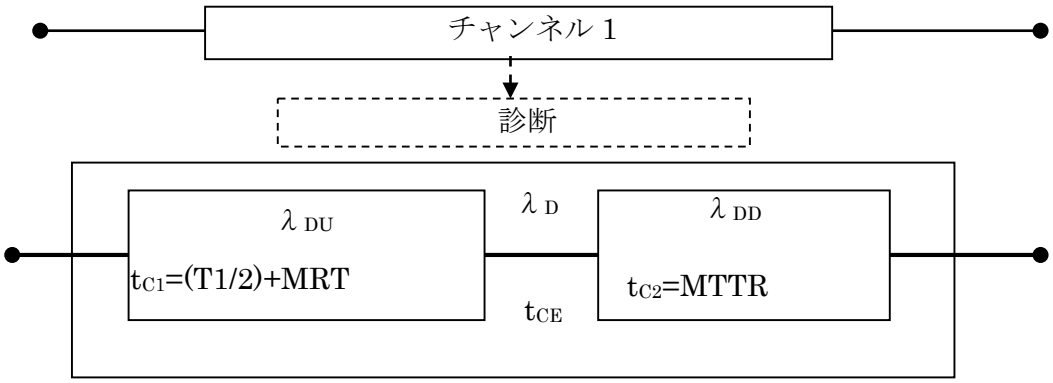
以下に上記パラメータに従った PFD、PFH の算出式を示す（表 5-12,-13）。

（ア） 1oo1 のアーキテクチャ

表 5-12　1oo1 ハードウェア・アーキテクチャ

1oo1 タイプ	HFT 0

このタイプは、1 チャンネルで構成されたハードウェア・アーキテクチャである。
比較的、安全度レベルの低いサブシステム、要素に組み込まれる。



1oo1 信頼性ブロック図

不可動時間：t_{CE}

$T_{CE}=(\lambda_{DU}/\lambda_D)\cdot\{(TP/2)+MRT\}+(\lambda_{DD}/\lambda_D)\cdot MTTR\}$

$PFD_G=\lambda_D t_{CE}=(\lambda_{DU}+\lambda_{DD})\ t_{CE}$

$PFH_G=\lambda_{DU}\cdot TP/TP=\lambda_{DU}$

a．PFD

不可動時間：$t_{CE}=(\lambda_{DU}/\lambda_D)\cdot\{(TP/2)+MRT\}+(\lambda_{DD}/\lambda_D)\cdot MTTR$

$=(1-DC)\cdot\{(TP/2)+MRT\}+DC\cdot MTTR$

DC：診断カバー率

$(1-DC)\cdot\{(TP/2)+MRT\}$：検出されない故障($\lambda_{DU}$)で停止している時間の平均

DC・MTTR：検出された故障で停止(平均修復時間)している時間

不可動時間は、検出されない故障で停止している時間と検出された故障で修理停止している時間の和である。

b．PFH

PFH_G は、TP 期間内で発生する機能失敗(故障)の平均確率であり、危険側故障になるまでの平均時間（MTTF または MTBF）の逆数である。

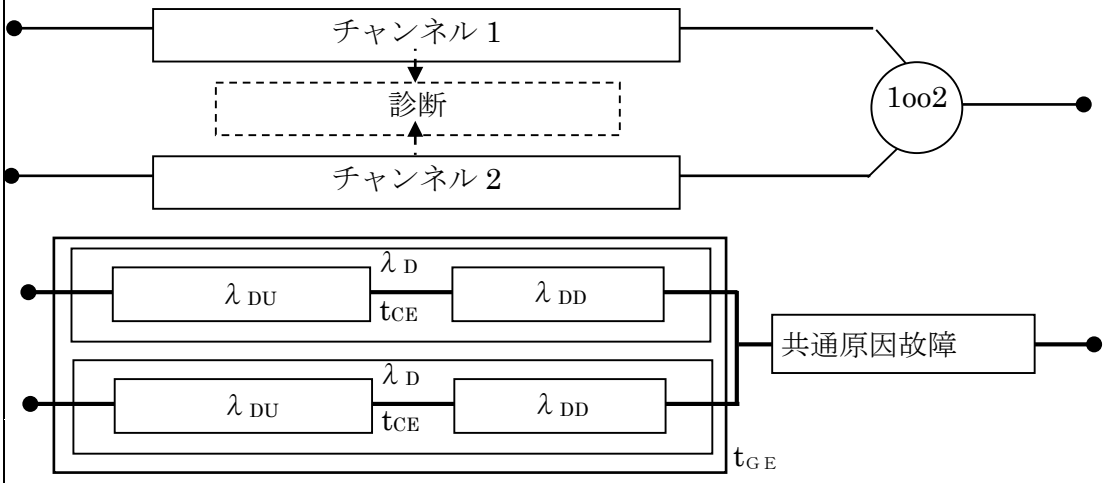
故に $PFH_G=\lambda_{DU}$　となる。

（イ） 1oo2 のアーキテクチャ

表 5-13　1oo2 ハードウェア・アーキテクチャ

1oo2 タイプ	HFT 1

このタイプは、2 つのチャンネルで構成された冗長化ハードウェア・アーキテクチャである。このアーキテクチャの低頻度動作モード要求時の平均故障率は、次式となる。



1oo2 信頼性ブロック図

$t_{CE}=(\lambda_{DU}/\lambda_D)\cdot\{(TP/2)+MRT\}+(\lambda_{DD}/\lambda_D)\cdot MTTR$

$t_{GE}=(\lambda_{DU}/\lambda_D)\cdot\{(TP/3)+MRT\}+(\lambda_{DD}/\lambda_D)\cdot MTTR$

共通原因故障を考慮して

$PFD_G=2\{(1-\beta_D)\lambda_{DD}+(1-\beta)\lambda_{DU}\}2t_{CE}\cdot t_{GE}+\beta_D\lambda_{DD}\cdot MTTR+\beta\lambda_{DU}\{(TP/2)+MRT\}$

$PFH_G=2\{(1-\beta_D)\lambda_{DD}+(1-\beta)\lambda_{DU}\}(1-\beta)\lambda_{DU}\cdot t_{CE}+\beta\lambda_{DU}$

a．PFD

$PFD_G=2\{(1-\beta_D)\lambda_{DD}+(1-\beta)\lambda_{DU}\}^2t_{CE}\cdot t_{GE}+\beta_D\lambda_{DD}\cdot MTTR+\beta\lambda_{DU}\cdot\{(TP/2)+MRT\}$

$2\{(1-\beta_D)\lambda_{DD}+(1-\beta)\lambda_{DU}\}^2t_{CE}\cdot t_{GE}$ は、TP 期間中の危険側故障率、後項の $\beta_D\lambda_{DD}\cdot MTTR+\beta\lambda_{DU}\{(TP/2)+MRT$ は共通原因故障率。

“$2\{(1-\beta_D)\lambda_{DD}+(1-\beta)\lambda_{DU}\}^2\cdot t_{CE}\cdot t_{GE}$” の意味は、以下である。

ⅰ．$\{(1-\beta_D)\lambda_{DD}+(1-\beta)\lambda_{DU}\}\cdot t_{CE}$

どちらかのチャンネルが故障する確率。

ⅱ．$\{(1-\beta_D)\lambda_{DD}+(1-\beta)\lambda_{DU}\}\cdot t_{CE}\cdot\{(1-\beta_D)\lambda_{DD}+(1-\beta)\lambda_{DU}\}t_{GE}$

どちらかのチャンネルの故障中に他方のチャンネルが故障し、危険側故障となる確率。

チャンネル 1 が故障し、チャンネル 2 が故障する場合とチャンネル 2 が故障し、チャンネル 1 が故障する場合の 2 通りがあるので、2 倍となる。

$2\times\{(1-\beta_D)\lambda_{DD}+(1-\beta)\lambda_{DU}\}2t_{CE}\cdot t_{GE}$

ⅲ．共通原因故障

共通原因故障は、2 チャンネル同時に起きることを想定。その時、故障原因は同じで同じ現象が起きるものとする。

この条件で、2 つのチャンネルに同時に故障が起きるので、危険側故障の発生確率は、1 つの故障として取り扱う。

共通原因故障の危険側故障率は、以下になる。

$\beta_D\lambda_{DD}\cdot MTTR+\beta\lambda_{DU}\{(TP/2)+MRT\}$

故に

$PFDG=2\{(1-\beta_D)\lambda_{DD}+(1-\beta)\lambda_{DU}\}^2t_{CE}\cdot t_{GE}+\beta_D\lambda_{DD}\cdot MTTR+\beta\lambda_{DU}\{(TP/2)+MRT\}$

注意：

チャンネル間の同時故障の確率は、２つの故障率の掛け算となり、小さな値になるが、

共通原因故障は、故障率と時間の掛け算なので、チャンネル間の同時故障の確率より大きな値になるのが一般的である。
危険側故障率は、共通原因故障の寄与が大きい。

b. PFH

$PFH_G=2\{(1-\beta_D)\lambda_{DD}+(1-\beta)\lambda_{DU}\}(1-\beta)\lambda_{DU}\cdot t_{CE}+\beta\lambda_{DU}$

PFH は、2 つのチャンネルでどちらかが λ_{DU} 故障になるか、どちらかの危険側故障 $\{(1-\beta_D)\lambda_{DD}+(1-\beta)\lambda_{DU}\}$が潜在し、作動要求が来ない状態で、他方が DU 故障になり、作動要求が派生した時、検出されない危険側故障が起きることを表す。

第 1 項の"2"は、チャンネル 1 が起きてからチャンネル 2 の故障が起きる場合とチャンネル 2 の故障が起きてからチャンネル 1 の故障が起きる場合の 2 通りがあることを表す。

共通原因故障は、共通原因故障原因により検出されない危険側故障が発生することを表す。　共通原因故障は、2 チャンネル同時に発生する。1 つの原因で発生するので、発生確率は、以下になる。

共通原因故障　⇒　$\beta\lambda_{DU}$

故に、

$PFH=\{(1-\beta_D)\lambda_{DD}+(1-\beta)\lambda_{DU}\}\cdot(1-\beta)\lambda_{DU}\cdot t_{CE}+\beta\lambda_{DU}$

この式は、同じ回路の冗長システムの式である。

(9) 決定論的原因故障の回避の要求

決定論的能力(SC)としての安全度に関わる決定論的原因故障回避の方策は、表 5-14 の遵守ルートのいずれか 1 つを達成することで適合できる。

表 5-14　ルート概要

ルート 1S	決定論的原因故障の回避のための要求事項と、決定論的原因故障を抑制するための要求事項を遵守する方法。
ルート 2S	装置の使用実績を証拠だてて要求事項を遵守する方法。
ルート 3S	既存のソフトウェアを使用する方法。

注.S は決定論的安全度を意味する

ア　ルート 2S、使用実績について

信頼性に関する大量な情報の幅広いユーザからのフィードバックデータは、市場実績(Field experience)の情報から、統計的な手法によりランク付けを行う。例えば、SIL1、2→"低"、SIL3→"中"、SIL4→"高"を適用する（表 5-15)。

表 5-15　市場からのフィードバックデータ

No.	ランク	最少運転時間と運転中の条件	最少実績種数	信頼限界
1	低	10,000h 安全に関わる重大な故障のないこと	10 種類	95%以上
2	中	高と低の中間。		
3	高	10,000,000h　最低 2 年の運転実績。 運転中、過去を含め、些細な事にわたり、安全に関わる重大な故障のないこと、それら故障について詳細な文書があること	10 種類	99.9%以上

ｉ．"低"レベルは、10,000 時間：

10 種類以上のアプリケーションで、約 1 年の運転実績(1 年=8760 時間≒10,000 時

間)で、その間、安全に関わる重大な故障がないこと
ⅱ．”高”レベルは、10,000,000 時間：
10 種のアプリケーションで約 10 年の実績があり、過去の運転の全ての変更事項の詳細な文書があり、その変更事項は安全機能に大きな影響がないことが条件で、統計的に 99.9%の正確な実績である必要がある。
ⅲ．“中”は、”低”と”高”の中間である。

イ　決定論的原因故障の回避のための技法又は手段

（ア）　管理による決定論的原因故障の抑制

決定論的原因故障は、人の行動、思考が起因となる故障、又は故障状態である。いわゆるヒューマンエラーに起因する。

全安全ライフサイクルの遂行ではすべてのフェーズで人が関わる。それ故、どこのフェーズでも決定論的原因故障の原因を作りこむ機会がある。特にハードウェア、ソフトウェア設計においては、決定論的原因故障原因を作りこまない、回避する方策の適用が必要である。

決定論的原因故障の要因の一つは人のミスである。人のミスを最小限に抑制するためには業務管理が必須である。以下に管理の要点を列挙する。

a．1 人作業を避け、二人以上で作業する
ⅰ．業務情報の共有化；会議、会合で情報を共有する。
ⅱ．管理者は、担当者の進捗を確認し、負荷の平準化を図る。
一人に負荷が集中し、設計の隅々まで目が届かなくなることを防止。

b. コミュニケーションを図る
ⅰ．関係部署との情報の共有化
ⅱ．情報共有化のため文書は分かり易く記述する。
・図式表現を使用
・箇条書き、分かり易い表現。
・概要から詳細仕様へ、
・機能別にモジュール化

c. 設計仕様では主要機能に付随する機能を見落とさない
・ハードウェアとソフトウェア間、サブシステム間、サブシステム内の各機能要素間のインタフェース仕様の明確化
・ハードウェアとソフトウェア、サブシステム、サブシステム内の各機能要素の事象発生順序、時間関係の明確化
・制御の同期性、事象発生の同時性の明確化。

d. 出来るだけ人の手を排除

自動化を図った安全機能の試験方法、保守時の正常さの確認方法を決め、そのため必要となるハードウェア、ソフトウェアは設計段階から仕様に入れ、開発を行う。

e. コンピュータ支援ツールの利用

人の手作業を排除する。
・仕様作成段階では、要件管理ソフトウェアなどコンピュータ支援ツールを利用し、仕様の欠落、考え違いによる誤仕様の発生を抑える。
・設計工程では、CAD などコンピュータ支援ツールを使用し、ヒューマンエラーの発生を抑える。
・仕様作成から設計段階、設計段階から試験までデータ変換を手作業で行う工程がない一貫したソフトウェアツールが望ましい。

f．計画を作成する

試験実施前に試験計画、試験項目、合否基準を決め、それに従って作業を行う。計画と違った場合、決められた変更手順を経て、責任者の承諾をもって作業を行う。

ⅰ．モジュール試験、統合試験、適合確認試験,妥当性確認試験では該当の試験フェーズより前の設計段階で試験計画(試験項目、試験手順、試験環境、試験器、試験者、試験プログラム等)を作成する。このことで、タイムリーな試験実施が行え、再現性が確保できる。

ⅱ．形式試験、即ち仕様、機能確認試験を行う

ⅲ．合否判定を試験実施前に決める。

ⅳ．試験機器は校正済みであること。バージョン管理も行う。

ⅴ．合格にならなった時の変更手順を事前に決めておく。

ⅵ．変更実施は、責任者の承認の元で行う。

ⅶ．仕様では、曖昧性を残さない。決まらない仕様は、何が決まらないか明らかにし、文書化する。

ウ　電子等制御システム設計要求仕様作成時の決定論的原因故障の回避

（ア）　ハードウェアに潜在する設計起因の決定論的原因故障の抑制

設計起因の決定論的原因故障は、設計に関係する仕様の誤解や仕様の欠落、過剰や設計者の力量不適格、関係部署とのコミュニケーション不足による情報共有不足などに起因する。そのような要因発生を極力抑制するため、下記のような項目の実施が必要となる。

a．管理面

決定論的原因故障の除去体制を構築する。

・ハードウェア・ソフトウェア設計・開発工程の管理

仕様の確認、進捗の確認ができる管理体制を作る

・規格、指針、法律、業界標準の遵守設計

・設計・開発工程のマイルストーンごとのデザインレビューの実施

b．欠落のない仕様と文書

・予見可能な誤使用を考慮した仕様作成。

・構造化設計による仕様と機能の役割分担の明確化と分かり易く欠落のない最適仕様作成

・モジュール化設計による安全機能の詳細仕様の明確化

・仕様や設計内容の分かり易さと理解しやすさのため準形式手法による文書の図形式表現。・

・コンピュータ支援ツールによる人為作業の低減

c．使用環境の耐性

安全機能を実行する装置・機器が以下のような悪い環境条件下の耐性を持ち、安全機能が誤動作しないこと。

悪環境に対する耐性の主な項目は以下である。

・電磁環境の耐性：電磁妨害、電磁放射、静電気

・電源変動の耐性：商用電源の変動、瞬停、雷サージ、電源遮断、電源投入、ラッシュ電流、誤配線、誤電圧投入等

・運搬、運用環境：振動(機械的振動、輸送中振動、走行中振動等)、衝撃(落下、衝突等)

・オペレータの操作ミスの対応：ボタン配置、ボタンの色(色覚異常対応すること)、ボタンの大きさ、表示メッセージの表現。

オペレータの力量を把握し、操作ミスを抑制しなければならない。

・周辺機器のエラー時の対応：退避しようとしたら扉が開かない、安全ネットワークが

故障し、正常信号が送られてこない時など。

エ　安全関連システムの設計時の決定論的原因故障の回避

決定論的原因故障の発生を抑制するため、決定論的原因故障が発生しても、その発生に対して、耐性のある設計仕様を持つことが必要となる。

ⅰ．保守性／試験性が良いこと

保守作業後、簡単に正確に安全機能が動作することが試験で確認できる仕様とする。試験方法は設計・開発工程で盛り込まれる。

ⅱ．人為的誤操作を考慮した設計

特にオペレータや保全者の能力とその限界に注意を払い、誤操作せずにオペレータや保全者がその責務を遂行できるような仕様に盛り込む。

・設計段階で予見可能な重大な誤操作を防止、排除する仕様を盛り込む。
・それらの仕様は完成前に別の関係者が確認すること
・オペレータ、又は保全者の操作ミスでかえって事態が複雑になり、容易に復旧できないことが起きることを想定し、その方策を盛り込む。

特に安全度水準が高い安全機能には、多様化ハードウェアが有効である。

（ア）　多様性のあるハードウェア

多様化の技法又は手段は主に決定論的原因故障に対する方策である。多様化では、入力と出力が同じではあるが、処理方法、使用部品が違うため故障率と故障タイプが異なり、同じ故障結果とならないハードウェア・アーキテクチャである。

比較的高い SIL に採用される技術である。多様化により共通原因故障の割合を抑えられ、高い SFF 値を得やすくなる。

低い安全度水準で多様性のあるハードウェアを使用する場合は、同じ機能を異なった設計で実行する 2 つ以上の項目、高い安全度水準では、異なった機能を実行する 2 つ以上の項目が必要である。

例えば、低い安全度水準であれば、温度検出として A 社と B 社の少し仕様の異なる熱電対を使用する。高い安全度水準であれば、A 社の熱電対と C 社の赤外線温度計を使用する。

オ　環境ストレスによる決定論的原因故障の抑制の技法又は手段

安全機能を実行する装置・機器は、その設置環境に適応しなければならない。安全機能の実行を脅かし、故障に至らしめる環境因子には、設計の段階から対応する必要がある（表 5-16）。

注　M:必ず実施すべき、HR:実施すべき、　R:実施が望ましい技法及び手段

（ア）　表の項目の概要説明

ａ．電源システムからのストレス

・電源遮断：停電による電源遮断、危険側故障検出による動力側電源遮断
　電源装置不具合による電源遮断、バッテリ不具合による電源遮断
・電圧変動：負荷変動による電源変動、電源装置不具合による変動、電源短絡による電圧変動、瞬停、バッテリの満充電・放電による変動、
・過電圧

表 5-16　環境ストレスによる決定論的原因故障の抑制

No.	技法又は手段	SIL 1	SIL 2	SIL 3
1	電圧低下、変動、過電圧、低電圧、AC 電源の周波数変動のような危険側故障の原因となる他の現象	M 低	M 中	M 中
2	電源ラインと信号ラインの分離	M	M	M
3	妨害に対する耐性の強化	M 低	M 低	M 中
4	温度、湿度、水、振動、塵埃、腐食など物理的環境への対策	M 低	M 高	M 高
5	プログラム順序モニタ	HR 低	HR 低	HR 中
6	温度上昇に対する対策	HR 低	HR 低	HR 中
7	多数の電線の空間的分離	HR 低	HR 低	HR 中
8	アイドル電流の考え方を明確にする。 継続的制御が、安全状態にするかその状態を維持するために必要としない電流	R	R	R
9	信号線の断線と短絡の検出の仕方	R	R	R
10	オンラインモニタによる故障検出	R 低	R 低	R 中
11	冗長化による試験	R 低	R 低	R 中
12	コード保護	R 低	R 低	R 中
13	逆転信号通信	R 低	R 低	R 中
14	多重化ハードウェア	－ 低	－ 低	－ 中

電源不具合による過電圧、1 次側 2 次側短絡、バッテリ充電回路の故障、電源配線間違い

・低電圧

電源遮断時、過負荷による定電圧、電源短絡、

・AC 電源の周波数変動

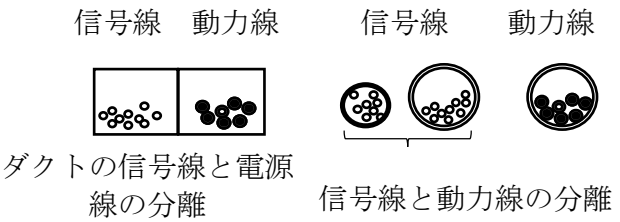
AC 周波数(50Hz、60Hz)の仕様間違い、ジェネレータの故障

低い安全度水準では、電源システムからのストレスにより、電源の過電圧などの異常が検出された場合、電源遮断により電源異常の影響を排除するか、二次電源への切り替えを行う。高い安全度水準では、異常部の遮断のような安全な遮断か、二次電源への切り替えによる電圧制御、又は電源遮断か二次電源への切り替えを行う。

b. 電源ラインと信号ラインの分離

電源ラインと信号ラインは分離し、別の配線経路とする。

電源ラインと信号ラインを接近並走した場合、クロスさせた場合、電源側の電磁ノイズが信号ラインに誘導される。特に高い周波数のノイズは誘導されやすく、信号ラインを通して、安全機能の論理処理部へノイズが入った時、部品の故障、誤処理につながる可能性がある。



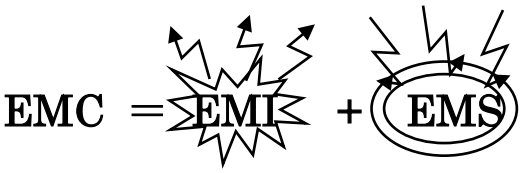
ダクトの信号線と電源線の分離　　信号線と動力線の分離

信号ラインに冗長化した安全信号が配線されている場合、冗長化した信号配線を同じケーブルや配線経路を通した時、同時にノイズの重畳や断線、短絡が起きるかもしれないので、冗長化した一方の信号線は、他方と分離配線することで共通原因故障の要因を回避することができる。

c. 妨害に対する耐性の強化

電磁妨害に対し、耐性がなければならない。

電磁妨害波耐性は、EMC で評価される。



EMC（電磁両立性）とは、電気・電子機器や装置から放出される電気的ノイズを抑え（EMI：Electro-Magnetic Interference)、かつ周囲から放射された電気的ノイズによって電気・電子製品が不具合を起こさない（EMS：Electromagnetic Susceptibility）ための 2 つの性能を言う。

電気・電子機器や装置から出る電気的ノイズは、放射電磁波(妨害電波)と呼ばれ、別の電気・電子機器に入り込んで悪影響を与えることがある。エミッション(emission)方策は、この妨害電磁波の放射を許容値以下にすることである。

どの安全度水準であっても EMC の強化が必要であり、それぞれの適用分野先の規格で定義されたレベル以上が必要である。

EMS は電磁感受性のことで電気・電子機器が電気的ストレス（電界、磁界、電圧、電流）に曝された時に耐えられる能力を言う。

EMI の許容値、EMS の耐性値は機器・装置の適応分野ごとに決められている。EMC 対策を行い、電磁環境での許容値、耐性を強化することは、安全性を維持するため必要なことである。EMC に関する許容値、耐性値は、適用分野ごとに経験的に決まっており、関連の規格に明記されていることもある。もし、無ければ類似の分野を参考にする。

要求される EMC の要求は、適応分野の要求事項に従う。

<u>主な EMC 試験</u>

・静電気放電イミュニティ試験(ESD)　JIS C 61000-4-2

人が静電気に帯電したまま安全機能を実行する装置・機器の導電部に触れるか近づいた場合、数万ボルトの静電気電圧が一瞬で放電し、その放電で誤動作する場合がある。その耐性を試験する。簡単な静電気対策は人が触れるところに導電材料を使用しないことである。

許容値の例：接触放電：±2kVto±8 kV　気中放電：± 2 kV to± 15 kV

・放射イミュニティ 試験 Rated,radio-frequency, electromagnetic field immunity:放射　　無線周波電磁界イミュニティ試験 JIS C 61000-4-3

無線設備から連続放射された電波や、さまざまな電磁波を発生する産業機器から放射された電磁波により装置本体の受ける影響を試験する

許容値の例：1V/m to 30V/m　80 MHzto 1000MHz　AM 変調 80%, 1kHz

・電気的ファストトランジェント／バーストイミューティ試験（Electrical fast

transient / burst immunity test）JIS C 61000-4-4

電源線や信号線に加わる、繰り返しの早い過渡的妨害を受けた場合の耐性評価試験

許容値の例：電源ポート：±0.5 kV to±4 kV,

信号・制御線ポート：±0.25kV to±2 kV

・サージイミュニティ試験 Surge immunity test JIS C 61000-4-5

電力システム統のスイッチング及び雷によるサージの急峻な立ち上がりの電圧による試験する。

許容値の例：±0.5kV to ±4kV:ライン-アース間、ライン-ライン間

・試験及び測定技術–無線周波電磁界によって誘導する伝導妨害に対するイミュニティ Immunity to conducted disturbances, induced by radio-frequency fields JIS C 61000-4-6

無線機器やその他電子機器から放射される電磁妨害波が安全機能装置・機器に接続されている伝導性ケーブルに作用する影響を試験する。

許容値の例：1V to 10V 0.15MHzto 80MHz AM 変調 80%, 1kHz

・電源周波数磁界イミュニティ試験(Power-frequency magnetic field immunity test) JIS C 61000-4-8

磁界の影響を受ける素子を使用している場合、導体を流れる電源周波数の電流または変圧 器から発生する磁界によって誤動作、故障しないかの影響を試験する。

許容値の例：50/60 Hz 連続磁界：lA/m to 100A/m 短時間磁界：300A/m to 1000A/m

・電圧ディップ、短時間停電及び電圧変動に対するイミュニティ試験(Testing and measuring techniques Voltage dips, short interruptions and voltage variations immunity tests) JIS C 61000-4-11

電源システム統の故障、又は急激な負荷変動によって起きる電源電圧の落ち込み(Dip)、短時間停電(瞬停)の影響を受けないことを確認する試験

許容値の例：電圧デッイップ：0%,1c ycle, I0 秒間隔で 3 回, 80%,300 cycles, I0 秒間隔で 3 回 短時間停電：0%,300 cycles,3 回

・CISPR22(VCCI)情報技術装置(ITE)の無線妨害波特性の許容値および測定法

電源ポート、 通信ポートの妨害波電圧と電流、筐体(3m 法)から放射されている妨害波が許容値以下であることを立証する。

・CISPR11 工業用・科学用・医療用の高周波装置に電磁妨害の許容値および測定法

電源ポート、筐体(10m 法)から放射されている妨害波が許容値以下であることを立証する。

(10) ディレーティング

ディレーティング(低減率)は、全てのハードウェア部品について考慮しなければならない。もし、ハードウェア要素、コンポーネントを仕様限界で使用、運転する必要がある場合、そのことの正当性(使う理由、その条件は、要素の仕様範囲で問題を起こさないこと)を文書化しなければならない。適切なディレーティングとしては、一般的に、1.5 倍の係数が使用される（図 5-18)。

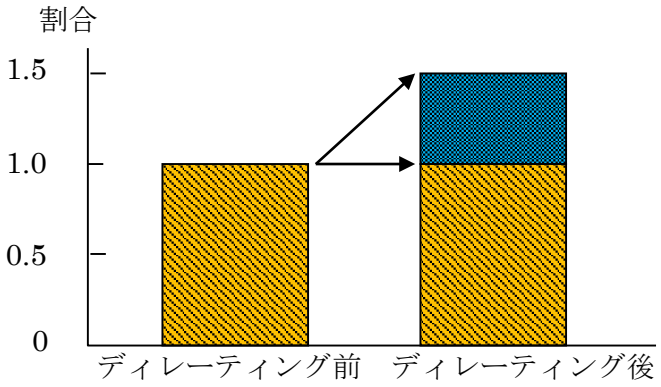


図 5-18　ディレーティング

(11)　データ通信の追加要求事項

ア　データ通信における通信欠陥

データ通信が、安全機能の実行方法として使用されている時、通信プロセスの残留欠陥率のような機能失敗尺度を算出する時、以下の項目に注意を払う必要がある。

ⅰ．伝送エラー: メッセージの破損
ⅱ．繰り返し　: 古いメッセージが繰り返し受信される
ⅲ．削除　　: メッセージが消去される
ⅳ．挿入　　: 別のメッセージが挿入される
ⅴ．再順序づけ: メッセージの受信順序を誤る
ⅵ．劣化　　: メッセージの内容が書き換えられる
ⅶ．遅延　　: 規定の時間内に通信が完了しない
ⅷ．偽装　　: （なりすまし）　認証されていない機器から信頼できない情報を受信する、又は、不正なアドレス指定を含む

ランダム故障となる安全機能の機能失敗尺度を算出する時、このデータ通信の機能失敗尺度にも注意を払う必要がある。

上記の通信欠陥の 1 つの偽装“masquerade”は、メッセージの発信源が正しく認識されていないことである。例えば、非安全システムの要素からのメッセージが安全要素のメッセージとして不正に確認されることであり、通信の分野ではこのような不正アドレスの事例が多くなっている。

イ　通信の残留欠陥の低減法

上記の通信プロセスの残留欠陥率のような必要とされる機能失敗尺度を確実に実施するために必要となる 技法又は手段には、次のような 2 つのアプローチが可能である。

ⅰ．全体通信チャンネルを IEC 61508(機能安全)、IEC61784-3(フィールドバス)、IEC62280(鉄道分野通信システム)に従い設計・開発し「ホワイトチャンネル」(図 5-19 参照)方式で、妥当性確認する方法。
ⅱ．通信チャンネルの一部が、「ブラックチャンネル」(図 5-20 参照)になっている方式で、IEC61508 に従って設計されていない場合、IEC61784-3(フィールドバス)、IEC62280(鉄道分野通信システム)に従った、通信チャンネルとインタフェースする安全関連システムのサブシステム又は、要素が実装されることである。

これらの要件を組み込む通信データとして、IEC61784-3 に従った、以下の例に示すような方法も広く行われている。

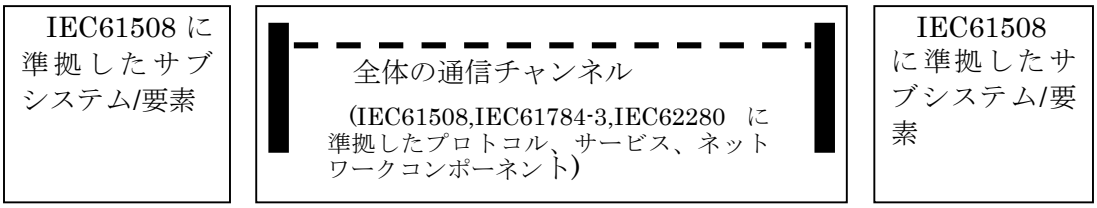


図 5-19　ホワイトチャンネル

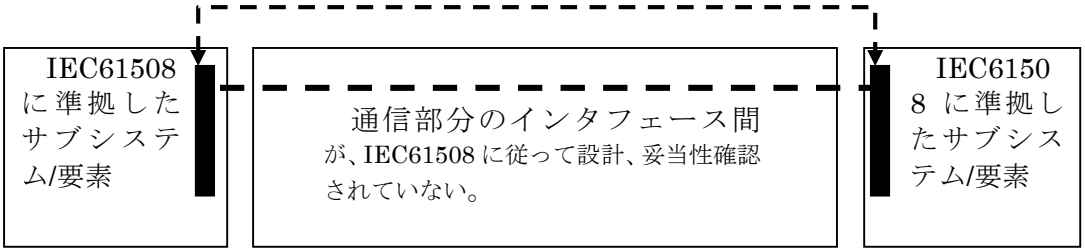


図 5-20　ブラックチャンネル

ホワイトチャンネルは、機能安全通信を規格の要求に従って仕様から設計開発まで行う方式である。新しい通信方式を構築する場合には有効であるが、開発期間が長くなる。

ブラックチャンネルは、既存の通信方式を利用し、通信データに機能安全の役割を持たせたほうほうである。既存の通信方式は、例えば、イーサネットのように通信仕様として公開されている情報に従い、通信データのアプリケーションを設計・開発するので。開発期間が短くなる。

ウ　ブラックチャンネルを使った安全通信の例

ブラックチャンネルは、既存通信方式に機能安全通信を埋め込む方式の 1 つであり、既存通信関連の装置やコンポーネントは、高い信頼性が必要である。

ブラックチャンネルの概略を TCP/IP の例で説明する。TCP/IP はインターネット通信に利用され、最も普及している通信方式である。

（ア）　TCP/IP の階層モデル

通信の階層は、インターネットでは 4 層あり、階層ごとに役割が決まっている。データ通信を行う場合、データを送る場合は、マイコンからアプリケーション層にデータを渡し、下位階層に向かって各階層で手続きが行われ、手続き情報を含めてデータ送信先へデータが渡される。受信側では各階層の上位に向かって通信情報が送られ、送信先の手続きが各層で確認され、アプリケーション層を経て送信先のマイコンへ通信データが届く。

アプリケーション層 : 上位のマイコンプログラムから通信データを受け取り、HTTP プロトコルを埋め込む/トランスポート層からの通信データから HTTP プロトコル外し、をマイコンへ渡す処理の部分。

トランスポート層 : 通信制御プロトコル部。装置 A、装置 B 間の通信の信頼性を制御する。HTTP データのチェックサム計算やシーケンス番号を付ける。装置 B で複数のブラウザが起動している場合、どのブラウザへデータを渡すかも制御する。

インターネット層 : 論理アドレス(IP アドレス)を割り付ける。ノードの識別を行う。

ネットワークインターフェース層 : 通信のためのハードウェアと MAC アドレスの割

り当てでノード間通信規定を制御する。

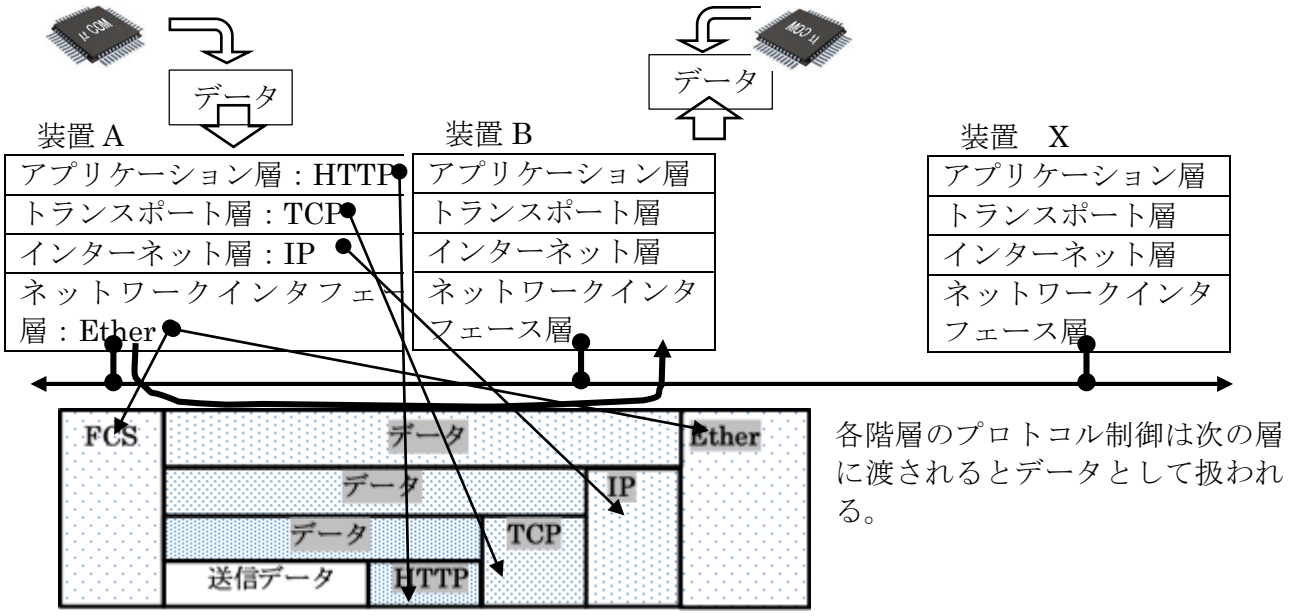


図 5-21　TCP/IP の階層

インターネットの通信方式を TCP/IP で使用するとした時、各階層は、送信の場合は上位のデータをカプセル化し、新たに自階層の処理を付加して、下位に渡していく。そして最終層のネットワークインタフェース層の物理的電気的 Ethernet 仕様のハードウェア素子、配線媒体を通して各層でカプセル化された通信データが送信される。受信側は、各層でカプセル化された通信データのプロトコルを確認し、上位へ送っていく。

ブラックチャンネル方式は、TCP/IP イーサネット仕様であれば、上図のアプリケーション層のデータ（この図では HTTP+送信データ）が安全通信に利用でき、それより階層は TCP/IP イーサネットの仕様に従うことになる。

安全通信では、このアプリケーション層に機能安全を達成する通信仕様を構築し、通信制御、通信の信頼性は既存の通信方式に依存することとなる。

安全通信は、通信障害について方策を講じなければならない。通信障害は、IEC-61784-3、IEC-62280 に記載されているので詳しくはそれらの規格を参照するとよい。それら規格で通信障害として挙げられている項目は、通信エラー、反復、喪失、挿入、誤配列、書換え、遅延、偽装（なりすまし）である。これらについて安全通信仕様の FTA、FMEA を行い、信頼性を確保する。

安全データの通信には、一般的に使用されるデバイスネットやイーサネットが使用されることがある。このような通信は、通信データを保護するため様々な方法が使用される。

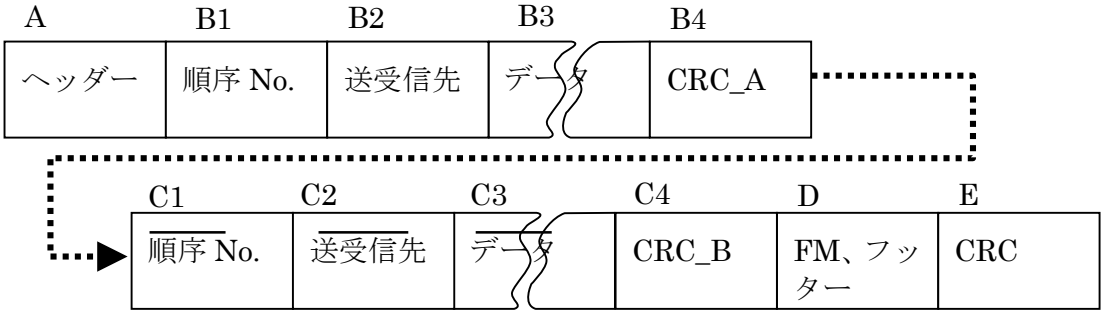


図 5-22　安全通信データの構成

通信データの形式を以下の条件とする。

(1) A と D と E は、通信のファームウェアによって作られる。ブラックチャンネル部に相当する。また、B,C、D がアプリケーション層のデータに相当する。

(2) B4 は、B1 から B3 の CRC。これは、個別の安全関連システムアプリケーションの通信制御ソフトウェアによって作られる。

(3) C1 から C3 は、B1 から B3 の反転データ(1 の補数又は 2 の補数)

(4) C4 は、C1 から C3 の CRC。(2)と同様、個別の安全関連システムアプリケーションの通信制御ソフトウェアによって作られる。

(5) D のフッターには、通信フレームの良否診断情報が含まれる。

(6) E は、通信のファームウェアによって作られる。例えば、B1 から D までの CRC。

以上の条件で、通信欠損のどの項目の判定に主に関係するかを簡略に表にまとめたものが以下である。

1　通信エラー　　D,E で判定

2　反復　B1,C1　順序 No.が更新されることで判定

3　喪失　B1 から B4、C1 から C4 のデータを比較することで判定

4　挿入　B1 から B4、C1 から C4 のデータを比較することで判定

5　誤配列　B1 から B4、C1 から C4 のデータを比較することで判定

6　書換え　B1 から B4、C1 から C4 のデータを比較することで判定

7　遅延　B1,C1 が規定の時間で更新されないことで判定

8　偽装（なりすまし）　B2,C2 の一致と B1 から B4、C1 から C4 のデータを比較することで判定。更に暗号化を加えることもある。

既に市販されている既存の通信方式を利用し他方が良い。既存通信を利用した安全プロトコルは、安全機器の要求仕様に合わせてカスタマイズされるが、その部分は、既存通信から見れば、データにあたる。開発者は開発コストが低減でき、ユーザは既存通信仕様でデータを受信し、送られたデータを解析するだけなので、ユーザにも開発費低減と安全通信の信頼性確保のメリットがある。広く使用されている安全通信には、デバイスネット Safety、イーサネット Safety、イーサ CAT などがある。

5 ソフトウェアの設計

(1) ソフトウェアの要求事項

設備機械、システムにおいて、ソフトウェアは、電気、電子、プログラマブル電子機器、装置で機能安全を実行、達成するため、幅広く利用され、大きな役割を担っている。

機能安全に重要なソフトウェアの開発活動は、ソフトウェア安全ライフサイクル(SSLC)に定義され、いくつかのフェーズ(フェーズ)に分割される。

ア　ソフトウェア安全ライフサイクル（SSLC）

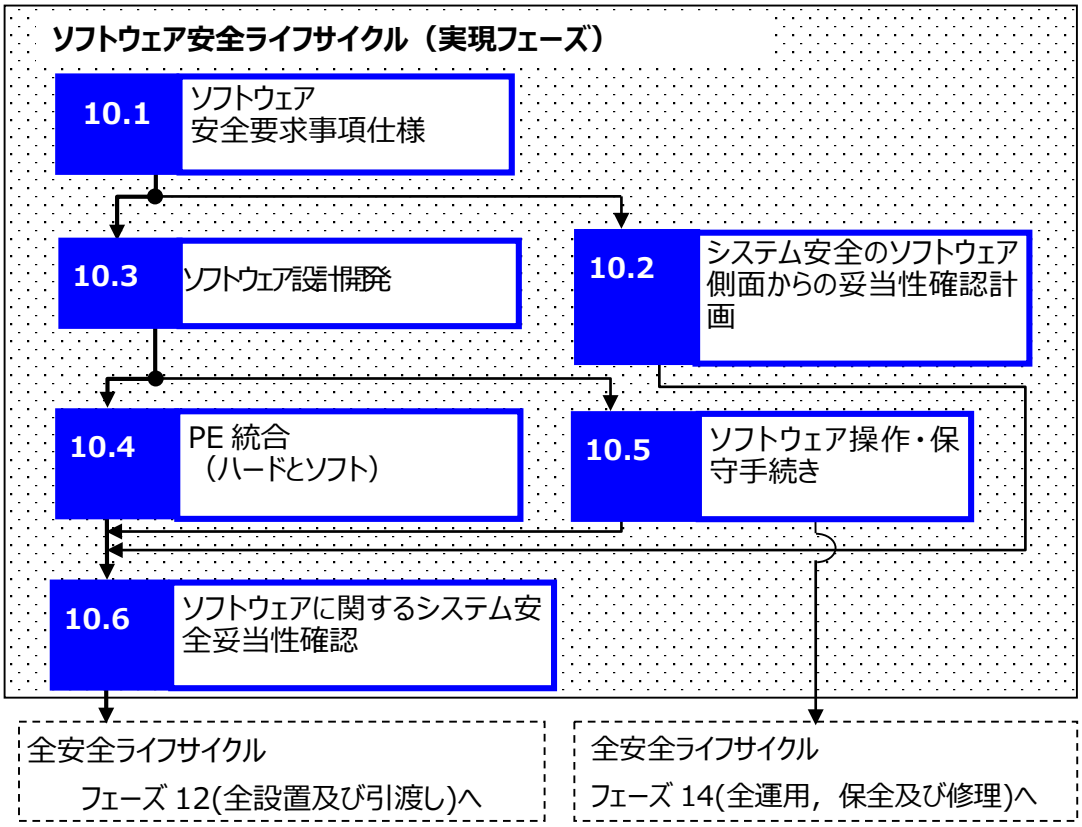


図 5-23　ソフトウェア安全ライフサイクル（実現フェーズ）

ソフトウェア安全ライフサイクル(SSLC)は、ソフトウェアの構想から廃棄までのプロセスをフェーズで定義したものである（図 5-21）。ソフトウェアはハードウェアに組み込まれ、要求仕様に基づいてプログラムが実行される。ソフトウェアの実行、運用フェーズは、ハードウェアに組み込まれているので、安全関連システムの全安全ライフサイクルのフェーズの中に含めて扱われる。

全安全ライフサイクルのフェーズ 9 で作成した電子等制御システム設計要求事項仕様書から全安全ライフサイクルのフェーズ 10 の実現フェーズの中にソフトウェアライフサイクルがある。

図 5-21 は、電子等制御安全システムハードウェアの実現フェーズ 10 の概略を示したものであり、各フェーズは次の項目となる。

フェーズ 10.1　電子等制御安全システムのアーキテクチャ仕様の内、ソフトウェアの要求事項を入力し、ソフトウェア安全要求仕様を作成する。

フェーズ 10.2　安全要求仕様の要求事項を満足していることを試験するための計画を作成する。

フェーズ 10.3　ソフトウェア安全要求仕様に基づき、ソフトウェアの設計・開発を行う。

フェーズ 10.4　設計・開発したソフトウェアを実際のハードウェアに入れて統合試験を行う。

フェーズ 10.6　ソフトウェア安全要求仕様の条件及び 10.2 で作成した計画に基づき、電子等制御安全システムハードウェアによりソフトウェアの妥当性確認試験を行う。

ソフトウェアの妥当性確認は、試験によって行われ、ソフトウェア安全要求事項仕様に基づいて試験項目が計画され、その計画に従って実施される。

この妥当性確認では、予見できる故障(設置環境、誤操作、入出力信号タイミングずれ等)についても試験を行う。このことは、正しい条件で正しく動き、不正な条件では予め決められた処理を行い、暴走やダンマリ、意図しない動作を行わないことを確認することである。

(2) ソフトウェア安全ライフサイクル

ア　ソフトウェアの開発、設計のV字型モデル

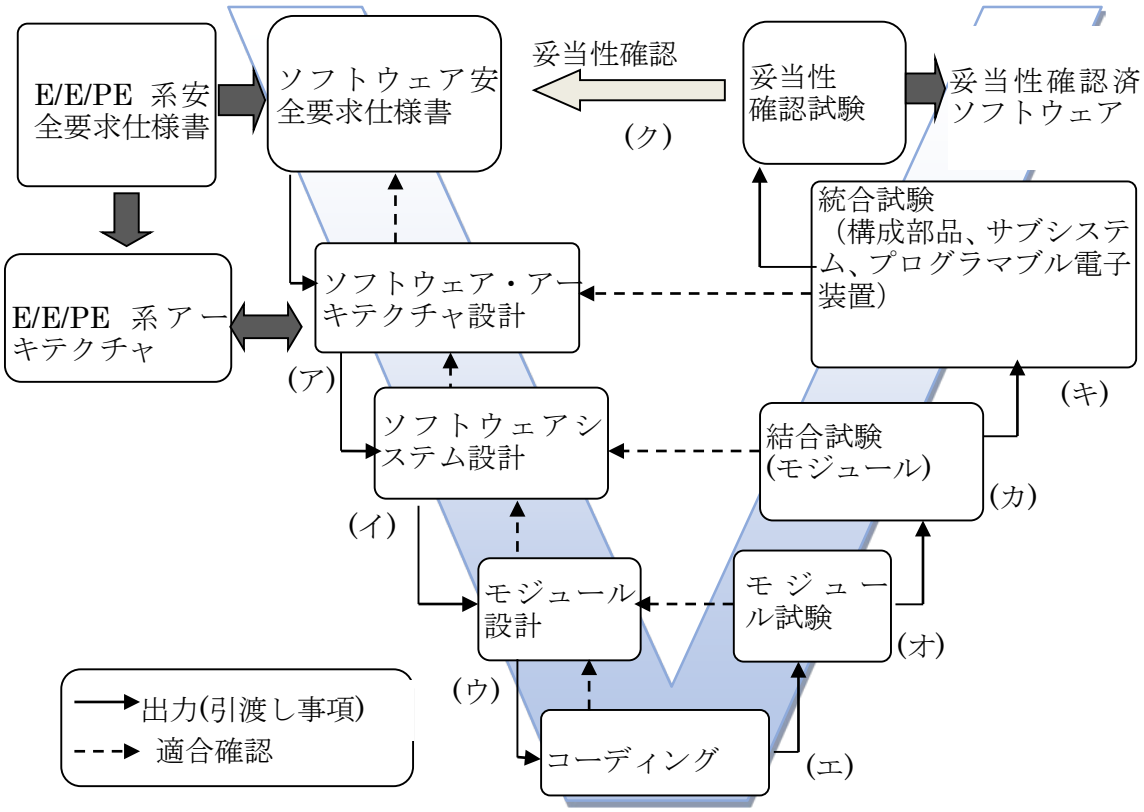


図 5-24　V字型モデル

ソフトウェアの安全ライフサイクルの実施には、図 5-24 で示すV字型モデルが推奨される。このV字型モデルは、左上から中央下、そこから右上に流れるVの字型のフローチャートとなっている。

（ア）　ソフトウェア・アーキテクチャ設計

電子等制御システム安全要求仕様書から作成したソフトウェア安全要求仕様書に従って安全機能を抽出し、ソフトウェアの構造を決める。このフェーズでは他にオフラインサポートツールの選定、プログラミング言語の選定、妥当性確認試験を計画する。

（イ）　ソフトウェアシステム設計

ソフトウェア･アーキテクチャ仕様からソフトウェアの機能動作、操作、入出力信号、

変数等の仕様を決定し、ソフトウェアシステム設計仕様を作成する。同時に結合試験（モジュール）の計画を行う。

（ウ） モジュール設計

ソフトウェアシステム設計仕様の機能別の設計情報より更に細分化し、単一機能まで分解し、できれば 1 入力 1 出力単位までの単一機能までモジュール化し、モジュール設計仕様を作成する。同時にモジュール試験仕様の計画をする。

（エ） コーディング

モジュール設計仕様に基づき、コーディング規約に従って、コーディングをする。また、モジュール試験仕様を作成する。

（オ） モジュール試験

モジュール設計仕様、モジュール試験仕様に従い、モジュール単位で試験を行い、各モジュールのコーディングが正しいことを確認する。

（カ） 結合試験(モジュール)

ソフトウェアシステム設計仕様に従って機能単位にモジュールを組み合わせて当初の機能が仕様通りに動作することを確認する。

（キ） 統合試験

電子等制御システムハードウェアにソフトウェアを実装し、機能試験を行う。ソフトウェア・アーキテクチャの要求事項仕様書の機能が実行できるかの確認になる。想定した不具合は不具合として検出できることも確認する。

（ク） 妥当性確認試験及び適合確認

電子等制御システムの安全要求事項仕様が達成できているか妥当性確認試験で確認する。実際の使用環境、又はそれに準じた条件で試験を行う。

・実線：出力(引渡し情報)

各フェーズからの出力で、次フェーズに情報を引き渡す情報である。

・破線：適合確認(検証)

前のフェーズからの出力情報とそれを受けた次フェーズの出力情報が前フェーズからの入力情報に 100%従っているかを試験によって確認することである。フェーズ途中での仕様の欠落、不要な仕様の追加のないことをこの適合確認で確認する。フェーズを移るたびに行う。

ソフトウェア工程で推奨されるＶ字型モデルはソフトウェアの品質管理に着目している。工程管理、日程管理には不向きのため、このような場合はウォーターホール型やそれぞれの経験に基づいた管理方式が使用される。

(3) ソフトウェアの安全度水準

リスク低減に必要な安全機能に対し、要求される安全度は、ハードウェア・アーキテクチャの制約により決定できる。ソフトウェアは、ハードウェアに要求された安全度水準が最低限の達成目標となる。

ソフトウェアに割り付けられた全ての安全機能の仕様達成のための制約事項を明確にし、要求されたハードウェア安全度達成のために必要なソフトウェアで行う要求事項の内容(下記等)を明確にする。

（ア） 既存ソフトウェアの流用

既存ソフトウェアの信頼性が目的とする安全要求事項に合致していることを検討し、その仕様と流用可否について記述する。原則、使用しようとするソフトウェア内に使用しない機能があってはならない。

（イ） ソフトウェアの非安全部の扱い

同一の安全システムにおいてソフトウェアが安全機能と非安全機能の両方を実装する場合、非安全機能の故障が安全機能に悪影響を与えることがないように相互間の独立性を持った設計としなければならない。もし、それができなければ、安全機能と非安全機能の両方を実装しているソフトウェアは、全て安全関連のソフトウェアとして扱う。

（ウ） ソフトウェア安全要求事項に対する技法又は手段

ソフトウェアの安全要求仕様書に対して技法および手段には表 5-17 のものが推奨される。

表 5-17 ソフトウェア安全要求事項

No.	技法又は手段	SIL 1	SIL 2	SIL 3
1a	半形式的方法	R	R	HR
1b	形式的方法	--	R	R
2	システム安全要求事項とソフトウェア安全要求事項間の前方トレーサビリティ	R	R	HR
3	安全要求事項と認知されている安全性ニーズ間の後方トレーサビリティ	R	R	HR
4	上記の適切な技法又は手段を支援するためのコンピュータ支援特殊ツール	R	R	HR

（エ） 技法又は手段の概説

a. 半(準)形式的方法

半形式的方法には、次のような技法および手段が推奨されている。

ⅰ. 論理/ファンクションブロック図
ⅱ. シーケンス線図
ⅲ. データフロー図
ⅳ. 有限状態機械/状態遷移図、又は時間ペトリネット
ⅴ. 全体(エンティティ)関係属性データモデル
ⅵ. メッセージ順序表
ⅶ. 意思決定表/真理値表
ⅷ. UML

推奨される上記の技法又は手段の多くは図表記法である。

b. 半(準)形式的方法

状態遷移図 (state transition diagrams)

ⅰ. 状態遷移図は、有限個の状態を遷移と動作の組み合わせで抽象化した「動作モデル」である（図 5-23)。

(4) ソフトウェアのアーキテクチャ

ア　ソフトウェア・アーキテクチャ設計の技法又は手段

ソフトウェア･アーキテクチャ設計のフェーズで検討しなければならない技法又は手段は、要求されるソフトウェア安全度により異なる。各安全度で同じ技法又は手段が要求される場合は安全度ごとに情報の深度が異なる。

以下の技法又は手段はソフトウェア・アーキテクチャの基本形である。

（ア）　実時間処理の安全と性能

タイム・トリガー・アーキテクチャ（TTA）のシステムは、タイマーによって起動がかかる構造である。この技法又は手段では、システム動作が、同期化され、同じ時間基準でプログラムが実行される。プログラムの各機能は、時間管理され、処理時間の固定枠が割り当てられる。それ故、各機能間は、定義されたタイムスケジュールに従って、情報交換を行う。

ｉ．最大周期時間が保証された周期的動作

ソフトウェア安全機能のプログラム順序が予め決められ、その処理時間の合計の最大処理時間が定義された動作のこと。

一般的には、処理時間が伸びるのは、周期内で例外的処理（エラー処理やリカバリー処理）を行う時など特殊な時に限られ、通常の動作は、数 ms 単位で信号読み取り、論理処理、出力処理、その他表示、オペレータ用付帯処理などが周期的に行われる（図 5-26）。最大処理時間は、正常な状態と判定される最大処理時間を定義する。最大周期時間は、プログラムの構成、対応安全関連システムに依存するが、原則的には周期動作で許された周期時間を超えないこととする。

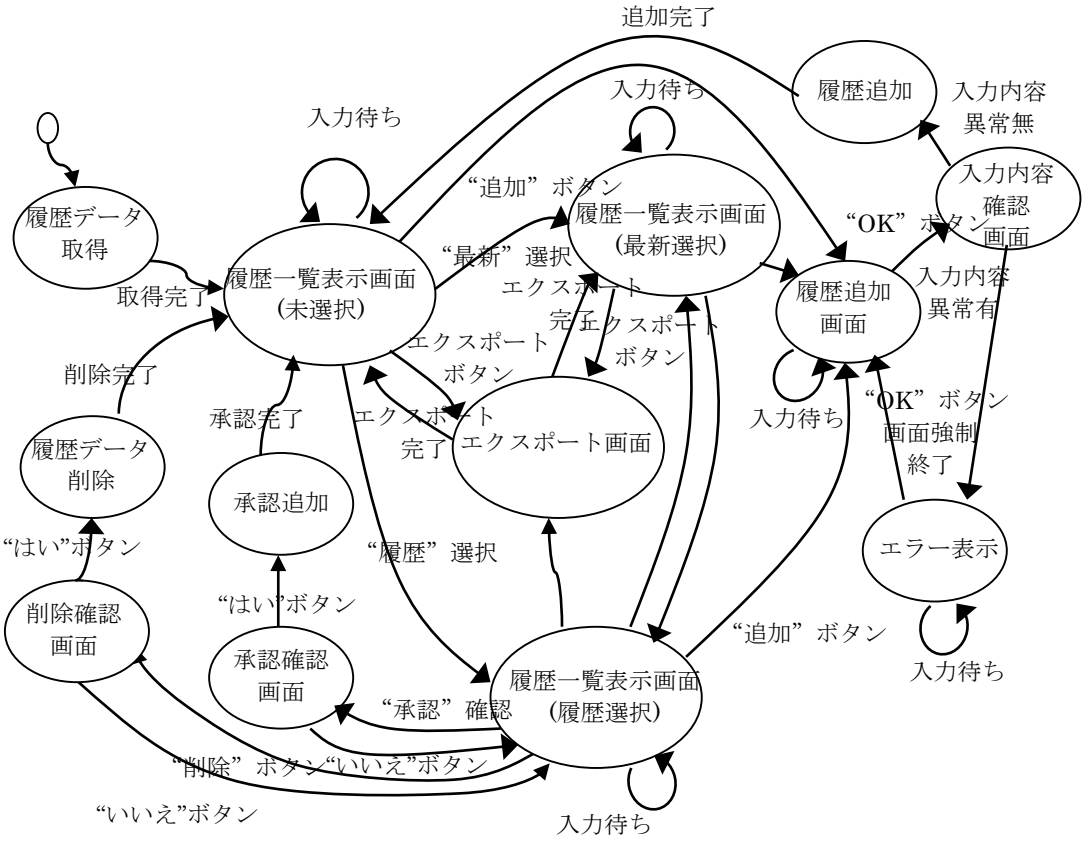
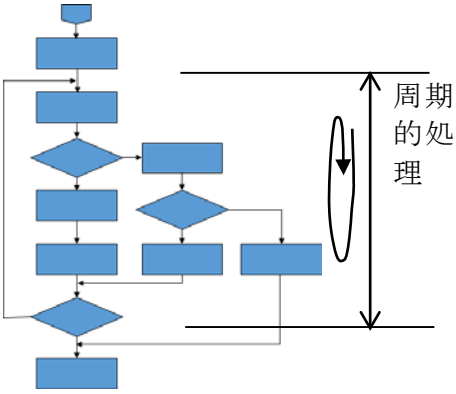


図 5-25　状態遷移図の例

ⅱ．低い安全度水準の場合

・処理タイミングを仕様書に記述する。
・処理タイミングと潜在的障害の関係を検討する。(自プログラム、他プログラムとの処理タイミングが遅れた場合、短くなった場合に起こる障害など)。
・タイミングとプログラム実行機能の関係を明らかにする。



周期的処理のプログラム処理の最大時間(又は、最悪時間)を保障値とする

図 5-26　周期的動作

ⅲ．高い安全度水準の場合

低い安全度水準の要求に以下を加える。

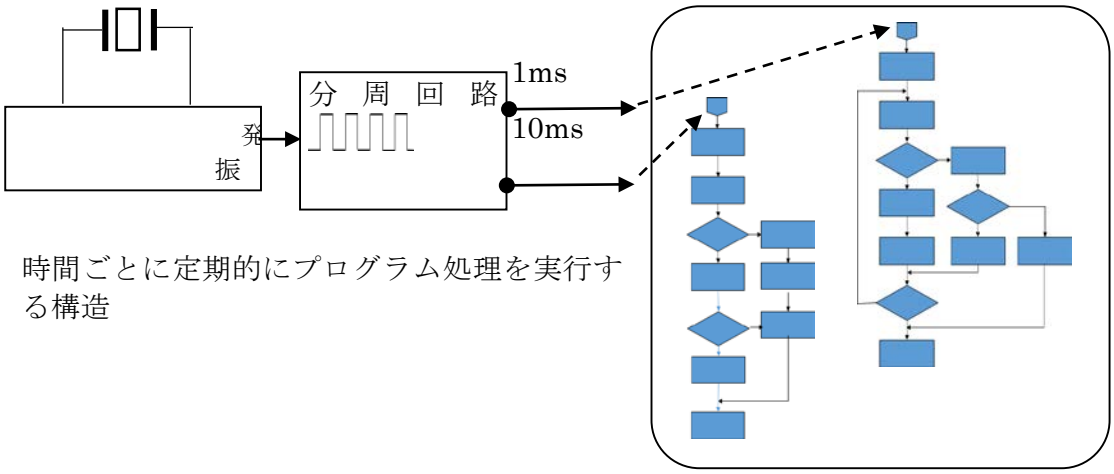
・時間タイミングを厳密に記述し、最大時間を明らかにする。(メッセージ・シーケンス・チャートを作成し、プログラム間のメッセージ交換、時間タイミング、メッセージ交換失敗時のリカバリー処理、待ち時間などを明確にする。)
・潜在的障害に関してタイミングとの関連を厳密に記述し、最大時間を明らかにする。(プログラム進行シーケンス・チャートなど作成し、プログラム順序、進行の遅延、短縮を明確にし、境界値近傍、０処理の考察も行う。)
・タイミングとプログラム処理の関係を厳密に明示し、最大処理時間を明示する。
・タイミングの適合確認方法、試験方法を明らかにする。(タイミング測定が難しい場合は、自プログラムでメモリの一部に処理時間のラップ、処理経過順序の記録を残す方法がある。)

（イ）　タイム・トリガー・アーキテクチャ

ハードウェアで時計を持ち、時間ごとに処理プログラムを決め、時間がくると処理を行うソフトウェア・アーキテクチャである（図 5-27)。

例えば、10ms ごとに入力処理、論理処理、出力処理を行い、100ms ごとに表示関係のキー入力処理、論理処理、表示出力処理を行う、また、1s ごとにシステム稼働率の計算を行うなどの技法である。

時計は、マイコンのクロックを元にしたカウンター値でもマイコン外のクロックでもよい。



時間ごとに定期的にプログラム処理を実行する構造

図 5-27　タイム・トリガー・アーキテクチャ

ⅰ．低い安全度水準の場合
・タイムトリガータイミングに関して、仕様書に記述する。
・タイムトリガータイミングと潜在的障害の関係を検討する。
・タイムトリガータイミングとプログラム実行機能の関係を明らかにする。
ⅱ．高い安全度水準の場合
低い安全度水準の要求に以下を加える。
・タイム・トリガーの時間割り当てを厳密に記述し、タイミング仕様を明らかにする。
・潜在的障害に関してタイムトリガータイミングとの関連を厳密に記述する。
・タイムトリガータイミングとプログラム処理の関係をわかり易く、用語定義、構文の複雑さをなくし、記述する。
・動作タイミングの適合確認方法、試験方法を仕様の中に盛り込み、適合確認に時間がかからないようにする。
・要求される HFT を満足することを明示する。
・タイム・トリガーは一般的に割り込みを使用する。この割り込みが、外部からの共通原因故障要因から影響を受けないように防御されていることを明示する。

（ウ）　イベント・ドリブン、最大応答時間保証付き

イベント・ドリブン・システムでは、システムの動作は、ある事象により予測不可能な時点で、動作にトリガーがかけられる（図 5-28)。

ある事象が起きた時に処理が開始されるアーキテクチャで、通信処理、操作者とのインタフェース処理などに良く使用される。安全機能に対し、この方式を使用する場合は、トリガータイミング、最悪の最大処理時間を明確にする必要がある。

イベント(事象)が起きた時から出力が完了するまでの時間を最大応答時間とする。

トリガー信号のスキャン待ち、割り込み待ち、通信時間、リトライ時間、ネットワーク経由伝達時間等の最大値を合計したものになる。

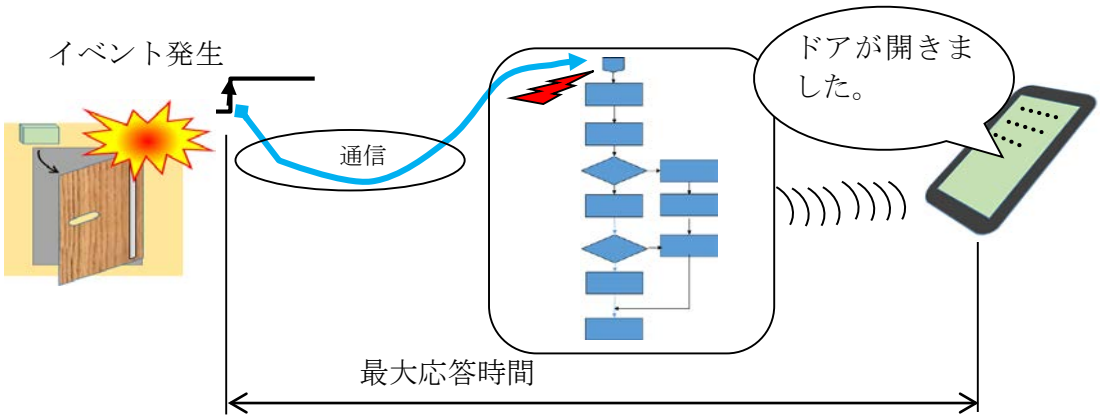


図 5-28 イベント・ドリブンの例

イ　ソフトウェアシステム設計

ソフトウェア・アーキテクチャの仕様により、ソフトウェアの構造が決定した。このフェーズでは、構造体に含まれるソフトウェアの機能分析を行い、階層化構造を作成する。この階層化構造に従って、モジュール化設計を行う。モジュール化されたソフトウェアは、構造化される。構造化された各モジュールは、モジュールごとの仕様、モジュール間インタフェース仕様を決める。

モジュール化は、ソフトウェアの決定論的原因故障の要因を排除する技法又は手段である。

（ア）　構造化手法による設計

ソフトウェアをモジュール化するに際し、構造化手法を用いる。

ⅰ．安全関連システムの安全関連の要求仕様書、ソフトウェアのアーキテクチャ設計仕様書に基づきシステムを構造化しモジュール化を図る。
ⅱ．ソフトウェアを安全関連部と非安全部とに分離する。
ⅲ．データの誤入力を予防する範囲チェックやデータの適合性チェックの仕様を含める。
ⅳ．フォールトトレランス/フォールト検出構造であること
ⅴ．共通原因故障の影響が無いこと
ⅵ．　適合確認が可能で試験が可能な設計であること
ⅶ．システム安全のソフトウェア面に対する妥当性確認計画の要求事項を仕様に含める。
ⅷ．すでに安全性が適合確認されたソフトウェアモジュールを使用する。
ⅸ．将来のソフトウェア変更が容易になる構造とする。
ⅹ．ソフトウェアの結合試験の要求事項を仕様に含める。
ソフトウェアシステム統合試験は、ソフトウェア安全要求仕様の安全度水準を満足していることを確認するために規定されていなければならない。

（イ）　モジュール化への対処の技法又は手段

モジュール化への対処は、ソフトウェアに要求される安全度水準により、下記のような推奨される技法又は手段がある（表 5-18）。これらの技法や手段は、ソフトウェアモジュールに潜在的は故障が入りこまないようにする管理的技法又は手段である。

ⅰ．プログラムは、簡潔で分かり易く記述する
ⅱ．モジュール単位の機能がわかり易く、動作が予測できるようにする。

iii．モジュールの機能の適合確認、試験が可能な構成とする。このことは重要である。

No.	技法又は手段	SIL 1	SIL 2	SIL 3
1	ソフトウェアモジュール規模制限	HR	HR	HR
2	ソフトウェアの複雑さの抑制	R	R	HR
3	情報の隠蔽/カプセル化	R	HR	HR
4	パラメータ数の制限/固定数のサブプログラム･パラメータ	R	R	R
5	サブルーチン及び、関数における一入力点/一出力点	HR	HR	HR
6	完全に定義されたインタフェース	HR	HR	HR

(5) サポートツールに対する要求事項

サポートツールとは、ソフトウェア安全ライフサイクル中に使用するコンピュータ支援ツールことで、オフラインサポートツールと呼ぶ。

これらのツールは一定の信頼性が必要である。その信頼性がソフトウェアの安全性に与える影響度合いにより、以下の 3 つのクラスに分類し、管理を行う。

クラス	サポートツールの要件（図 5-27 参照）
T1	直接的、間接的にも安全関連システムのコード、データを出力しないツール。 例：自動的にコードを発生しないテキストエディターや要求事項や設計を支援するツール、構成管理ツール
T2	設計や実行コードの試験、適合確認を支援するツール。ツールに不具合が潜在し、表面で出てこなくても、不具合を知らずに使用しても安全機能を実行するソフトウェアに直接的に不具合を作り込むことのないツール。 例：適合確認試験時のモジュール組み合わせ発生、自己診断占有率測定ツール、静的解析ツール
T3	安全関連システムの実行コードを直接的、間接的に出力するツール。 例：コンパイラ最適化(ソースコードプログラムより不要とされた生成コードを除去したオブジェクトコードを発生する)、実行コード内のランタイムパッケージを一体化したコンパイラ

ア　オフラインサポートツールの条件

オフラインサポートツールは、ソフトウェア開発活動の各工程を一気通貫して使用することが望ましい。そうすることで、工程間の人の手によるデータ変換などによるヒューマンエラーを無くすことが出来る。これは、決定論的故障の低減に良い影響を与える。

(6) プログラミング言語

ソフトウェア設計においてプログラミング言語は重要な位置にある。プログラミング言語は、開発目標に合わせて選定すべきである。

機械設備等の安全関連システムで安全機能を実行する部分は、一般的に電子装置や機器であり、そこにはマイコンやアプリケーション・ソフトウェアに対応した安全 PLC が使用される。

安全機能を実装するソフトウェアのプログラミングは決定論的原因故障の要因を潜

在させてはならないので、プログラミング言語やその周辺関連ツールは高い信頼性が要求されるとともに汎用的仕様から適用を制限にした仕様も要求される。
プログラミング言語とその関連のコンパレータ、リンカ他の選定への要求事項は以下である。

（ア） 適切なプログラミング言語
適切なプログラミング言語とは、安全機能を実装する対象のもつ要求事項(仕様)を解決することに適したプログラム言語のことである。プログラミング言語は以下の項目を考慮して総合的に選定する。
ⅰ．プラットフォーム
ソフトウェアを実行する装置、機器の環境が何であるか、プログラム実行のベースとなる OS があるのか、あるなら OS に適したプログラミング言語はなにか。
ⅱ．実稼働までの時間
実稼働までの時間とは、ソフトウェアを開発し、対象の装置、機器の、システムにソフトウェアをインストールし、目的の安全機能が正しく動作開始するまでの時間である。
実稼働までの時間内で、もっとも開発効率が上がり、デバッグ、修正、ドキュメント作成が容易なプログラミング言語とその関連は何か。
ⅲ．パフォーマンス
プログラム実行ベースのプラットフォームで最高、最適な性能（Ex.実行速度）が出せるプログラミング言語であること。
ⅳ．サポート
プログラム作成中に問題が発生した時、その解決のため、技術的な支援をサポートする体制、組織があること。
サポート体制は、自社内でも、サポートツール供給者でも、コミュニティでもよい。

（イ） 強い型付けのプログラミング言語
強い型付けとは、プログラミング言語が型の規則を強く適用することである。ある 2 つのデータに対し、型の互換性を検出し、互換性がなければエラーとするか、型の強制変換を行う。
弱い型付け（Weak typing）とは、プログラミング言語が型の規則を強要しないことである。
Java や Ruby は、強い型付け言語で、アセンブリ言語や C 言語は、弱い型付けのプログラミング言語と言われる。

（ウ） 言語サブセット
プログラミング機能の一部を取り出して、特定の用途に利用できるように再構築したもの。
プログラミングの汎用性を機能制限し、使用目的に専用化したものと捉えることができる。言語サブセットは、プログラミングにおける決定論的原因故障の要因の発生確率を減らし、残存障害の検出確率を上げ、バグ発生を無くすために取られる方法である。
弱い型付けのプログラミング言語を使用する場合、バグ発見、エラー解析が難しい場合、静的解析ツールが併用されるべきである。
例えば、静的解析ツールとしては、MISRA C、MISRA C＋＋のコーディング規約に従って検査を行う市販の LDRA や QAC、C/C++テストがある。

（エ） 認証されたツールとトランスレータ
サポートツールの認証は、一般的には独立した部署や機関、国の検査機関で行われる。ソフトウェア安全ライフサイクルの全フェーズ（仕様作成、設計、コーディング、試験および妥当性確認）で使用されるツールや構成管理で使用されるツールは、原則的に認

証(認定)が必要である。
しかし、Ada や Pascal のコンパイラ（トランスレータ）だけが定期的に認証手続きを受けるようになっているが、他のプログラミング言語には、認証されたものがなかった。ただ近年、機能安全関連の開発が多くなり、認証機関が認証したプログラミング言語のコンパイラ（トランスレータ）が市場に出てきた。

（オ） 使用実績による信頼性の確保のツールとトランスレータ

トランスレータは、過去の多くのプロジェクトに使用し不適切な実行の証拠がない場合、統計的に信頼性を評価し、それを使用することができる。もし、トランスレータが小さな欠陥を有していることがわかった場合、安全関連プロジェクトを実施中は、その欠陥に関連する情報を記録し、その欠陥を避けて使用する。

通常、認証済みのツールやトランスレータは限られているので、認証されていないツールやトランスレータを使用せざるを得ない。それ故、(オ)が選択されることが多い。(オ)では、”increased confidence from use”の文言が有り、「使えば使うほど信頼性の高くなった」物が良いとしている。これは、市場で広く使用され、その使用結果がフィードバックされ、ツールやトランスレータの信頼性が一層向上していると見なされるとする立場からである。

認証されたツール、トランスレータを使用しない場合は、上記の点を考慮し、適切なプログラミング言語とその関連ツールを選択する。使用する際、選択したツールやトランスレータの信頼性を裏付ける文書を入手する。例えば、バージョン情報、バグ履歴など。

（カ） プログラミング言語の推奨事項

対象のアプリケーケーションにインストールするプログラミング言語として、いくつかの良く知られたプログラミング言語の推奨がある。

ⅰ．サブセット付き C とコーディング規約、および静的解析ツールの使用

C 言語そのものは弱い型付けの言語であるため、原則使用ができない。しかし、サブセット C であり、コーディング規約、静的解析ツールと併用することで弱い型付けを補完できる。

組み込みシステムによく使用される C 言語は、サブセットであり、コーディング規約に則り、静的解析ツールを併用すれば、使用することができる。静的解析ツールとしては、現在、LDRA、QAC のようなソフトウェア静的解析ツールがあり、日本製の富士通等から出始めている。

ⅱ．サブセット付き C++とコーディング規約、および静的解析ツールの使用

ⅰ．C 言語と同様条件。

ⅲ．アセンブラ

サブセット付きアセンブラとコーディング規約で使用可能。

アセンブラは、機械語に近い言語である。強く推奨はされないが、コーディング規約と対象マイコンに専用に作られたアセンブラを使用することができる。

自己診断プログラムや制御時間や応答時間が厳しい場面などでは、アセンブラを使用しなければならないことがある。

ⅳ．その他の言語

よく使用される C 言語や C++言語以外にも数々の言語が市場に出ている。そのような言語を選択する時は、統計的な使用実績を考慮して選定する。

ⅰ． 一般に広く使用されており、また、

ⅱ．使用経験があり、よくその仕様を熟知しているツールやトランスレータを選択するとよい。

ⅲ．使用する際、選択したツールやトランスレータの信頼性を裏付ける文書を入手する。例えば、バージョン情報、バグ履歴など。

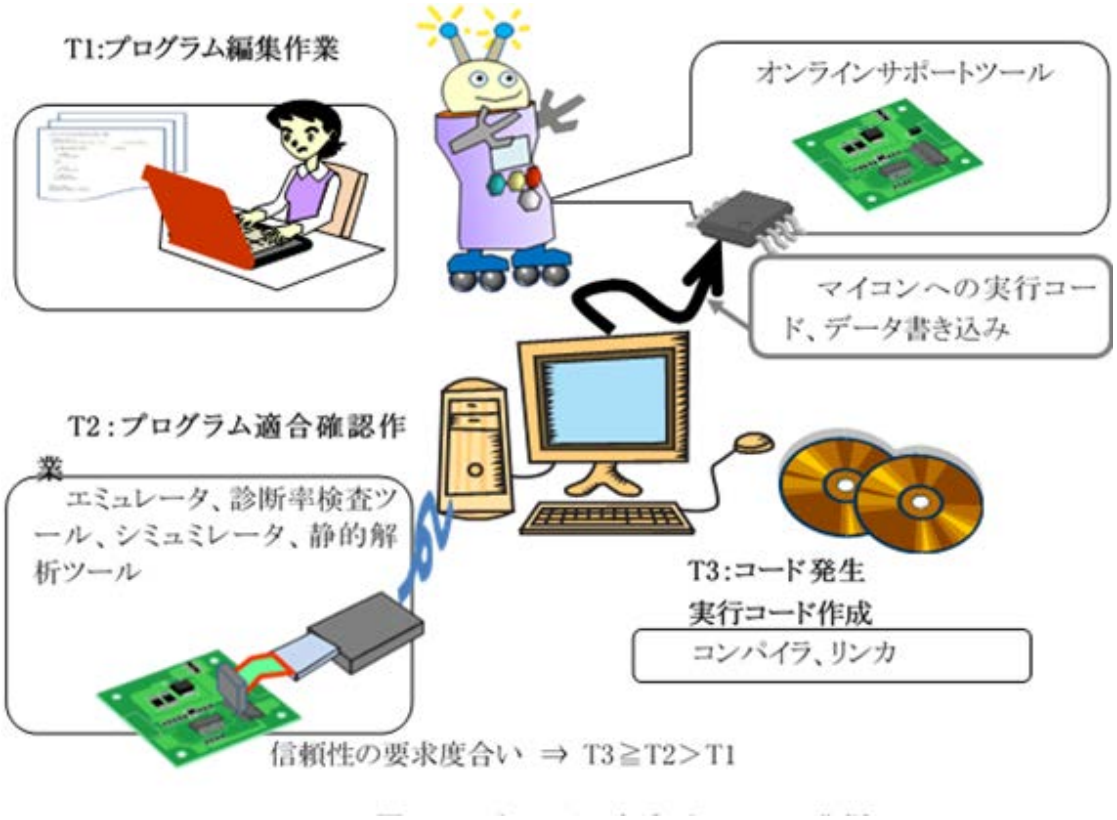


図 5-29　オフラインサポートツールの分類

(7) ソフトウェアモジュール設計

イ　詳細設計開発の要求事項

前工程のソフトウェアシステム設計フェーズにて、ソフトウェアは小さなモジュールにまで分割され、そのモジュールを階層的に結合する構造化設計が行われ、モジュール間のインタフェース仕様ができている。

モジュール設計のフェーズでは、前工程の設計仕様に従って詳細設計を行う。詳細設計では、モジュールの内部構造設計とモジュール間のインタフェースの詳細仕様(入出力変数の型、タイミング等の仕様)を定義し、コーディングのための仕様を確定する。

モジュールの内部構造設計とは、いわゆるフローチャートの作成である。

ソフトウェアの詳細設計は、以下のような方針で行う。

(ア)　詳細設計

ⅰ．前工程からのソフトウェアモジュール仕様、機能を確認する。更にモジュール化が必要なものはここでモジュール分割する。

例えば、コーディング規約の規模制限によって分割が必要になる場合。

ⅱ．それぞれのソフトウェアモジュールの処理フローチャート設計を行う。

ⅲ．モジュール間のインタフェース仕様の詳細を決める。

・モジュール間のインタフェース仕様
・データの型
・データやり取りの手順
・タイミング
・エラー検知方法
・エラー検知後の処理
・非安全部とは直接インタフェースせず、専用のインタフェースプログラムを介

する。

ウ　モジュールの機能仕様の表現

モジュールの機能仕様を記述する場合、構造化図形方法、半形式的方法、形式的設計方法および精緻化方法の内１つ以上の技法又は手段を選択する。よく使用されるフローチャートは、半形式的方法に分類できる。フローチャートの場合、モジュール内の構造化がわからないので、必要に応じ、モジュール構造を表す構造化図形方法も同時に選定する。

このような図式は、矛盾なく記述する。

(8) コーディング

ア　ソースコード実装の要求事項

コーディングによって得られるソースコードは、安全度水準に対応して、以下の要求事項に従って作成される。

コンピュータ支援設計ツール、設計およびコーディング規約は、ソースコード及びコーディング品質を出来るだけ統一するため使用される。

(ア)　コードの信頼性確認

ⅰ．コーディングされたソースコードは、モジュールごとに設計審査(DR)される必要がある。
ⅱ．ソースコードの DR は、適合確認の１つである。
ⅲ．ソースコードが自動化ツールで生成される場合、サポートツールの信頼性評価に決定論的原因故障の要因を含まないことが必要である。
ⅳ．ソースコードが既存ソフトウェアから再利用(流用)される場合、使用実績に基づく信頼性評価を行い、安全性に問題が無いことを証明する必要がある。
ⅴ．設計審査(DR)の審議では以下の内容を少なくとも含み、その確認を文書化する。
ⅵ．読みやすく、理解しやすいソースコードであるか。
　・ コメントが書かれ、その内容がプログラムの内容と一致している
　・コーディング長が適切である。
　・再帰がない。
ⅶ．ソフトウェアモジュール設計のオフラインサポートツールの要求事項を満足しているか。
ⅷ．コーディング規約を遵守しているか。
ⅸ．ソフトウェアの詳細設計で規定された要求事項を全て満足しているか。

(イ)　コーディング規約の着眼点

安全関連のソフトウェアプログラミング時のコーディング作業において、コーディング規約は、読みやすくメンテナンスしやすいコードを書くことにあり、ルールに従うことで、エラーの作りこみの可能性を減らし、適合確認が容易になる。実際のコーディングにあたっては, プロジェクトメンバー全員がこのルールに合意していることが必要である。

a. コードの分かりやすさ
　ⅰ．命名規約：変数名、定数名、関数名、クラス名の付け方
　ⅱ．コーディング様式：括弧、スペース、区切り記号の使い方
　ⅲ．禁止事項

b. ソースコードの文書化のルールを明確にすること
　ⅰ．インデントのルール
　ⅱ．カラーコード(小文字/大文字)

iii．コメントの書き方(行数/A4、英語、ローマ字、日本語)
iv．プロパティーの記述順
v．シングルクォート（’ ’）？ダブルクォート？（” ”）
vi．サイズの単位（px? em? %?）
vii．法人組織（例えば、会社、著者、等）
viii．内容説明
ix．入力および出力情報。
x．構成管理(バージョン)履歴

（ウ） 参考となるコーディング規約

コーディング規約には、国際的に、MISRA C; 2004、MISRA C++; 2008 がある。MISRA C は MISRA (Motor Industry Software Reliability Association)が開発した C 言語のためのソフトウェア設計標準規格(コーディング規約)である。ANSI/ISO/IEC 規格の C 言語で記述する組み込みシステムで、安全性と可搬性(移植性)と信頼性を確保することを目的としている。

MISRA C++も上記同様、C++用のソフトウェア設計標準規格(コーディング規約)である。

これらは、下記、ホームページから購入することができる。

http://193.35.217.33/MISRAHome/tabid/55/Default.aspx

イ コーディング

ソフトウェアのコーディングは、以下の項目に注意して実施し、安全機能の動作を確実にする。またコーディング規約では、以下の内容をコーディング時の遵守事項として設計に適した形で表現する。

(9) ソフトウェアシステム結合試験の実施

ソフトウェアシステム結合試験では、いくつかのモジュールを結合し、試験を行う。その結合試験は、少なくともサブシステム(I,L,O)単位に分割し、要素及びサブシステムが相互に正しく動作し、サブシステムを結合したシステムでも正しく動作することを確認する。

ソフトウェアシステム結合試験は、サブシステム単位の機能動作確認後、サブシステムを結合したシステム試験を行う（表 5-19～22）。

機能分割したソフトウェアからサブシステム結合試験までの試験において、全入力の組み合わせ、全出力の組み合わせ試験を行う必要はない。試験は、同値クラスの機能集合に分け、構造化に基づいた試験をおこなう。そして、境界値解析や制御フロー解析により、試験の組み合わせの無駄を省き、受容可能な数まで減らすことができる。

決定論的安全度水準は、通常定量化できない。しかし、場合によっては信頼性成長のような統計的な手法による定量化が有効なことがある。決定論的安全度水準を定量化する手法は正当化できれば受容可能である。

ソフトウェアモジュール試験の結果は文書化する必要がある。

試験に通らない場合の是正処置の手順は、予め規定しなければならない。

ア ソフトウェア結合試験の技法又は手段

表 5-19 ソフトウェアモジュール試験及び統合

No.	技術/方法	SIL 1	SIL 2	SIL 3
1	確率的試験	---	R	R
2	動的解析及び試験	R	HR	HR
3	データ記録及び解析	HR	HR	HR
4	機能的及びブラックボックス試験	HR	HR	HR

5	性能試験	R	R	HR
6	モデルベース試験	R	R	HR
7	インタフェース試験	R	R	HR
8	試験管理および自動化ツール	R	HR	HR
9	ソフトウェア設計仕様書とモジュール及び統合試験仕様書間の前方トレーサビリティ	R	R	HR
10	形式的適合確認	---	---	R

（ア） 動的解析および試験

安全関連系の動的解析は、完成段階に近い状態で、そのプロトタイプ(試作品)に、目的とする動作環境の代表的な入力データを入力することで実行される。安全関連系において、その入力値を与えた時の動作が要求された動作に適合すれば、動的解析は、十分満足されたことになる。

動的解析によって、検出された安全関連系の故障は、全て訂正され、変更され、新しい動作を行う変更版は、再解析されねばならない。

（イ） データ記録及び解析

この方法は、ソフトウェアプロジェクトに関係する全ての情報、データ、決定事項および決定に至った理由の文書化、安全に関する適合確認、妥当性確認、評価及びそれらの文書を維持、変更、管理を容易にするための方法である。

プロジェクト実施中に作成される詳細な文書は、維持管理しなければならない。これら文書は次のような内容を含むべきである。

・各ソフトウェアモジュールで実行される試験
・決定事項とその理由
・発生した問題とその解決方法

ここで作成した文書は、開発プロジェクト中に決定されたある種の結論の理由が、保守技術者に必ずしもわからないことがあるので、データ記録は、サーバー等による維持管理が非常に重要である。

（ウ） 機能的およびブラックボックス試験

機能試験

機能試験は、作成した仕様書及び設計フェーズでの障害を明らかにすることで、ソフトウェア及びハードウェアの実装及び統合中の故障を回避することが目的である。

機能試験は、システムに規定した仕様が、達成されているかどうか確認するために行う。システムの機能試験では、通常、期待した動作仕様を適切に満足するための入力データ(値)が与えられる。入力データを与えた結果として、出力データが観測され、予め仕様書で規定した出力データと比較される。

多重チャンネル・アーキテクチャ用に設計された電子部品の機能試験を行う時、チャンネル毎に異なったメーカの部品を使用して製造したものを、試験に使用することが望ましい。これは、潜在的な共通モード故障を明らかにするためである。

ブラックボックス試験

この試験は、システムやプログラムの機能を、構築した評価基準に従い仕様書から系統的に導出した、仕様に従った試験データを用いて仕様で規定した環境で実行するものである。

これによりシステムの動作が明らかになり、仕様書との比較が可能になる。この試験を行うためのシステム内部構造の知見は不要である。

この試験は、非試験装置が仕様書で要求される機能をすべて正確に実行するかどうかを判定するものである。

試験データの例として、以下の項目がある。

・許容範囲のデータ
・非許容範囲のデータ
・レンジ限界のデータ
・極端な値
・上記の組み合わせ
他の評価基準も、種々の試験実施活動（モジュール試験、統合試験、システム試験）において有効である。

（エ） 性能試験
表 5-22 参照のこと

（オ） モデルベース試験
モデルベース試験（MBT）は、ブラックボックス方法である。モデルベース試験は、システム要求事項や特定機能のモデルを使い、効率的な試験ケース/手順を自動的に生成する。
・モデルの作成（システム要求事項から）
・期待入力の生成
・期待出力の生成
・試験の実行
・実際の出力と期待出力の比較
・さらなる活動（モデルを変更、更なる試験ケースの生成、ソフトウェアの信頼性/品質の評価）の決定

（カ） インタフェース試験
いくつかのレベルに詳細に掘り下げた、完全性の高い試験が可能な方法である。最も重要なレベルの試験は以下に対するものである。
・極端な値でのインタフェース変数のすべて
・他のインタフェース変数が通常値であるときに、個別に極端な値になるインタフェース変数のすべて
・他のインタフェース変数が通常値であるときに、各インタフェース変数の領域値のすべて。
・組み合わせの全変数の全値（小さなインタフェースに対してのみ可能）
・各サブルーチンの各呼び出しに関連した特定な試験条件
インタフェースが、誤ったパラメータ値を検出するための比較機能によって障害を防げない時、上記の試験が特に重要である。
これらはまた、既存サブプログラムを使った新しい構成が作られた時の試験としても重要である。

（キ） 試験管理および自動化ツール
試験管理および自動化ツールは、IEC61508-7 の「ANNEX C, C.4.7 Test management and automation tools」を参照下さい。
適切な支援ツールを使うことで、システム開発におけるより労働集約的で誤りを発生しやすい作業を機械化し、試験管理において、系統的アプローチができるようになる。これらのツールのサポートが得られることで、通常試験や逆戻りの試験の両方に、より完全なアプローチが実施できる。

（ク） ソフトウェア設計仕様書とモジュールおよび統合試験仕様書間の前方トレーサビリティ
トレーサビリティは、IEC61508-7 の「ANNEX C, C.2.11 Traceability」を参照下さい。
第 3.1.2 節「ソフトウェア安全要求仕様書作成時の技術/方法」の No.2 「トレーサビリティ」参照のこと。

（ケ）　形式的適合確認

形式的適合確認は、IEC61508-7 の「ANNEX C, C.5.12 Formal proof (verification)」を参照下さい。

理論的かつ数学的なモデルやルールによって、プログラムの抽象モデルに関してプログラムの正しさを証明することである。

イ　「動的解析及び試験」の技法及び方法

表 5-20　動的解析及び試験

No.	技術/方法(注1)	SIL 1	SIL 2	SIL 3
1	境界値解析から試験ケースの実行	R	HR	HR
2	誤り推測から試験ケースの実行	R	R	R
3	誤りの埋込みから試験ケースの実行	---	R	R
4	モデルベースの試験ケースの生成から試験ケースの実行	R	R	HR
5	性能モデリング	R	R	R
6	同値クラス及び入力分割試験	R	R	R
7a	構造的テスト・カバレッジ(入力点)100%(注2)	HR	HR	HR
7b	構造的テスト・カバレッジ(命令文)100%(注2)	R	HR	HR
7c	構造的テスト・カバレッジ(分岐)100%(注2)	R	R	HR
7d	構造的テスト・カバレッジ(条件、MC/DC)100%(注2)	R	R	R

（ア）　境界値解析から試験ケースの実行

この方法は、パラメータの限界や境界値付近で発生するソフトウェアエラーを検出することが目的の方法である。

プログラムの入力範囲値は、同じような条件、仕様の関係(DC24V 信号、BCD 信号など)によって、いくつかの入力信号グループにクラス分けされる。

この試験は、このクラス分けした信号グループの境界値や極端な値を扱って行われる。仕様書の入力値範囲にある境界値がプログラム中で扱われているものと一致することを、この境界値試験で検査する。

その中で、特に間違いを起こしやすい以下のゼロ値使用は、直接トランスレーション(変換)でも間接トランスレーションにおいてでも、時として間違いをし易いので、特別な注意が必要である。

・除数のゼロ(ゼロ割り)
・ブランクの ASCII 文字
・空のスタックやリスト要素
・満杯の配列
・表のゼロ入力

一般的に、入力境界値は、出力値範囲の境界に直接対応していることが多い。試験ケースは、出力値が限界値になるように入力値を決めるべきである。また、出力値が仕様の境界値を超えるような試験ケースを規定できるかどうかも検討しなければならない。

例えば、もし出力値が、印刷された表のようなデータの並びである場合、その出力値の最初と最後の要素や、又は 0 個、1 個、2 個の要素しか含まない表のようなデータの並

びには、特に注意が必要である。

（イ） 誤り推測から試験ケースの実行
誤り推測から試験ケースの実行は、IEC61508-7 の「ANNEX C, C.5.5 Error guessing」を参照下さい。
今までの試験の経験や試験時の直感による試験ケースを実施すること。試験中のシステムの知識や特に関心を引く部分と、経験則や直感をうまく組み合わせると、決められた範囲に無い試験ケースを設計済の試験ケースの中に加えることができる。さらに、システムが十分に強健かどうかの検討も必要かもしれない。例えば、フロントパネルのボタンを早押ししたり、過度に頻繁に押したり、2 個のボタンを同時に押したらどうなるのか、など。

（ウ） 誤りの埋込みから試験ケースの実行
誤りの埋込みから試験ケースの実行は、IEC61508-7 の「ANNEX C, C.5.6 Error seeding」を参照下さい。
試験ケース一式が適切かどうかを確認することを目的とする。
既知の種類の誤りをプログラムに挿入し（埋め込み）、そのプログラムを試験条件下の試験ケースで実行する。もし、埋め込んだ誤りの一部だけしか見つからなければ、試験ケースの一式は適切ではないことがわかる。

（エ） モデルベースの試験ケースの生成から試験ケースの実行
前節のア ソフトウェア結合試験の技法又は手段ソフトウェア設計開発の(オ)「モデルベース試験」を参照のこと。
・モデルベース試験では、システム安全要求事項とソフトウェア設計仕様書の関連を確実にすることが必要である。
・モデルベース試験では、試験結果と期待した結果との評価を行い、さらに規定された要求事項の結果の評価を行う。
・モデルベース試験は、自動化され、試験の構成を正確に定義する。この試験では、ソースコードレベルのカバレッジ測定とリンクする。

（オ） 性能モデリング
全システムの資源の使用制約と組み合わせて、特定機能のスループットや応答要求事項の満足度を確認する。シミュレーションにより、システムの動作能力が十分あるのか、規定要求事項を満たすことができるかを保証するために行う。

（カ） 同類の値および入力分割試験
同類の値および入力分割試験は、IEC61508-7 の「ANNEX C, C.5.7 Equivalence classes and input partition testing」を参照下さい。
この試験は、入力値の領域の分割を決める入力値の同類値関係に基づく。
試験ケースでは、前もって指定した全分割を処理することを目標に選ばれる。少なくとも試験ケースの一つは各同類値クラスの中からから取られる。

（キ） 構造的テストの網羅率
出来上がったプログラムの解析に際し、プログラムの構造を表す指標を構造テストの網羅率という。プログラムコードの網羅率をコード網羅率と呼び、コード網羅率の目安は、100%が目標である。100%の網羅率達成が不可能なら 100%を達成できない理由を試験報告書に記録しなければならない。

（ク） 構造テスト・入力点網羅率 100%(SIL1,SIL2,SIL3)
ソースコードの実行テスト。複数のモジュールを結合したソフトウェアの中に入力点が無いものが存在しないことを確認する試験。入力しなかったことは使用されなかったことなので、使用されないソフトウェアは決定論的原因故障につながる可能性があるの

で、除去する。入力点(エントリー)について（コールグラフ(*1)）のカバレッジ：
プログラム中の全サブプログラム（サブルーチンや関数）が、少なくとも一度は呼び出されていることを保証する構造テストである。
この指標は、実行されないサブプログラムが含まれていないことを証明する方法である。決定論的原因故障の排除のためであり、実行されないプログラムが、動的オブジェクトや動的変数の起因によって誤実行されないようにするためである。
*１：コールグラフ；関数を呼び出す側と呼びだされる側との関係を矢印で表した図(有向グラフ)。

（ケ） 構造テストの命令網羅率 100%(SIL2,SIL3)
ソースコードの実行テスト。複数のモジュールを結合したソフトウェアのソースコード又はコンパイル後の機械語レベルでソフトウェアの実行経路をたどり、すべての命令が一度は実行されたことを確認する。
実行されていない命令は不要な命令であり、それは、決定論的原因故障につながる可能性があるので、除去する。
このような不要な命令は、ソフトウェアの変更を繰り返したり、他のソフトの一部を利用したりする時に発生し易い。

（コ） 構造テストの分岐網羅率 100%(SIL3)
プログラムコード中のすべての分岐の両側(分岐元、分岐先の情報)を検査する構造テストである。
これは、分岐により、他のプログラムへの影響(スタック内情報)のないことを確認する指標となる。
ソースコードの実行テスト。複数のモジュールを結合したソフトウェアのソースコード又はコンパイル後の機械語レベルでソフトウェアの実行経路をたどり、すべての分岐の分岐先、分岐先から見て分岐元が正しいかを確認する。未結合先へ分岐する場合は、試験未実施を文書化し、該当のソフトウェア結合後再試験をおこなう。すべての分岐を確認し、分岐先が無い、又は分岐元が無い場合は、ソフトウェアの決定論的原因故障につながる可能性があるので、更に解析を行い、分岐先、分岐元の不明をゼロにする。

ウ　機能的及びブラックボックス試験

表 5-21　機能的及びブラックボックス試験

No.	技術/方法	SIL 1	SIL 2	SIL 3
1	原因結果図から試験ケースの実行	---	---	R
2	モデルベースの試験ケースの生成から試験ケースの実行	R	R	HR
3	プロトタイピング/アニメーション	---	---	R
4	境界値解析を含めた、同類の値と入力分割試験	R	HR	HR
5	プロセス･シミュレーション	R	R	R

（ア）　原因結果図から試験ケースの実行

システム内において、基本事象の組み合わせの結果として、発生する事象の順序をコンパクトな図形式で解析・モデル化する技術である。

この技術は、重要な事象から開始し、結果図を動作の成功や故障を示す YES/NO ゲートを使って前方に遡る。これにより、問題の発生する事象シーケンスを作成できる。

（イ）　モデルベースの試験ケースの生成から試験ケースの実行

モデルベースによる試験ケースを自動的に作成し、その試験を実施することが必要である。これには、モデルベース試験を実施できるソフトウェアツールを使用することが望ましい。例としては、LDRA がある。

手動で仕様書やソフトウェアモジュールを基に、試験ケースを作成する場合は、SIL3 の安全度水準の要求に合致しない。

（ウ）　プロトタイピング/アニメーション

予め決められた仕様条件に準じて、システムが実装できるかどうかの可能性を検査するための技術の一つである。プロトタイプモデルやアニメーションにより、仕様書の作成者は、自身のシステム解釈を顧客により具体的に伝達でき、顧客との間の仕様や解釈の違いを見つけることができる。

プロトタイプモデルやアニメーションの対象として、システムの機能、制約、及び性能要求事項の中で特に強調したい部分が選ばれる。高機能なツールを使い、プロトタイプモデルやアニメーションが作製される。この段階では、ターゲットコンピュータの性能、実装言語、プログラム規模、保守性、信頼性及び使用可能性などの制約を考える必要はない。プロトタイプモデルやアニメーションは、顧客側の基準で評価され、システム要求事項はこの顧客評価の結果によって変更される可能性がある。

（エ）　境界値解析を含めた、同類の値と入力分割試験

試験をする境界値が、設計仕様書との正しい関連が求められ、入力データの入力順序が正しく定義される。そのソフトウェア構造は、管理が容易であることが条件である。また、境界値データは、同じ仕様のデータ毎にクラス分けされ、クラス内は同類である必要がある。

（オ）　プロセス・シミュレーション

シミュレーションは、ソフトウェアだけ、又はソフトウェアとハードウェアの組み合わせで行われる。

この試験では、以下を満たさなければならない。

・EUC の入力に等価な入力を提供すること。
・制御を忠実になぞる方法で試験されるソフトウェアの出力に応答すること。
・被試験システムの対処として、オペレータ入力の対策を準備すること。

ソフトウェア試験において、その試験は、入力と出力を備えたターゲットハードウェアのシミュレーションとなる。

エ　性能試験

表 5-22　性能試験

No.	技術/方法	SIL 1	SIL 2	SIL 3
1	アバランシェ/応力試験	R	R	HR
2	応答タイミング及びメモリ制限	HR	HR	HR
3	性能要求事項	HR	HR	HR

機能仕様が明確な試験対象のソフトウェアに対し、求められる性能が得られるかを試験する。通常は機能仕様≧性能仕様である。
性能試験は、ソフトウェアシステムの性能を測り、必要な性能が出ることを確かめる試験である。ハードウェア仕様とソフトウェアの処理速度が関連し、例えば、入力信号をどれだけ(本数や変化速度)受付けるか、出力はどれだけ可能か。通信ノード数・通信速度、割り込み処理件数などプログラム単体では問題が無くても、通信頻度、データベース検索、多入出力（I/0）など、同時処理によるソフトウェアの高負荷、長時間処理などで性能が低下することがある。
性能が仕様に従っていることを確認する試験は、0S やミドルウェアの性能にも影響されるため、それらの性能を確認し、ソフトウェアの性能を測定する。安全関連系では最悪値を以て性能とする。
性能試験は、安全要求仕様書に規定した性能に対し、設計上のその性能に対してディレーティング(マージン、又は安全率)を見込んだ性能に対して実施する。
性能確認のための３つの技法及び手段が推奨されている。該当する安全度水準(SIL)では実施が必要である・

（ア）　アバランシェ/ストレス試験
アバランシェ試験とストレス試験は耐久試験の一種である。簡単に言えば、アバランシェ試験は、定格値に比べ極端な何倍もの負荷を掛けても定格の性能が維持できることである。ストレス試験は、仕様限界の高い負荷を掛ける、又は掛け続ける試験である。
・アバランシェ試験
アバランシェとは「雪崩」のことである。性能試験における試験対象物に極端に高い、例外的な負荷を掛け、その結果に問題が無ければ、試験対象物が、通常の負荷に対しては、容易に耐えることができるとみなす技法及び手段のことである。
電子部品にアバランシェダイオードがある。
・ストレス試験
ストレス試験とは、想定された通常負荷より、高い負荷で正常に動作するか、隠れた故障が無いかを調べる技法及び手段である。耐久試験とも言う。
例えば、ハードウェアやソフトウェアに短時間に大量のデータを与える高い負荷をかけ、製品が正常に機能するかを調べる試験が該当する。
ハードウェアやソフトウェアは、低い負荷の動作では問題なく動作するが、高い集中的な負荷では、動作に問題を起こすということがある。
このような例として、通信情報を割り込みで処理している時、高い負荷の通信頻度を設定すると通信処理が終わらない内に次の通信割り込みがかかり、通信処理が多重に蓄積する状態になり、割り込み時のレジスタ退避のスタックメモリがオーバーフローすることになる。このことにより、マイコンのプログラムが正常なプログラムに戻れず、暴走し、危険状態に陥る事例がある。

通常の使用を想定したテストではなかなか不良が発見できないことがある。このような、アバランシェ/ストレス試験は、装置や機器の限られた状況下での故障発生を検知するために行われる試験である。

（イ） 応答タイミングおよびメモリ制限

システムやソフトウェアの安全要求事項の仕様には、システム構成の制約や機能に対して、メモリ容量や応答時間の要求事項が、通常含まれる。

(例)

・応答時間の例では、安全機能としてライトカーテンを設けた場合、要求される安全距離からライトカーテン遮光から非常停止出力までの応答時間が求められる。応答時間が長いプログラムでは、安全距離がより長くなる。

・メモリ容量の例としては、操作者がボタンを押し、表示器を操作する場合、押されたボタンより、表示データをメモリ内で検索するとした時、操作と表示に対する人の反応時間である最小約 140ms より短い応答時間で表示することが求められる。この時間制限により、メモリ内のデータ検索時間や演算時間が制約され、検索データメモリ容量が制限される。

タイミング、応答速度やメモリ配分を要求事項より解析し、平均および最悪条件下で、メモリや構成部品のリソースの配分を決める。

（ウ） 性能要求事項

性能要求事項は、ソフトウェア結合試験に対し、ソフトウェアシステム設計要求事項に基づき、試験対象の性能を明らかにし、それらの要求事項を定量的、定性的に規定することである。

規定された性能要求事項は、以下を考慮し、測定リストが作成された後、機能試験及び性能試験が実施される。

・性能事項をリストアップする(暗黙知的性能も含め)
・試験での測定方法を決める。
・試験の合格基準を決める。
・測定方法は再現性があり、正確であること。
・実行性のある試験方法であること(コスト、環境、時間等)
・基本性能とオプション的性能は分けて規定する。

(10) ソフトウェア面のシステム安全妥当性確認のフェーズ

ア ソフトウェア面の安全妥当性確認

ソフトウェア面の妥当性確認は、ソフトウェア安全要求事項を満足していることを試験によって確認することである。

通常、ソフトウェアは、組み込まれたハードウェアやそのシステム環境に依存して動作する。そのソフトウェアの妥当性確認に当たっては、ハードウェアやシステム環境が必要となる。

ソフトウェア面の安全妥当性確認試験ための技法又は手段として以下の内容を考慮する。

ⅰ．ソフトウェア安全要求事項に関する項目を全て抽出し、妥当性確認試験を完全に行う。
ⅱ．ソフトウェア安全要求事項に対し、正確な妥当性確認であること
ⅲ．妥当性確認試験方法は試験対象物、試験装置、試験環境が正確に定義され、誰でも同じ試験ができること。
ⅳ．試験の結果に再現性があること
ⅴ．モデル化による妥当性確認試験も可能である。

モデル化は、簡単に言えば「問題解決に必要なパラメータを抜き出して全体を簡単化・抽象化すること」で、動画(CAD による 3D シミュレーションなど)も該当する。

vi．実際の環境を使用する前、又は使用できない(周辺環境が未整備、実行すると損害が発生する)時、ソフトウェアをシミュレーションにより実行することが可能である。

シミュレーションでは、通常動作における入出力信号により想定される事象や望まれない状態をシミュレートする。

イ　安全システム妥当性確認のソフトウェア側面

ソフトウェアは、ハードウェアが実現しようする安全機能の一部を担っている。妥当性確認を行う環境はすべてのハードウェア環境が完備されているとは限らない。また、安全機能は複雑な条件設定が必要かもしれない。

そのような場合、以下の条件を満足すれば、安全機能のある面を取り出し、シミュレーションやモデル化で確認試験することが可能である。

ⅰ．ハードウェアの構成が単純であること。

一般的にはハードウェアの構成は単純である。入出力部、論理部、電源部、通信部等モジュール化構造になっており簡単な機能の組み合わせである。安全機能の複雑な条件はソフトウェアで実現されている場合が多い。

ⅱ．ソフトウェアがモジュール化されていること。

ソフトウェアは設計の段階からモジュール化され、構造化されている。

妥当性確認試験は、原則的にはソフトウェア統合試験完了後に行われ、選定される技法又は手段は、安全システムを試験するために選定される（表 5-23)。

No.	技術/方法	SIL 1	SIL 2	SIL 3
1	確率的試験	---	R	R
2	プロセス･シミュレーション	R	R	HR
3	モデリング	R	R	HR
4	機能的及びブラックボックス試験	HR	HR	HR
5	ソフトウェア安全要求仕様書とソフトウェア安全妥当性確認計画間の前方トレーサビリティ	R	R	HR
6	ソフトウェア安全妥当性確認計画とソフトウェア安全要求仕様書間の後方トレーサビリティ	R	R	HR

（ア）　プロセス・シミュレーション

妥当性確認試験の出力が定義され、それが、正しいことが証明され、出力結果が定義と同じであることが証明されること。妥当性確認に関係する外部環境が定義されていることが必要である。

（イ）　モデリング

SIL3(PLe)では、必須の事項である。

（ウ）　機能的およびブラックボックス試験

統合試験の内容と設計仕様書の矛盾がないことが必要である。

妥当性確認試験による出力が定義され、それが試験結果として満足される必要がある。更に、妥当性確認試験ケース毎に動作順序が定義され、その順序を試験によって満足できる必要がある。

（エ）　ソフトウェア安全要求仕様書とソフトウェア安全妥当性確認計画間の前方

トレーサビリティ

(オ)　ソフトウェア安全妥当性確認計画とソフトウェア安全要求仕様書間の後方トレーサビリティ

(a) 前方トレーサビリティ

初期工程、又は前工程の決定事項が、適切に次の工程で実施されるということ。

(b) 後方トレーサビリティ

後の段階で行われた決定が、初期工程、又は前工程で決定した要求事項に基づいている。

① ソフトウェア安全妥当性確認計画の内容が、ソフトウェア安全要求事項と相互に関連があり、矛盾がないこと(前方/後方トレーサビリティ)。

② ソフトウェア安全妥当性確認計画は、複雑でないこと、

③ 不要な事項が含まれていないこと。

④ トレーサビリティの情報は、ベースライン管理がされていること。

(11)　ソフトウェアの変更(部分改修)

ア　ソフトウェア変更のための要件

ソフトウェア運用中の変更(部分改修)は、変更後も決定論的対応能力が維持されていることが必要である。

変更は以下の要件によって開始され、ライフサイクルの中で決められた変更手順に従って、変更が実施される（図 5-28)。

ⅰ．機能安全が安全要求事項に対し、不満足であることが分かった。
ⅱ．決定論的原因故障が発見された。
ⅲ．新規または改正された安全関係の法令が発令された。
ⅳ．EUC またはその利用法に対する変更があった。
ⅴ．全体の安全要求事項の変更が必要となった。
ⅵ．運転及び保守性能の分析で、性能が目標以下であることがわかった。
ⅶ．定期的機能安全監査から是正勧告が出された。

要求された変更及びその変更活動は、インパクト(影響)解析およびソフトウェアの決定論的対応能力の評価結果により内容が決まる。

イ　ソフトウェアの変更に対する安全計画

変更が承認されたら、変更の実施計画を策定する。計画には、以下のことを考慮する。

ⅰ．作業者、設計者等、職員の確定
ⅱ．職員の必要な力量について検討
　変更後の安全度水準を維持するため、変更活動での設計作業の質を落とすことはできない。
ⅲ．変更仕様について詳細な検討
ⅳ．適合確認計画を検討
ⅴ．変更後の安全度水準の確認のために実施する再妥当性確認試験の範囲を検討
ⅵ．アプリケーション分野によっては特別な力量の要員について検討
ⅶ．全ての変更には実施経過の詳細情報の文書化が必要である。
　その文書化には、再適合確認や再妥当性確認のデータおよび結果を含める。

ウ　ソフトウェアの変更の実施と文書化

ソフトウェアの変更は、全て以下の事項を参照して、詳細に文書化する必要がある。

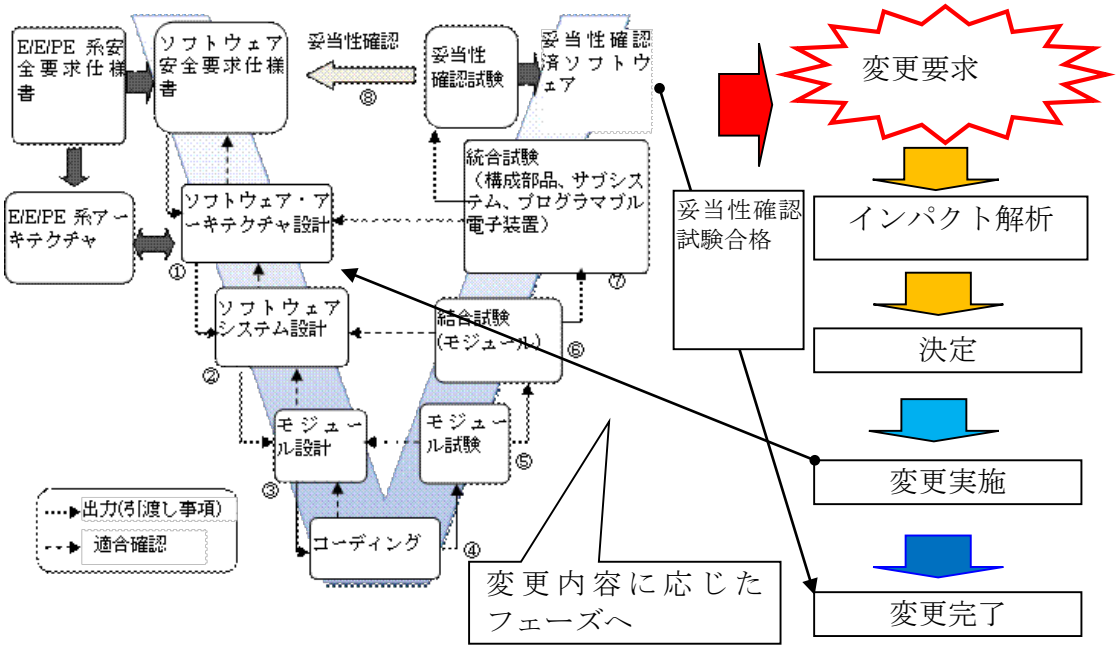


図 5-30　変更(部分改修)工程

ⅰ．変更要求の内容について
　変更が提案されたソフトウェアについて機能安全の観点から変更の影響を評価する影響(インパクト)解析を行い、関連部分への影響の明確化と決定した変更内容を記述する。
ⅱ．ソフトウェア変更の構成管理について
ⅲ．再妥当性確認試験の実施について
　再妥当性確認試験では、通常の運転条件からの逸脱の場合を含め、他のストレス試験の影響を記述する
ⅳ．変更活動の影響を受ける全ての情報を文書化する。

エ　ソフトウェアの変更に関する技法又は手段

ソフトウェアの変更は様々な工程で発生する。変更の及ぼす影響は様々で、それらに適切に対応しないとソフトウェアの決定論的原因故障の要因を作りこんでしまう可能性がある。

変更は、その場ですぐ対応することが必要な場合もある。このような場合は、その内容を記録し、変更のルールに従って再度変更を実施することが必要である。記録に残らない変更は、あってはならない。

変更が発生、変更を行う過程では、以下の技法又は手段を選択し、変更ルールに従い、責任者の承認の元で作業を進める。

表 5-24　ソフトウェアの変更(部分改修)

No.	技法又は手段	SIL 1	SIL 2	SIL 3
1	インパクト解析	HR	HR	HR
2	変更済ソフトウェアモジュールの再適合確認	HR	HR	HR
3	影響を受けるソフトウェアモジュールの再適合確認	R	HR	HR

4a	完全なシステムの再妥当性確認	---	R	HR
4b	回帰妥当性確認	R	HR	HR
5	ソフトウェア構成管理	HR	HR	HR
6	データ記録及び解析	HR	HR	HR
7	ソフトウェア安全要求仕様書とソフトウェア変更計画(再適合確認及び再妥当性確認を含む)間の前方トレーサビリティ	R	R	HR
8	ソフトウェア変更計画(再適合確認及び再妥当性確認を含む)とソフトウェア安全要求仕様書間の後方トレーサビリティ	R	R	HR

(ア)　インパクト(影響)解析

ソフトウェアで実行している機能の変更や機能アップに先立ち、その変更や機能アップが、他のソフトウェアモジュールに及ぼす影響を解析し、文書化すること。

インパクト(影響)解析は、変更箇所がどこに影響するかを調べる技法又は手段である。影響するかどうかは該当ソフトウェアの後方トレーサビリティで確認する。影響しないことを解析することが必要な場合もある。解析方法は、変更内容に依存する。主に機能試験や性能試験、ソフトウェアの構造テストを実施する。

解析の完了後に、ソフトウェアシステムの変更規模により再適合確認、再妥当性確認の実施内容を決定する。この決定は、影響を受けるソフトウェアモジュールの数、影響を受けたソフトウェアモジュールの危険性及び変更の性質に依存する。

影響の大きさにより、適合確認、再妥当性確認の範囲は以下のどれかを選択する。

・変更済のソフトウェアモジュールのみ。
・影響を受けた全ソフトウェアモジュール。
・システム全部。

ソフトウェアのインパクト(影響)解析を行う場合、以下を考慮する。

ⅰ．危険源及びリスクアセスメントが必要かどうか。
ⅱ．どこのソフトウェア安全ライフサイクルのフェーズから解析をするか。
ⅲ．電子等制御安全関連システムの機能安全に影響する変更は、ソフトウェア安全ライフサイクルの適切なフェーズへ戻って作業を開始する。
ⅳ．インパクト(影響)解析により、電子等制御安全関連システムに要求されている安全度水準と異なる安全度水準の必要性が出てきた場合、十分な危険源/リスクアセスメントを実施する。
ⅴ．影響(インパクト)解析の結果は、文書化する。

(イ)　影響を受けるソフトウェアモジュールの再適合確認

インパクト(影響)解析、後方トレーサビリティにより影響を受けるとされたソフトウェアの影響結果を再適合確認する。

影響に対し、要求事項と影響を受けるソフトウェアの関連は良いか、要求事項に関する影響は、正しいか、潜在的障害が作りこまれていないか、影響に関し、回帰試験や適合確認割合目標は達成されているか、確認試験を行う。

再適合確認では、リグレッションの確認を行う。リグレッションとはソフトウェアの変更によって修正済みのバグなどの決定論的原因故障の要因が復活することやソフトウェアのバージョンアップで機能低下することである。

可能な限り、ソフトウェアはモジュール化し、構造化し、ソフトウェア機能範囲を明確にしてリグレッションの試験を低減することが望ましい。

６ 機能安全制御システムの設計の例

(1) 一般事項

安全関連制御システム設計の構造化手法では、安全機能に対する機能およびインテグリティ要求事項を、複数のサブ機能に分解する。この過程は、JIS C 0508(IEC 61508)規格群が規定する機能安全の技術的枠組を機械産業部門内で実現するために用いる。図5-29 は、安全関連制御システムの設計を機械と統合する段階で用いる重要な用語を説明している。

本節に示す安全関連制御システムの設計例は、JIS B 9961(IEC 62061)に規定する機能分解の原則および指定の安全機能の実現法を明確に説明することを意図している。この例は簡単化しており、現実の用例では必要となるかもしれない追加方策、例えば、ホールド・ツゥ・ラン装置などは考慮していない。

図 5-31 に示す用語は設計過程を次の重要な二つの段階に区別することを意図している。

- 安全関連システム設計段階:機械の設計者または制御システムのインテグレータが実施する。
- サブシステム（およびサブシステム要素）設計段階：電気装置および制御装置（例えば、コンタクタ、インタロックスイッチ、PLC など）の供給者、および機械設計者または制御システムインテグレータが実施する。

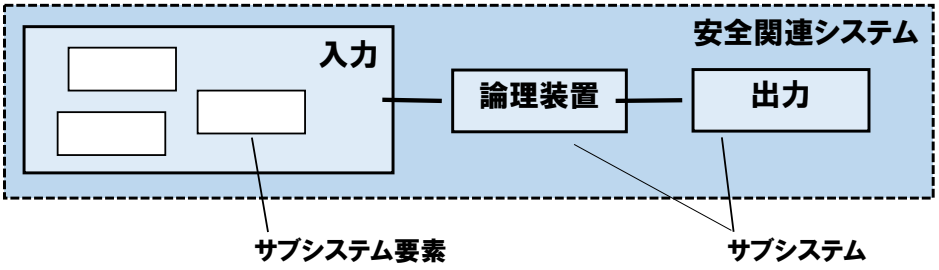


図 5-31 機能分解に用いる用語の図解

(2) 安全関連システム設計の例

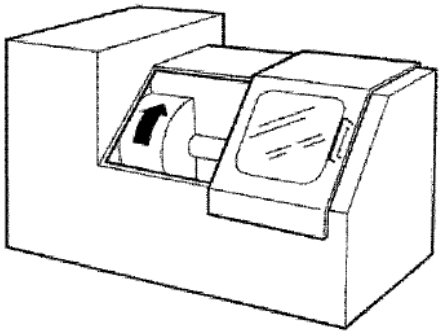


図 5-32 例題の機械

この規格が用いる方法論では、安全機能要求仕様の決定およびそれらの機能を実行する安全関連システムの設計に対して、トップダウン式の構造化手法を用いる。例題として、図 5-32 の機械（旋盤）を扱う。

また、本節は JIS B 9961(IEC 62061)の SIL に基づいた設計を行う。

ステップ 1： 安全関連制御システムの安全要求仕様を決定する。

安全関連制御システム安全要求事項仕様決定段階で、次の情報を得る（図 5-33)。要求安全度水準 SIL2 は、本書第 4 章 4 で述べたようにリスクアセスメントおよび安全機能（リスク低減）に要求される安全度要求(SIL)の分析に基づく。

安全機能要求仕様 (機能および要求安全度水準)	安全機能の例 機能要求 : ガードドアが開いているときは、軸の起点速度は規定値を超えてはならない 要求安全度水準 : SIL2

図 5-33 安全機能要求仕様の作成

ステップ 2： 安全関連システムの設計および開発。

ステップ 2.1： 安全要求仕様に規定された 安全機能を機能ブロックの構造に分解する（図 5-34)。

ステップ 2.2： 機能ブロックの構造は、安全関連システムアーキテクチャの初期概機能ブロックの構造は、安全関連システムアーキテクチャの初期概念である。各機能ブロックに対する安全要求事項は、対応する安全機能の安全要求仕様から導く。

安全機能の要求仕様作成 (機能およびインテグリティ)	安全機能の例 機能要求：ガードドアが開いているときは、軸の起点速度は規定値を超えてはならない インテグリティ要求：SIL2
↓	
安全制御系概念設計 (機能要求およびインテグリティ要求 SIL2 に対して)	次のセンサを用意する。 - ガードドアの位置センサ - 回転軸スピードセンサ センサ出力をロジックソルバで処理する。 - ドア開放または回転速度過大時にモータを外す信号を出す - ロジックソルバの信号に従いモータ電源をオフにする
↓ ↓ ↓ 機能ブロックに要求機能を割り付ける	

図 5-34 機能ブロック構造への安全機能分解

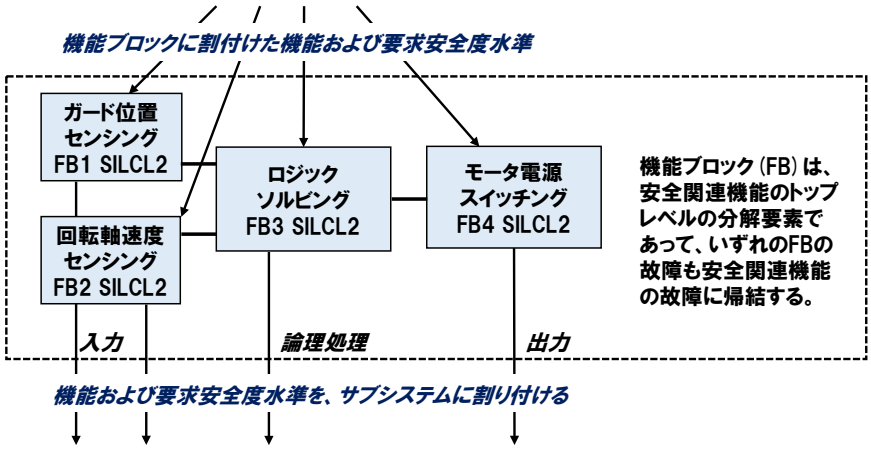


図 5-35 安全関連制御系アーキテクチャの初期概念

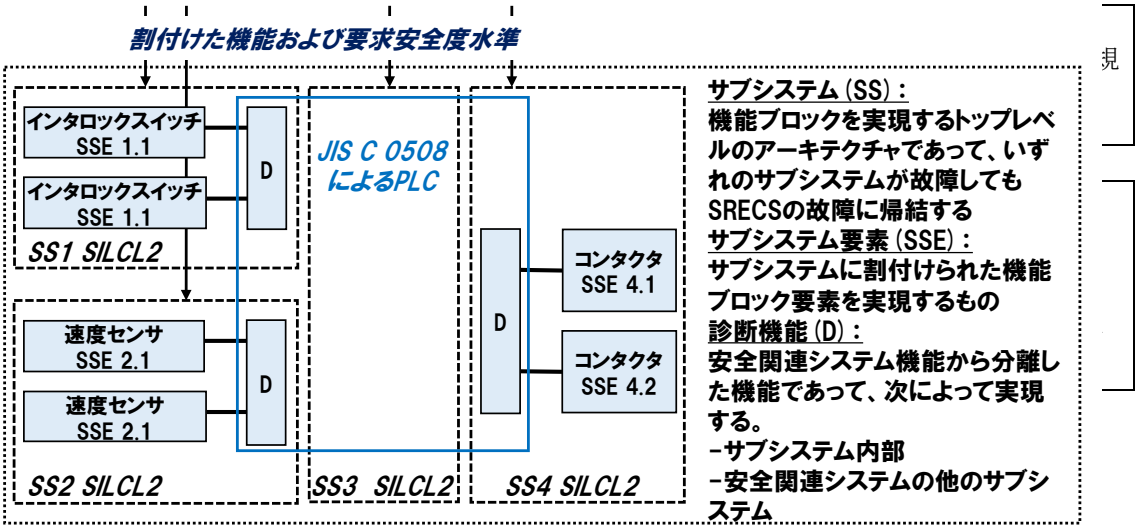


図 5-36 診断機能を SS3 に内蔵する 安全関連制御系アーキテクチャ

各機能ブロックを実現するサブシステム要素は、安全機能に割り付けた SIL と少なくとも同じ SIL を実現しなければならない。図 5-35 において、これは SIL 2 と表記されている。なお、ここで SILCL は、その機能ブロック(FB)が達成すべき SIL(要求 SIL)を意味する。

ステップ 3： 各機能ブロックを 安全関連システムアーキテクチャの中のサブシステムに割り当てる。

各サブシステムは、サブシステム要素で構成する。必要なら、フォールトを検出して適切なフォールト反応を起こすための診断機能も含める。安全関連システムアーキテクチャは、そのサブシステムおよびそれらの相互関係によって表現することが望ましい。

この例では、安全関連システムおよびそのサブシステムアーキテクチャの実現法には多くの選択肢がある。図 5-36 は、入力および出力の診断機能を JIS C 0508 の安全 PLC(同図 SS3)にて実現した例である。実際、規格適合性評価を得た安全 PLC のほとんどは、入出力の診断機能を内蔵している。

ステップ 4：安全関連システムが達成する SIL の推定

安全関連システムに付与できる SIL は、各サブシステムの SILCL のうちの最も低い値以下でなければならない。

安全関連システムの PFH_{DSRECS} は、安全機能の遂行にかかわるすべてのサブシステムの PFH $_D$ (PFH_{D1} ~ PFH_{Dn}) の和であり、該当する場合は、デジタルデータコミュニケーションの危険側伝送誤り (P_{TE}) を含めなければならない。すなわち、

$PFH_{DSRECS} = PFH_{D1} + \cdots\cdots + PFH_{Dn} + P_{TE}$

この例では、安全機能の目標故障率は SIL2 である。JIS C 0508(IEC 61508)によると、SIL2 とは、PFH_D が $10^{-6} > PFH_D \geqq 10^{-7}$ の範囲にあることである。各サブシステムの PFH_D を図 5-37 に示すように仮定すると、すべてのサブシステムの PFH_D の合計は 6×10^{-7} と見積もることができ、SIL2 の条件を満たしている。したがって、割り当てた安全機能を SIL2 のインテグリティで実行するためのすべての要求事項を満足する安全関

連システム設計であることが示されたことになる。

7 防護層(protection layer)

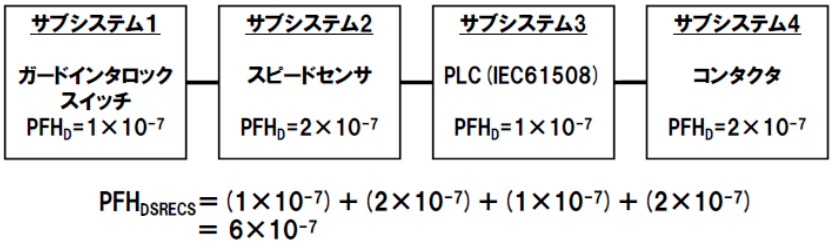


図 5-37 安全関連システムの PFH_D の見積り

(1) 概念

安全関連部の設計は、安全制御システムの他にも追加の保護方策などの独立した多層的な安全対策をとることが多い。このような、制御、予防または緩和によってリスクを軽減する任意の独立した機構のことを、「防護層(protection layer)」と呼ぶ。

防護層の考え方は、機械安全よりもプロセス安全の分野で確立し、JIS C 0511(IEC 61511)において定義されている。これは、危険な化学物質を貯蔵する容器の大きさを制限するなどのプロセス工学的仕組み、安全弁などのような機械工学的仕組み、安全計装システムまたは差し迫った潜在危険に対する緊急避難計画のような行政手続きであってもよい。これらの対処手段は、自動化されても、または人間によって開始されてもよい。

防護層の例を図 5-38 に示す。

図 5-38 プロセスプラントに見られる一般的なリスク軽減法

(2) 防護層への安全機能の割当て

機械およびその関連装置（例えば基本制御装置）に対して、潜在危険およびリスク評価を行わなければならない。この評価によって、それぞれの防護層への安全機能の割当ての概略を示す。

① 目的

この箇条の要求事項の目的は、次による。

a)防護層へ安全機能を割り当てる。

b)要求される 安全機能を決定する。

c)それぞれの安全機能に対する安全度水準を決定する。

② 割当過程

a)このプロセスおよびそれに関連した機器から生じる潜在危険を予防、制御または緩和するための個々の防護層への安全機能の割当て

b)安全機能へのリスク低減目標の割当て

c)規制および法令の要求事項が割当て過程の優先順位を決定する場合もある。

③ 共通原因、共通モードおよび従属故障にかかわる要求事項

防護層の設計は、防護層間および防護層と基本制御システムとの間の共通原因、共通モードおよび従属故障（他の故障発生が条件となって発生する故障）の発生の確からしさが防護層全体の全安全度要求事項に比較して十分に低いことを保証するために評価されなければならない。この評価は、定性的または定量的なもののいずれでもよい。

(3) 防護層の評価

a)防護層間での独立性

b)防護層間の技術的多様性

c)異なる防護層間での物理的な分離

d)防護層間および防護層と基本制御システムとの間の共通原因故障（例えば、開放弁の閉そくは 安全計装システムの検出端の閉そくという同類の問題を引き起こさないか)。

④ 防護層（PL）の評価基準

a） 独立性：他の PL と共通原因故障又は共通モード故障を引き起こす可能性がない。

b） 他の防護層と異なった技術で設計(多様化)されている。

c） 物理的な分離は、防護層間が電気的に分離されている。又は、位置的に分離されている。つまり、電源系統が異なる。空間的に分離されている。このことで防護層間の影響が低減されるなど。

ある防護層からの故障の影響を受けないように設計する。

d） 共通原因故障の例

２つ以上の防護層に機能が故障しないか？

⑤ 防護層(PL)の要件

- 少なくとも 10 倍に特定されたリスクを軽減する。
- 特異性→PL は，1 件の潜在的危険事象の結果を防止又は緩和するように設計されている。
- 複数の原因が同じ危険事象を引き起こすことがある。したがって，複数の事象シナリオが PL によって開始される場合がある。
- 他のいかなる要求された PL との共通原因故障又は共通モード故障を引き起こす可能性がないことが実証される場合，ある PL は他の防護層から独立している。

・　信頼性→PL は，その設計に際し，ランダム故障及び決定論的原因故障を取り組むことによって，それがなすように設計されたことを実行すると期待してよい。
・　監査能力–PL は，防護機能の定期的な妥当性確認を容易にするように設計される。

第６章　妥当性確認

１ 概要

(1) 妥当性確認とは

妥当性確認は、安全関連システムを構成する製品と全体システムに対して行う。

本章では、JIS C 0508-4(IEC 61508-4)の 3.8.2 項で定義される妥当性確認(validation)について機能安全規格に適合させるための実際の具体的作業について述べる。

なお、妥当性確認とは、次のように定義されている。注記２にあるように、安全関連系が安全要求仕様に適合していることの確認である。検証(verification)との違いに注意してほしい。

JIS C 0508-4　3.8.2

妥当性確認（validation）

仕様上に定めた使用法に関する特定の要求事項が満足されていることの審査、及び客観的な証拠の提供による確認。

注記 1　この規格群では、次の三つの妥当性確認フェーズを取り扱う。

- 全安全妥当性確認（JIS C 0508-1 の図 2 参照）
- E/E/PE 系妥当性確認（JIS C 0508-1 の図 3 参照）
- ソフトウェア妥当性確認（JIS C 0508-1 の図 4 参照）

注記 2　妥当性確認は、検討段階又は設置前後の安全関連系が全ての観点から安全要求仕様に適合していることを実証する業務である。そのため、例えば、ソフトウェア妥当性確認は、客観的な根拠を審査し提示することによって、当該ソフトウェアがソフトウェア安全要求仕様を満足することの確認を意味する。

妥当性確認とは、安全関連系への安全要求事項の割当てを考慮して、安全関連系の安全要求仕様への適合性についてその妥当性を確認することを目的とする。安全関連系の仕様のほとんどは、仕様の評価試験によって評価されているので、ここでは主に機能安全規格への適合性について確認する。

機能安全規格への適合性は、以下の３つの視点から判断される。

- 開発プロセスが機能安全マネジメントに従っていたか
- 採用した開発手法が SIL または PL の要求に適合している
- 信頼性指標(PFD/PFH、MTTFd、DCavg など)が目標値を満足しているか

(2) 機能安全マネジメント

機能安全は、設計ミスやバグなど体系的故障を回避するために、一般的な品質管理マネジメントよりも厳格なマネジメントプロセスを要求している。安全関連系の要求分析から実現までが、当初計画したマネジメントプロセスに適合していたかを監査する。

例えば、JIS C 0508 によれば、妥当性確認には以下の文書を参照する。

- 経時的な形式による妥当性確認業務の記録

・使用した全安全要求仕様の改訂番号
・（テスト又は解析によって）妥当性確認した当該安全機能
・使用した機器及び装置，並びに校正データ
・妥当性確認業務の結果
・テストしたアイテム，適用した手順，及びテスト環境の校正の同定
・期待したものと実際の結果との不整合

もし、実際の結果が予想とは異なる場合、当初の要求を見直すか妥当であると判断するかを決定する。その判断を文書化しなければならない。

(3) SIL/PL 要求適合

よく、SIL/PL への適合性では、PFD/PFH あるいは MTTFd、DCavg の数値指標に目がいくが、それだけが SIL/PL の要求ではない。JIS C 0508-2 付属書 A や JIS C 0508-3 付属書 A、B には、安全関連部の開発において採用すべき手法が SIL 毎に示されている。

これらの要求への対応方法は、開発計画書(V&V プラン)あるいは設計仕様書、試験仕様書に記載されているので、その内容を確認する。別の方法で代替した場合は、その妥当性について判断する。この判断には、規格要求からチェックリストを作成し、要求への対応を記載する。SIL2 チェックリストの例を表 6-1 に示す。

表 6-1　SIL2 要求適合チェックリストの例（IEC61508-2 表 A.16 に基づく）

表 A.16−環境上のストレス又は影響によって生じる決定論的原因故障を管理するための技法及び手段			
ID	技法または手段	要求度	対応
1	危険側故障をもたらすことがある電源喪失，電圧変動，過電圧，低電圧，交流電源周波数変動などの現象に対する手段	M	
2	通信線からの電力線の分離	M	
3	電磁イミュニティの増大	M	
4	的環境（例えば，温度，湿度，水，振動，ほこり，腐食性物質）に対する手段	M	
5	プログラムシーケンス監視	HR	
	...		

製品(コンポーネント)およびシステムの SIL 適合評価のワークフローを図 6-1 および図 6-2 に示す。

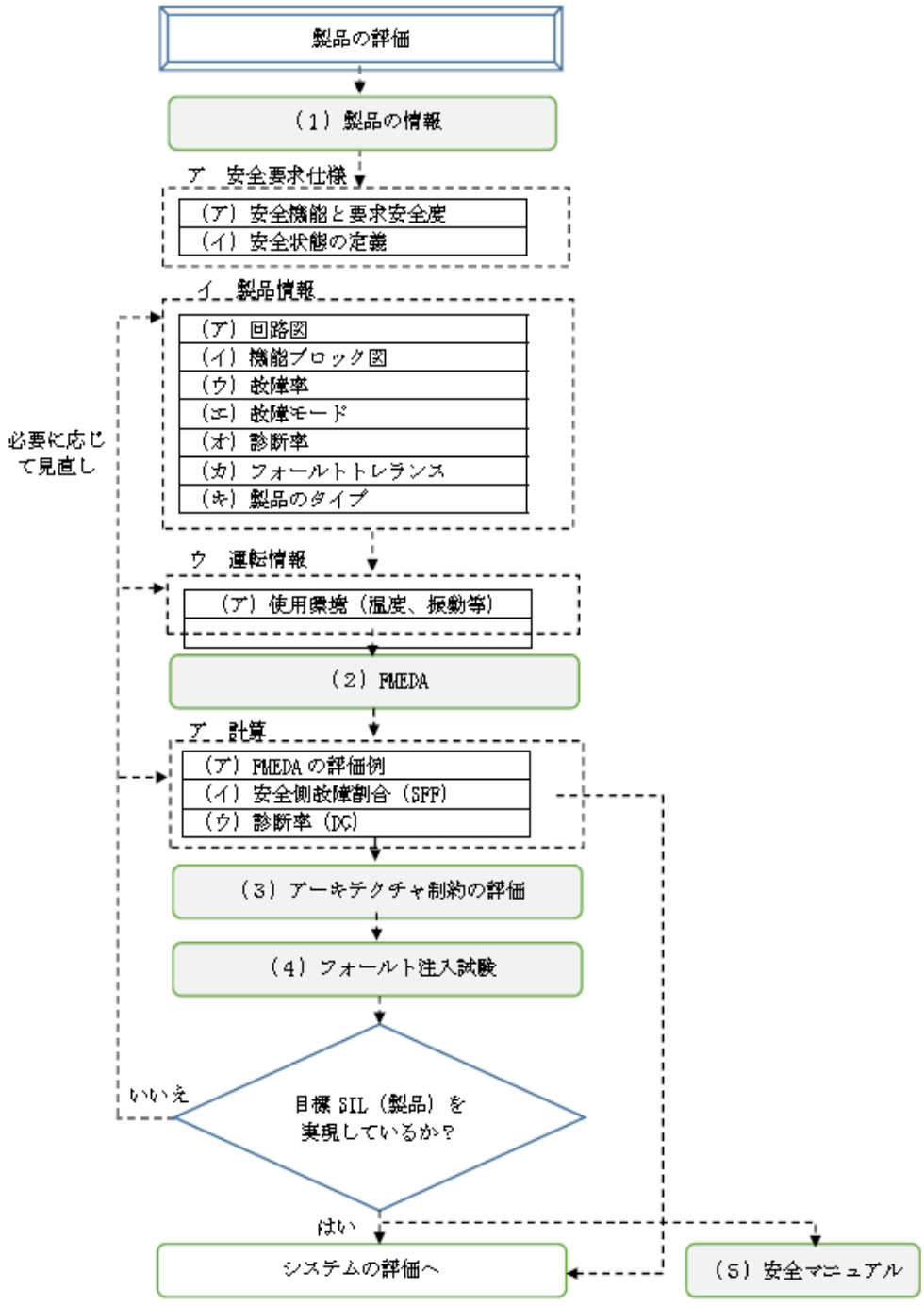


図 6-1　製品(コンポーネント)の SIL 適合ワークフロー

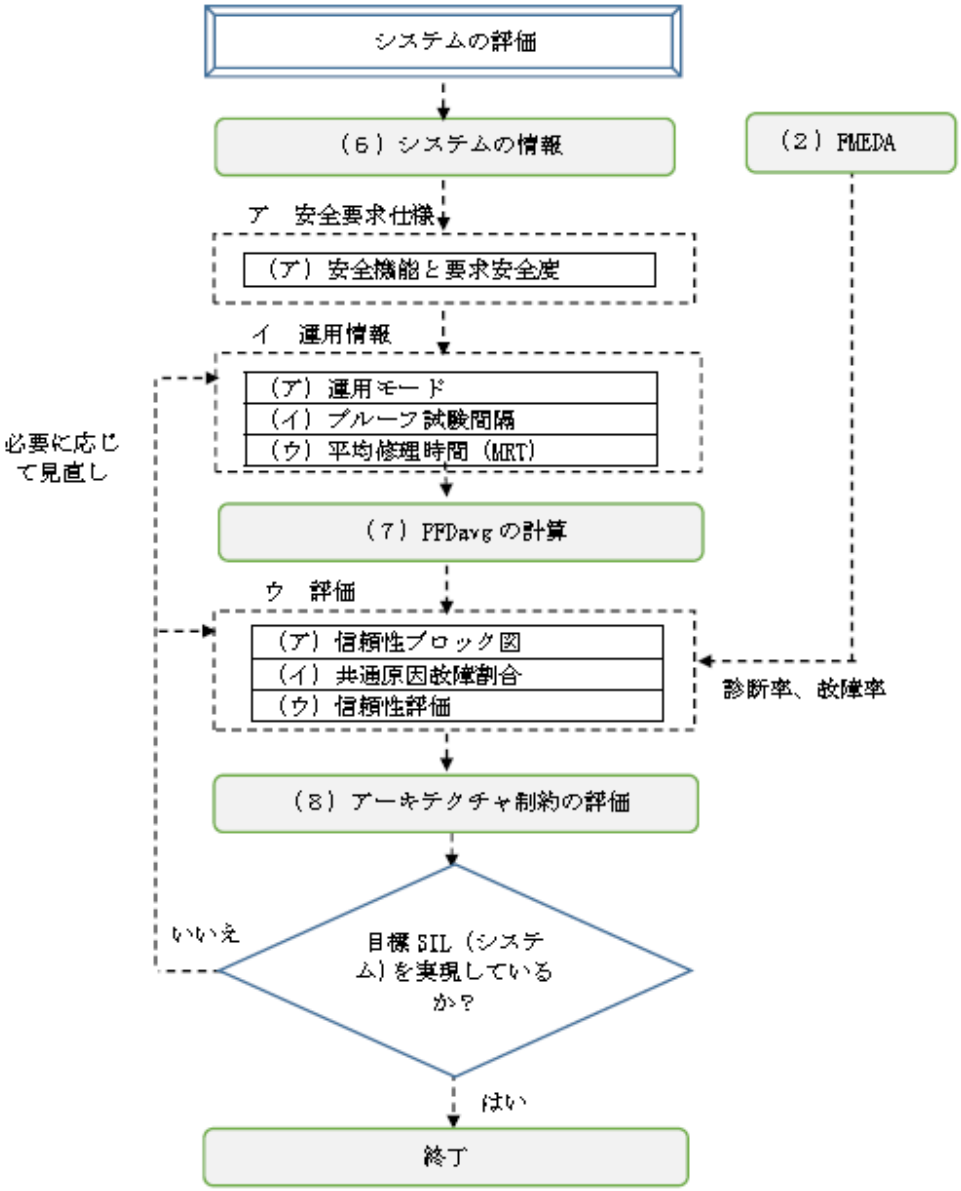


図 6-2　システムの SIL 適合ワークフロー

２ 全安全妥当性確認

(1) 要求事項

全安全妥当性確認は、機能安全ライフサイクル（本書第 5 章、図 5-2）における「フェーズ 13」に該当する。この細分箇条の要求事項は、安全関連システムに固有のものである。これらは、EUC 耐用年数全体にわたって管理することが必要な他リスク軽減措置に関して、既に立てられている仮定を特に考慮して、他リスク軽減措置との観点からみて検討することが望ましい。その場合、機能の安全性を達成するために、同様の要件が全ての他リスク軽減措置に必要である。

妥当性確認は、安全関連システムの安全機能の全安全妥当性確認計画に従って行わなければならない。妥当性確認の過程で使用する全ての計測器・計測装置を、国家標準又は供給者の仕様書を参照して校正しなければならない。

(2) 文書化

妥当性確認に関する文書化された情報には、次の事項を含めなければならない。

・経時的な形式による妥当性確認業務の記録
・使用した全安全要求仕様の改訂番号
・(テスト又は解析によって) 妥当性確認した当該安全機能
  - 使用した機器及び装置、並びに校正データ
  - 妥当性確認業務の結果
  - テストしたアイテム、適用した手順、及びテスト環境の校正の同定
  - 期待したものと実際の結果との不整合

実際の成績結果と期待されたものとに不整合があるときは、妥当性確認を続行するか、又は変更の要求によって妥当性確認業務以前のフェーズに戻るかを決定する。実施した解析及び決定を文書化しなければならない。

3 安全関連システムの妥当性確認

(1) 要求事項

安全関連システムの安全妥当性確認は、準備した計画に従って実施しなければならない（JIS C 0508-3 の 7.7 も参照)。

プログラマブル電子式の安全関連システムの妥当性確認は、ハードウェア及びソフトウェアの両方の妥当性確認で成り立つ。ソフトウェアの妥当性確認の要求事項は、JIS C 0508-3 に規定している。なお、安全関連システムの安全ライフサイクルにおいて、安全関連システムの安全妥当性確認は、設置以前に実施するものとしているが、場合によっては、安全妥当性確認が設置後まで実施できないことがある（例えば、アプリケーションソフトウェアの開発が設置後までに完了していない場合)。

妥当性確認に使用するすべてのテスト装置は、正しく動作するかをテストしなければならない。また、すべての計測器・測定装置は、国家標準とトレーサビリティが取れた基準器または広く認知された手順に準拠した基準器と校正しなければならない。安全関連システム安全要求事項（JIS C 0508-1 の 7.10 参照）で規定している各安全機能、安全関連システム設計要求仕様（7.2 参照)、並びに安全関連システム運用及び保全手順の十分な実現を、テスト及び／又は解析で妥当性確認しなければならない。十分な独立性若しくは個々の要素又はサブシステムの間の非干渉化を解析的に実証できない場合は、関連の機能動作の組合せをテストしなければならない。

供給者又は開発者は、EUC 及び EUC 制御システムの開発者が、JISC 0508-1 の全安全妥当性確認の要求事項を満たすことができるように、安全関連システムの安全妥当性確認テストの結果を利用できるようにしなければならない。

安全関連システムの安全妥当性確認に発生するフォールトを回避するため、規格に従った一連の適切な技法及び手段を使用しなければならない。

(2) 文書化

各安全機能に関して次の事項を記載した、安全関連システムの安全妥当性確認テストの適切な文書を作成しなければならない。

a)使用中の安全関連システムの安全妥当性確認計画の版。

b)テスト（又は解析）中の安全機能及び安全関連システムの安全妥当性確認の計画中に規定した要求事項への個別の参照先。

c)使用したツール及び機器並びに校正データ。

d)各テストの結果。

e)予想した結果と実際の結果との差異。

各安全機能に関して個別の文書は必要でないが、a)~e) の情報は全ての安全機能に適用しなければならず、また情報が安全機能ごとに異なっている場合は、その関係を記述しなければならない。

差異が生じた場合（すなわち、実際の結果が規定の許容差を超えて予想結果と異なっている場合)、安全関連システムの安全妥当性確認テストの結果は、次の事項を含めて文書化しなければならない。

a)実施した解析。

b)テストを続行するか、又は変更要請を出して、妥当性確認テストの初期段階に戻らなければならないかどうかについて下した決定。

4 ソフトウェア妥当性確認

(1) 概要

ソフトウェア妥当性確認の要求事項の目的は、統合したシステムが、要求安全度水準で、ソフトウェア安全要求仕様に必ず適合するようにすることである。ソフトウェアのシステム安全妥当性確認は、ソフトウェア開発プロセスの最後のフェーズになる。

ソフトウェアは、通常、その基盤となるハードウェア及びシステム環境から引き離した状態では妥当性確認することはできない。

(2) 要求事項

妥当性確認に関する要求事項を実現するための適切な技法及び手段を選択する場合、安全妥当性確認について、次の特性（特性の解釈の手引書は IEC 61508-7 の附属書 C を、参考となる定義は附属書 F を参照）を検討することが望ましい。

- ソフトウェア設計仕様に関する妥当性確認の完全性
- ソフトウェア設計仕様に関する妥当性確認の正確性（正常完了）
- 再現性
- 正確に定義した妥当性確認構成

安全妥当性確認計画で、安全関連ソフトウェアの要求事項への適格性を安全関連システム（JIS C 0508-2 の 7.7 参照）に関して既に確立している場合は、妥当性確認を繰り返す必要はない。

妥当性確認業務は、システム安全のソフトウェアに関する妥当性確認計画に規定するとおりに実施しなければならない。

システム安全の安全関連ソフトウェアの妥当性確認は、次の要求事項を満たさなければならない。

a)テストは、ソフトウェアの主要な妥当性確認法でなければならない。妥当性確認業務を補足するために、解析、アニメーション及びモデリングを用いてもよい。

b)ソフトウェアは、次のシミュレーションによって実行しなければならない。

1) 通常動作時に出る入力信号

2) 予想する事象

3) システム動作を要求する望ましくない状態

c)サプライヤ及び／又は開発者（若しくは適合性に責任を負う複数の当事者）は、製品が JIS C 0508-1 及び JIS C 0508-2 の要求事項を満たすことができるように、システム安全のソフトウェアの妥当性確認に関する文書化した結果、及び全ての関連文書を、システム開発者に提供しなければならない。

システム安全の安全関連ソフトウェアの妥当性確認結果は、次の要求事項を満たさなければならない。

a)テストは、規定した安全関連ソフトウェアの全ての要求事項を正確に満たし、ソフトウェアが想定外の機能を実行することがないことを、示さなければならない。

b)テストケース及びそれらの結果は、安全度水準が要求する以降の解析及び独立した評価（JIS C 0508-1 の箇条 8 参照）用に文書化しなければならない。

c)システム安全のソフトウェアの妥当性確認結果を示す文書には、ソフトウェアが妥当性確認に合格したか、又は妥当性確認に不合格となった理由のいずれかを、明記しなければならない。

(3) 文書化

ソフトウェア開発の性質に応じて、JIS C 0508-1 の箇条 7.7 への適合責任は複数の当事者が負うことがある。責任分担は、安全計画時に文書化しなければならない（JIS C 0508-1 の箇条 6 参照)。

システム安全のソフトウェアの妥当性確認結果は、文書化しなければならない。ソフトウェア安全妥当性確認では、安全機能別に、次の結果を文書化しなければならない。

a)業務のシーケンスを遡及できるようにする、妥当性確認業務の経時的記録

b)使用するシステム安全のソフトウェアの妥当性確認計画のバージョン

c)（テスト又は解析によって）妥当性確認する安全機能と合わせて、システム安全のソフトウェアの妥当性確認計画の参照

d)校正データ、並びに校正に使用するツール及び機器

e)妥当性確認業務の結果

f) 予想結果と実際の結果との不整合

予想結果と実際の結果との不整合が生じた場合、妥当性確認を続けるか、又は変更要請を出して開発ライフサイクルの前の段階に戻るかどうかに関して行った解析及び決定事項を、システム安全のソフトウェア妥当性確認結果の一部として、文書化しなければならない。

附録 A 機能安全関係法令及び関係通達

＜機能安全指針関係＞

○ 労働安全衛生法

（技術上の指針等の公表等）
第二十八条　厚生労働大臣は、第二十条から第二十五条まで及び第二十五条の二第一項の規定により事業者が講ずべき措置の適切かつ有効な実施を図るため必要な業種又は作業ごとの技術上の指針を公表するものとする。
２～４　略

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

（関係通達：平成 28 年９月 30 日付け基発 0930 第 32 号）

第２

５　機能安全指針の制定

(1)　趣旨及び適用（機能安全指針１関係）

ア　「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１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こと。

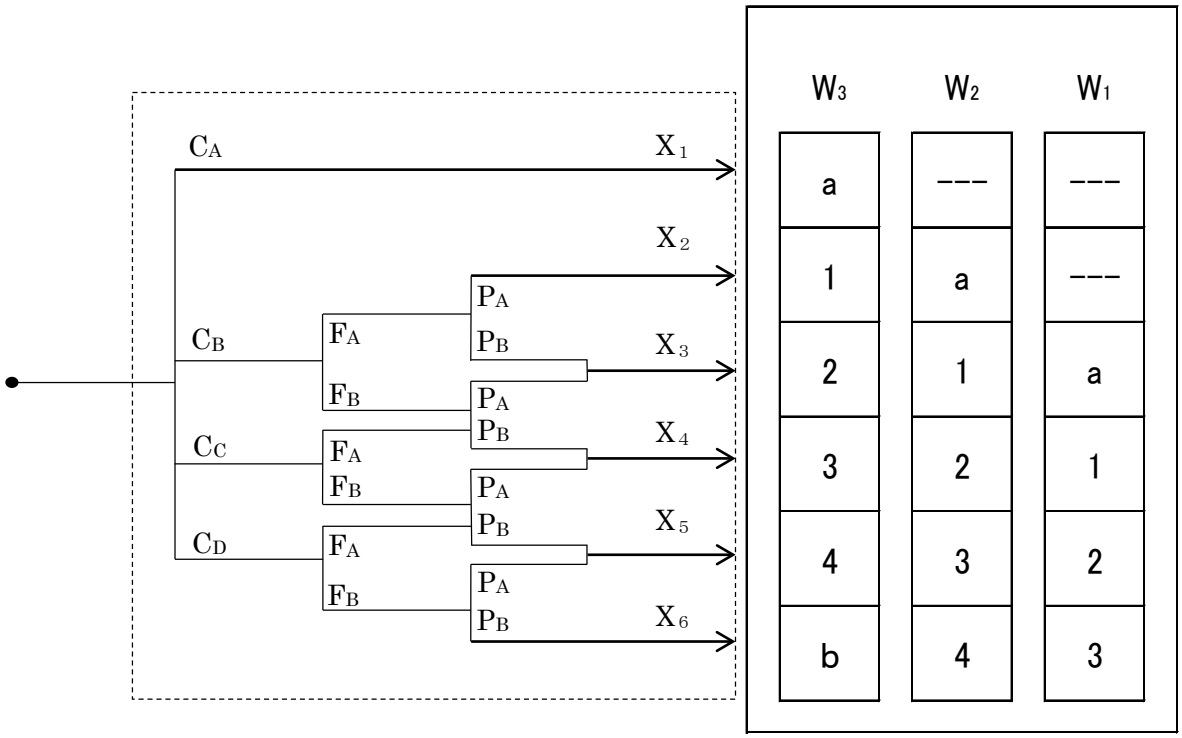
イ　機能安全指針は、新たに電子等制御の機能を付加することによって安全確保を図ることが可能な全ての機械等に対して適用されること。

(2)　要求安全度水準の決定（機能安全指針３関係）

発生状況により、同一の故障が危険側の故障となったり、安全側の故障となったりするような複雑な電子等制御でない場合であって、どのような故障が発生しても危険側の故障とならないように制御できる方策（フェールセーフ）が採用されているときは、要求安全機能及び安全関連システムの特定とそれに対する要求安全度水準の決定を省略することができること。ただし、フェールセーフがコンピュータ制御の機能によって実現している場合は、フェールセーフの故障を想定した要求安全機能の特定及び要求安全度水準の決定が必要であること。

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

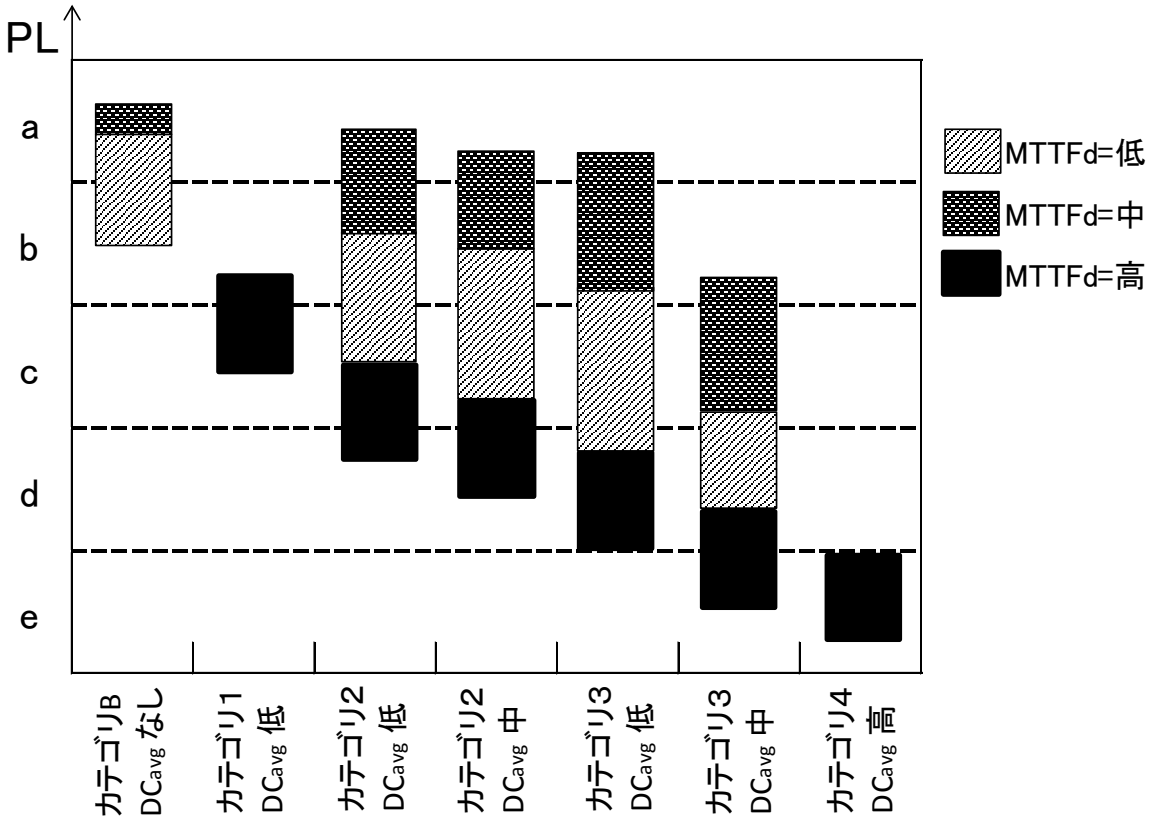
低頻度の作動要求モードにおける要求安全度水準の計算例
（国際電気標準会議の規格 61508-6 を参考にしたもの）

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

$\mathrm{PFD_{avg}}$：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

＜ロボット関係＞

○　労働安全衛生法（昭和 47 年法律第 57 号）

（事業者の講ずべき措置等）
第 20 条　事業者は、次の危険を防止するため必要な措置を講じなければならない。
一　機械、器具その他の設備（以下「機械等」という。）による危険
二　爆発性の物、発火性の物、引火性の物等による危険
三　電気、熱その他のエネルギーによる危険

（安全衛生教育）
第 59 条　略
２　略
３　事業者は、危険又は有害な業務で、厚生労働省令で定めるものに労働者をつかせるときは、厚生労働省令で定めるところにより、当該業務に関する安全又は衛生のための特別の教育を行なわなければならない。

○　労働安全衛生規則（昭和 47 年労働省令第 32 号）

（特別教育を必要とする業務）
第 36 条　法第 59 条第 3 項の厚生労働省令で定める危険又は有害な業務は、次のとおりとする。
１～32　略
31　マニプレータ及び記憶装置（可変シーケンス制御装置及び固定シーケンス制御装置を含む。以下この号において同じ。）を有し、記憶装置の情報に基づきマニプレータの伸縮、屈伸、上下移動、左右移動若しくは旋回の動作又はこれらの複合動作を自動的に行うことができる機械（研究開発中のものその他厚生労働大臣が定めるものを除く。以下「産業用ロボット」という。）の可動範囲（記憶装置の情報に基づきマニプレータその他の産業用ロボットの各部の動くことができる最大の範囲をいう。以下同じ。）内において当該産業用ロボットについて行うマニプレータの動作の順序、位置若しくは速度の設定、変更若しくは確認（以下「教示等」という。）（産業用ロボットの駆動源を遮断して行うものを除く。以下この号において同じ。）又は産業用ロボットの可動範囲内において当該産業用ロボットについて教示等を行う労働者と共同して当該産業用ロボットの可動範囲外において行う当該教示等に係る機器の操作の業務
32　産業用ロボツトの可動範囲内において行う当該産業用ロボツトの検査、修理若しくは調整（教示等に該当するものを除く。）若しくはこれらの結果の確認（以下この号におい

て「検査等」という。）（産業用ロボツトの運転中に行うものに限る。以下この号において同じ。）又は産業用ロボツトの可動範囲内において当該産業用ロボツトの検査等を行う労働者と共同して当該産業用ロボツトの可動範囲外において行う当該検査等に係る機器の操作の業務

33～38　略

（関係告示：労働安全衛生規則第 36 条第 31 号の規定に基づく厚生労働大臣が定める機械（昭和 58 年労働省告示第 51 号））

労働安全衛生規則第 36 条第 31 号の厚生労働大臣が定める機械は、次のとおりとする。

一　定格出力（駆動用原動機を二以上有するものにあっては、それぞれの定格出力のうち最大のもの）が 80 ワット以下の駆動用原動機を有する機械

二　固定シーケンス制御装置の情報に基づきマニプレータの伸縮、上下移動、左右移動又は旋回の動作のうちいずれか一つの動作の単調な繰り返しを行う機械

三　前二号に掲げる機械のほか、当該機械の構造、性能等からみて当該機械に接触することによる労働者の危険が生ずるおそれがないと厚生労働省労働基準局長が認めた機械

（運転中の危険の防止）

第 150 条の４　事業者は、産業用ロボットを運転する場合（教示等のために産業用ロボットを運転する場合及び産業用ロボットの運転中に次条に規定する作業を行わなければならない場合において産業用ロボットを運転するときを除く。）において、当該産業用ロボットに接触することにより労働者に危険が生ずるおそれのあるときは、さく又は囲いを設ける等当該危険を防止するために必要な措置を講じなければならない。

（関係通達：昭和５８年６月２８日付け基発第３３９号　労働基準局長通達）

第３の５

（１）略

（２）産業用ロボットを使用する事業者が、労働安全衛生法第 28 条の２による危険性等の調査（以下「リスクアセスメント」という。）に基づく措置を実施し、産業用ロボットに接触することにより労働者に危険の生ずるおそれが無くなったと評価できるときは、本条の「労働者に危険が生ずるおそれのあるとき」に該当しないものとすること。評価結果は、「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 日付け指針

公示第１号。以下「指針」という。）に基づき記録し、保管するものとすること。

なお、リスクアセスメントは指針に基づき実施するとともに、指針の９（３）前段アの「はさまれ、墜落等の物理的な作用」の危険性による負傷の重篤度及びそれらが発生する可能性の度合の見積りに当たっては、特に以下の事項に留意するものとすること。

イ　産業用ロボットのマニプレータ等の力及び運動エネルギー

ロ　産業用ロボットのマニプレータ等と周辺構造物に拘束される可能性

ハ　マニプレータ等の形状や作業の状況（突起のあるマニプレータ等が眼などに激突するおそれがある場合、マニプレータ等の一部が鋭利である場合、関節のある産業用ロボットのマニプレータ間に挟まれる可能性がある場合等）

（３）「さく又は囲いを設ける等」の「等」には、次の措置が含まれること。

イ～ニ　（略）

ホ　国際標準化機構（ISO）による産業用ロボットの規格（ISO 10218－1：2011 及び ISO 10218－2:2011）によりそれぞれ設計、製造及び設置された産業用ロボット（産業用ロボットの設計者、製造者及び設置者がそれぞれ別紙に定める技術ファイル及び適合宣言書を作成しているものに限る。）を、その使用条件に基づき適切に使用すること。なお、ここでいう「設置者」とは、事業者（ユーザー）、設置業者、製造者（メーカー）などの者のうち、設置の安全条件に責任を持つ者が該当すること。

別紙（技術ファイル及び適合宣言書の内容）

１　技術ファイルの内容

（１）機械の全般的説明

（２）機械の全体図、制御回路の図面及び機械の運転の理解に必要な関連する記述と説明

（３）機械が本質的な安全及び健康の要件に適合していることの確認に必要な、完全な詳細図面、付随する計算書、試験結果、証明書等

（４）以下の内容を含む、リスクアセスメントを実施した手順を示す文書

①機械に適用される本質的な安全及び健康の要件のリスト

②同定された危険性又は有害性の除去又はリスクの低減のために実施された防護方策の説明及び該当する場合は機械に関連する残留リスクの明示

（５）使用した規格及び他の技術仕様書、また、それらの規格等に含まれる本質的な安全及び健康の要件の説明

（６）製造者又は製造者若しくは正式な代表者に選定された機関によって実施された試験の結果を示す技術報告書

（７）機械の取扱説明書の写し

（８）該当する場合は、組み込まれた部分完成機械の組込宣言書及び当該部分完成機械に関する組立て説明書

２　適合宣言書の内容

（１）製造者の名称、住所及び正式な代表者の氏名
（２）上記１の技術ファイルを編さんする権限を付与された者の名称及び住所
（３）総称としての表示名、機能、モデル、型式、製造番号、商品名を含む機械の説明及び識別方法

（関係通達：平成 25 年 12 月 24 日付け基安安発 1224 第 1 号　労働基準局安全衛生部安全課長通達）

1　改正施行通達の記の第 3 の 5 の(2)関係
① 略
②イの産業用ロボットのマニプレータ等の力及び運動エネルギーについては、国際標準化機構(ISO)の産業用ロボットの規格の技術仕様書(TS15066)において、人に危害を加えないと判断される数値を審議中であること。本技術仕様書が制定され、制御によらず構造的に当該数値以下となることが担保される場合、この観点において危険の生ずるおそれが無いと判断できる一例となること。
③ロについて、マニプレータ等と周辺構造物との間隔(最接近距離)を 500㎜ 以上とするか、又は人体がマニプレータ等と周辺構造物との間に拘束された場合、駆動用動力なしで人力で開放できる場合は、この観点において危険の生ずるおそれが無いと判断できる一例となること。
2　改正施行通達の記の第 3 の 5 の(3)のホ関係
国際標準化機構(ISO)の産業用ロボットの規格(ISO　10218-1:2011 及び ISO　10218-2:2011)については、それぞれ対応する日本工業規格(JIS　B8433-1(予定)及び JIS B8433-2(予定))を作成準備中であること。

＜ボイラー関係＞

○　労働安全衛生法

（作業主任者）
第十四条　事業者は、高圧室内作業その他の労働災害を防止するための管理を必要とする作業で、政令で定めるものについては、都道府県労働局長の免許を受けた者又は都道府県労働局長の登録を受けた者が行う技能講習を修了した者のうちから、厚生労働省令で定めるところにより、当該作業の区分に応じて、作業主任者を選任し、その者に当該作業に従事する労働者の指揮その他の厚生労働省令で定める事項を行わせなければならない。

○　労働安全衛生法施行令

（作業主任者を選任すべき作業）
第六条　法第十四条 の政令で定める作業は、次のとおりとする。
１～３　略
４　ボイラー（小型ボイラーを除く。）の取扱いの作業
５～23　略

○　ボイラー及び圧力容器安全規則（昭和四十七年労働省令第三十三号）

（ボイラー取扱作業主任者の選任）
第二十四条　事業者は、令第六条第四号 の作業については、次の各号に掲げる作業の区分に応じ、当該各号に掲げる者のうちから、ボイラー取扱作業主任者を選任しなければならない。
一　取り扱うボイラーの伝熱面積の合計が五百平方メートル以上の場合（貫流ボイラーのみを取り扱う場合を除く。）における当該ボイラーの取扱いの作業　特級ボイラー技士免許を受けた者（以下「特級ボイラー技士」という。）
二　取り扱うボイラーの伝熱面積の合計が二十五平方メートル以上五百平方メートル未満の場合（貫流ボイラーのみを取り扱う場合において、その伝熱面積の合計が五百平方メートル以上のときを含む。）における当該ボイラーの取扱いの作業　特級ボイラー技士又は一級ボイラー技士免許を受けた者（以下「一級ボイラー技士」という。）
三　取り扱うボイラーの伝熱面積の合計が二十五平方メートル未満の場合における当該ボイラーの取扱いの作業　特級ボイラー技士、一級ボイラー技士又は二級ボイラー技士免許を受けた者（以下「二級ボイラー技士」という。）
四　令第二十条第五号 イからニまでに掲げるボイラーのみを取り扱う場合における当該ボイラーの取扱いの作業　特級ボイラー技士、一級ボイラー技士、二級ボイラー技士

又はボイラー取扱技能講習を修了した者

2　前項第一号から第三号までの伝熱面積の合計は、次に定めるところにより算定するものとする。

一　貫流ボイラーについては、その伝熱面積に十分の一を乗じて得た値を当該貫流ボイラーの伝熱面積とすること。

二　火気以外の高温ガスを加熱に利用するボイラーについては、その伝熱面積に二分の一を乗じて得た値を当該ボイラーの伝熱面積とすること。

三　令第二十条第五号 イからニまでに掲げるボイラーについては、その伝熱面積を算入しないこと。

四　ボイラーに圧力、温度、水位又は燃焼の状態に係る異常があつた場合に当該ボイラーを安全に停止させることができる機能その他の機能を有する自動制御装置であつて厚生労働大臣の定めるものを備えたボイラーについては、当該ボイラー（当該ボイラーのうち、最大の伝熱面積を有するボイラーを除く。）の伝熱面積を算入しないことができること。

（関係告示：ボイラー及び圧力容器安全規則第二十四条第二項第四号の規定に基づき厚生労働大臣が定める自動制御装置（平成十六年厚生労働省告示第百三十一号）抄）

ボイラー及び圧力容器安全規則第二十四条第二項第四号の厚生労働大臣が定める自動制御装置は、同令第二十五条第二項の規定により厚生労働大臣が定める技術上の指針に適合していると労働基準監督署長が認定した自動制御装置又は次の各号のいずれにも該当する自動制御装置とする。

一～三　（略）

（関係通達：平成 28 年 9 月 30 日付け基発 0930 第 32 号）

第２

1　自動制御装置告示の一部改正

認定適合自動制御装置は、ボイラーの運転の状態に係る異常があった場合に、当該ボイラーを安全に停止できる高い信頼性を有し、改正前の自動制御装置告示で定める自動制御装置と同等以上の信頼性があることから、自動制御装置告示で定める自動制御装置の種類に認定適合自動制御装置を追加したこと。

（ボイラー取扱作業主任者の職務）

第二十五条　事業者は、ボイラー取扱作業主任者に次の事項を行なわせなければならない。

一　圧力、水位及び燃焼状態を監視すること。

二　急激な負荷の変動を与えないように努めること。

三　最高使用圧力をこえて圧力を上昇させないこと。

四　安全弁の機能の保持に努めること。

五　一日に一回以上水面測定装置の機能を点検すること。

六　適宜、吹出しを行ない、ボイラー水の濃縮を防ぐこと。

七　給水装置の機能の保持に努めること。

八　低水位燃焼しや断装置、火炎検出装置その他の自動制御装置を点検し、及び調整すること。

九　ボイラーについて異状を認めたときは、直ちに必要な措置を講じること。

十　排出されるばい煙の測定濃度及びボイラー取扱い中における異常の有無を記録すること。

2　ボイラーの運転の状態に係る異常があつた場合に当該ボイラーを安全に停止させることができる機能その他の機能を有する自動制御装置であつて厚生労働大臣の定める技術上の指針に適合していると所轄労働基準監督署長が認定したものを備えたボイラーについては、前項第五号の水面測定装置の機能の点検を三日に一回以上とすることができる。

3　前項の所轄労働基準監督署長の認定を受けようとする者は、適合自動制御ボイラー認定申請書（様式第十七号）に、当該申請に係る自動制御装置が前項の厚生労働大臣が定める技術上の指針に適合していることを厚生労働大臣の登録を受けた者が証明した書面を添えて、所轄労働基準監督署長に提出しなければならない。

（関係通達：平成 28 年 9 月 30 日付け基発 0930 第 32 号）

第２

２　認定適合自動制御装置に係る点検頻度の特例（ボイラー則第 25 条関係）

(1)　第 25 条第２項関係

ア　ボイラー則第 25 条第１項第５号の規定は、自動運転中に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）が多数発生したことに対する対策として、水面測定装置の故障を早期に発見して事故を防止する趣旨のものであるため、自動制御装置の信頼性が高くなることに応じ、点検の頻度を下げることが妥当であること。認定適合自動制御装置は、ボイラーの運転の状態に係る異常があった場合に、当該ボイラーを安全に停止できる高い信頼性（要求安全度水準）を有していると評価されるものであるため、認定適合自動制御装置を備えたボイラーについては、水面測定装置の機能の点検の頻度を、通常１日に１回以上のところ、３日に１回以上としたこと。

なお、「３日に１回以上」は、ボイラーに係る欧州規格（EN 12952、EN 12953等）が、機能安全に適合するボイラーの点検頻度を72時間以下とすることを推奨していることを踏まえたものであること。

イ　適合自動制御装置については、これを備えるボイラーごとに所轄労働基準監督署長の認定を行うこととし、認定の基準として、機能安全指針を定めたこと。

(2)　第25条第３項関係

ア　自動制御装置の設計及び機能が機能安全指針に適合していることをボイラーの設置者が証明することは困難であるため、専門知識を有する第三者機関である、厚生労働大臣の登録を受けた者（以下「登録適合性証明機関」という。）が適合性を証明した書面を所轄労働基準監督署長へ提出する認定の申請書に添付することを求めたこと。

イ　認定の対象となる適合自動制御装置には、新たに設置されるボイラーに備え付けられるもののみならず、すでに設置されているボイラーに新たに備え付けられるものも含まれること。

ウ　適合自動制御ボイラー認定書申請書（様式第17号）のボイラーの「種類」の欄には、ボイラーの種類（丸ボイラー（炉筒煙管ボイラー等)、水管ボイラー（貫流ボイラー等)、鋳鉄ボイラー又は特殊ボイラー（廃熱ボイラー等)）及び燃料・熱源の種類（油、ガス、バイオマス、廃熱等）を記載する必要があること。

エ　所轄労働基準監督署長の認定に当たっては、認定を受けようとする適合自動制御装置に係る適合証明書（登録省令様式第４号の４）の「用途及び仕様」及び「使用条件」が、適合自動制御ボイラー認定申請書に記載されているボイラーの種類等に合致している必要があること。

（関連通達：平成15年3月31日付け基発第0331001号（改正：平成28年9月30日付け基発0930第35号）抄）

別添３

認定適合自動制御装置を備えたボイラーの点検及び運転に関する基準

１　総則

(1) 目的

この基準は、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２項の規定により、ボイラーの運転の状態に係る異常があった場合に当該ボイラーを安全に停止させることができる機能その他の機能を有する自動制御装置であって、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。以下「指針」という。）に適合していると所轄労働基準監督署長が認定したもの（以下「認定適合自動制御装置」という。）を備えたボイラーについて、その運転上の安全を確保することを目的とする。

(2) 適用

ア　この基準は、認定適合自動制御装置を備えたボイラー（以下別添３において「ボイラー」という。）について適用する。

イ　ボイラーの点検及び運転を行う場合には、法令により定められたところによるほか、この基準によるものとすること。

(3) ボイラー取扱作業主任者の勤務場所等

ア　ボイラー取扱作業主任者は、ボイラーに異常が発生したことにより当該ボイラーが自動停止した後に、蒸気等の供給先に対する措置又はボイラーの再起動等を適切に実施するため、少なくとも１時間程度でボイラー設置場所に到達できる場所で勤務すること。

イ　認定適合自動制御装置は、ボイラーの運転の状態に係る異常があった場合に、要求される信頼性の水準（要求安全度水準）で当該ボイラーを安全に停止できる機能を有していると評価されているものであることから、ボイラー取扱作業主任者により、３日に１回以上、ボイラー設置場所でボイラーの状態が正常であるかどうかを点検することが求められること。

２　認定適合自動制御装置の要求安全機能及び要求安全度水準

認定適合自動制御装置の要求安全機能の特定及び要求安全度水準の決定については、指針で定める事項のほか、次に掲げる事項に留意すること。

(1) 指針の３－１によるリスクの解析においては、次に掲げる事項に留意すること。

ア　リスク解析の対象となる範囲は、ボイラー則第32条で規定するボイラー本体、燃焼装置、自動制御装置、附属装置及び附属品とすること。

イ　リスク解析の対象となる故障には、別添２の２（1）で定める重故障のほか、熱源の種類に応じ、燃料又は廃熱ガス等の供給に起因する故障を含むこと。

(2) 指針の３－２による要求安全機能及び安全関連システムの特定においては次に掲げる事項に留意すること。

ア　指針の３－１のリスク解析の結果により特定された全ての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。

イ　この際、別添２の２（1）及び（2）に定める機能等を参考とすること。

(3) 指針の３－３による要求安全度水準の決定において指針の別紙１による手法を使用する場合、次に掲げる事項に留意すること。

ア　負傷又は疾病の重篤度については、ボイラーの最高使用圧力と内容積の積の大きさ、ボイラーの破裂等の影響の及ぶ範囲にいる労働者及び一般公衆の人数を考慮すること。

イ　危険事象の回避可能性については、破裂等の発生を考慮して決定すること。

ウ　要求安全機能の作動要求確率については、容器の構造上の安全率、安全弁等の機械式の安全装置の信頼性等を考慮すること。

(4) その他、IEC61508、ISO13849 又はこれと同等以上の国際規格等に定める事項に留意すること。

３　ボイラーの機能等

ボイラーは、次に掲げる機能等を有するものであること。また、ボイラー設置者は、施錠等により、ボイラーの設置場所に関係者以外が立ち入れない措置を講ずること。

(1)　ボイラーの運転の状況に係る異常が発生したとき又はボイラーが自動停止したときに、表示灯の点灯等により異常の内容が識別できる表示機能を有する装置を設けること。この場合、異常が復旧するまで表示が維持されるものでなければならないこと。

(2)　認定適合自動制御装置の機能によって停止した場合、手動により当該装置がリセットされない限り再起動できないものとすること。

(3)　４に掲げる機能を有する情報端末に、次に掲げる事項を知らせる機能を有する装置を設けること。

ア ボイラーの運転の状況に係る異常が発生したこと

イ ボイラーが自動停止したこと

ウ １時間毎にボイラーが異常なく運転していること

エ 蒸気等の利用側の安全の確保のため、自動停止後に迅速な対応が必要な場合、上記アからウの機能を多重又は並列とすること。

(4)　ばい煙の排出状況を監視することができる機能を有する装置を設けること。

(5)　見やすい箇所に、認定適合自動制御装置を備えたボイラーである旨を掲示するとともに、当該ボイラーに係る適合自動制御ボイラー認定証を備え付けること。

４　情報端末の機能等

情報端末は、次に掲げる機能を有すること。

(1)　ボイラーの運転の状況に係る異常が発生したこと又はボイラーが自動停止したことを振動、警報音等により周囲に確実に知らせることができること。

(2)　異常が発生した又は自動停止したボイラーの設置場所及び固有識別番号等を特定できること。

(3)　異常が発生した場合にボイラーを情報端末から強制的に停止する機能を設ける場合、当該ボイラーが停止したことを情報端末に知らせる機能をボイラーに設けること。ただし、この機能は、ボイラーの運転を遠隔制御するためのものではないこと。

(4)　１時間ごとに、ボイラーが異常なく運転されていることを知らせる通信を受信できること。また、必要に応じ、当該通信が受信できなかった場合に、振動、警報音等によりその旨を周囲に確実に知らせる機能を有すること。

(5)　認定適合自動制御装置の機能を停止することができないこと。

(6)　認定適合自動制御装置の機能によりボイラーが停止した場合に、情報端末から当該ボイラーを再起動することができないこと。

5　取扱い

(1)　運転要領等の作成

ア　ボイラーの取扱い及び点検方法等を定めた運転要領等を作成し、それによって取扱い等を行うこと。

イ　運転要領等には、次に掲げる事項を含むこと。

①　ボイラー設置場所での点検の間隔（最大 72 時間）、運転制御及び安全関連機器の整備・点検の内容

②　水管理等のボイラーの管理に関する事項

③　その他運転管理に必要な事項

(2)　起動時の措置

ア　圧力が大気圧まで低下し、かつ温度が周辺の温度まで低下したボイラーを起動する前には、必要に応じて、次に掲げる装置が正常であるかどうかを確認すること。

① 燃焼安全装置

② 自動圧力制御装置

③ 自動水位制御装置

④ 警報装置

イ　起動前には、次に掲げる系統等が正常であるかどうかを確認すること。

① ボイラー付属品

② 燃料系統

③ 通風系統

④ 給水系統

⑤ 操作用動力源

ウ　起動は、ボイラーの設置場所で行うこと。

エ　起動後、ボイラーの圧力、水位、燃焼状態等が安定するまでボイラーの設置場所で圧力、水位、燃焼状態等を監視すること。

オ　定常停止は、ボイラーの設置場所で行うこと。

(3) 点検等

ア　起動後１時間以内、その後は 72 時間以内ごとに、ボイラー取扱作業主任者により、ボイラー設置場所でボイラーの状態が正常であるかどうか点検すること。

イ　認定適合自動制御装置の認定を受けた者の定める方法及び頻度で認定適合自動制御装置を点検すること。

ウ　煙道煙濃度を監視するために、排煙濃度計を使用する場合は、保護ガラスの清掃を行う等により機能を維持すること。

(4) 情報端末の管理

ア　ボイラー取扱作業主任者は、ボイラー運転中に常時、情報端末を携帯する又は情報端末を設置した場所に常駐すること。シフト制勤務とする場合は、交代の際に、情報端末を確実に引き継ぐこと。

イ　情報端末を携帯する者は、次に掲げる事項を実施すること。

①　情報端末の通信が無線による場合は、電波を受信可能な場所で勤務すること。

②　１時間ごとに、情報端末を確認し、ボイラーの運転状況を確認すること。ただし、情報端末が、１時間ごとのボイラーからの通信が受信できなかった場合に、振動、警報音等によりその旨を周囲に確実に知らせる機能を有する場合はこの限りでないこと。

③　適切な頻度で情報端末の電池の充電状況を確認し、必要な充電を行うこと。

＜登録適合性証明機関関係＞

○　労働安全衛生法及びこれに基づく命令に係る登録及び指定に関する省令（昭和四十七年労働省令第四十四号）　（抄）

（登録）
第一条の二の四十四の二　ボイラー及び圧力容器安全規則（昭和四十七年労働省令第三十三号。以下「ボイラー則」という。）第二十五条第三項の登録（以下この章において「登録」という。）は、同項の証明（以下この章において「適合性証明」という。）を行おうとする者の申請により行う。
2　登録の申請をしようとする者は、登録適合性証明機関登録申請書（様式第四号の二）に次の書類を添えて、厚生労働大臣に提出しなければならない。
一　申請者が法人である場合は、その定款又は寄附行為及び登記事項証明書
二　申請者が個人である場合は、その住民票の写し
三　申請者が次条各号の規定に該当しないことを説明した書面
四　次の事項を記載した書面
イ　申請者が法人である場合は、その役員の氏名及び略歴並びに社員、株主等の構成員（以下「構成員」という。）の氏名（構成員が法人である場合は、その法人の名称）
ロ　適合性証明を行う者（以下この章において「適合性証明員」という。）を指揮するとともに、適合性証明の業務を管理する者（以下この章において「実施管理者」という。）の氏名及び略歴
ハ　適合性証明員の氏名及び略歴
ニ　第一条の二の四十四の四第一項第一号の機械器具その他の設備の数、性能等及びその所有又は借入れの別
ホ　適合性証明の業務以外の業務を行つているときは、その業務の種類及び概要
ヘ　イからホまでに掲げるもののほか、第一条の二の四十四の四第一項各号の要件に適合していることを証する事項

（関係通達：平成 28 年 9 月 30 日付け基発 0930 第 32 号）
第２
３　登録適合性証明機関（登録省令第１章の６関係）
(1) 登録（第１条の２の 44 の２関係）
登録適合性証明機関は、ボイラーの自動制御装置が機能安全指針に適合していることを証明する書面（適合性証明書）を発行する機関として厚生労働大臣の登録を受けるものであるが、ボイラー以外の機械等の電子等制御の機能が機能安全指針に適合し

ていることを証明することを妨げるものではないこと。

（欠格条項）

第一条の二の四十四の三　次の各号のいずれかに該当する者は、登録を受けることができない。

一　法又は法に基づく命令の規定に違反して、罰金以上の刑に処せられ、その執行を終わり、又は執行を受けることがなくなつた日から起算して二年を経過しない者

二　第一条の二の四十四の十四の規定により登録を取り消され、その取消しの日から起算して二年を経過しない者

三　法人であつて、その業務を行う役員のうちに前二号のいずれかに該当する者があるもの

（登録基準）

第一条の二の四十四の四　厚生労働大臣は、第一条の二の四十四の二の規定により登録を申請した者（以下この項において「登録申請者」という。）が次に掲げる要件の全てに適合しているときは、その登録をしなければならない。

一　次に掲げる適合性証明を行うために必要な試験で使用する機械器具その他の設備を有し、これを用いて適合性証明を行うものであること。

イ　電気試験

ロ　放射能・放射線試験

ハ　機械・物理試験

ニ　化学試験

ホ　産業安全機械器具試験

二　実施管理者として、次のいずれかに該当する者を置いていること。

イ　学校教育法による大学又は高等専門学校において理科系統の正規の課程を修めて卒業した者（大学改革支援・学位授与機構により学士の学位を授与された者（当該課程を修めた者に限る。）を含む。次号において同じ。）であつて、十年以上機械等の運転の状態に係る異常があつた場合に当該機械等を安全に停止させることができる機能その他の機能を有する自動制御装置であつて厚生労働大臣の定める技術上の指針に適合するもの（以下「適合自動制御装置」という。）又は国際規格等に適合するこれと同等のもの（以下「適合自動制御装置等」という。）の研究、設計、製作若しくは検査又は適合性証明の業務に従事した経験を有するもの

ロ　学校教育法による高等学校において理科系統の正規の学科を修めて卒業した者であつて、十五年以上適合自動制御装置等の研究、設計、製作若しくは検査又は

適合性証明の業務に従事した経験を有するもの

ハ　イ又はロに掲げる者と同等以上の知識経験を有する者

三　適合性証明員が次のいずれかに該当する者であること。

イ　学校教育法による大学又は高等専門学校において理科系統の正規の課程を修めて卒業した者であつて、二年以上適合自動制御装置等の研究、設計、製作若しくは検査又は適合性証明の業務に従事した経験を有するもの

ロ　学校教育法による高等学校において理科系統の正規の学科を修めて卒業した者であつて、五年以上適合自動制御装置等の研究、設計、製作若しくは検査又は適合性証明の業務に従事した経験を有するもの

ハ　イ又はロに掲げる者と同等以上の知識経験を有する者

四　登録申請者が、機械等を製造し、又は輸入する者（以下この号において「製造者等」という。）に支配されているものとして、次のいずれにも該当するものでないこと。

イ　登録申請者が株式会社である場合にあつては、製造者等がその親法人（会社法（平成十七年法律第八十六号）第八百七十九条第一項に規定する親法人をいい、当該登録申請者が外国にある事務所において適合性証明の業務を行おうとする者である場合にあつては、外国における同法の親法人に相当するものを含む。）であること。

ロ　登録申請者の役員（持分会社（会社法第五百七十五条第一項に規定する持分会社をいう。第一条の十三第一項第六号ロにおいて同じ。）にあつては、業務を執行する社員）に占める製造者等の役員又は職員（過去二年間に当該製造者等の役員又は職員であつた者を含む。）の割合が二分の一を超えていること。

ハ　登録申請者（法人にあつては、その代表権を有する役員）が、製造者等の役員又は職員（過去二年間に当該製造者等の役員又は職員であつた者を含む。）であること。

2　登録は、登録適合性証明機関登録簿に次の事項を記載してするものとする。

一　登録年月日及び登録番号

二　氏名又は名称及び住所並びに法人にあつては、その代表者の氏名

三　事務所の名称及び所在地

（関係通達：平成 28 年 9 月 30 日付け基発 0930 第 32 号）

第２

3　登録適合性証明機関（登録省令第１章の６関係）

(2)　登録基準（第１条の２の 44 の４関係）

ア　第１号に規定する試験で使用する機械器具その他の設備は、登録適合性証明機関の事務所において所有することを原則とするが、国際標準化機構（ＩＳ

O）及び国際電気標準会議（ＩＥＣ）の規格 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機関が所有する設備を使用することも認められること。

イ　第２号及び第３号の「適合性証明」には、自己が所属する事業場で製造した機械等に対する適合性証明（いわゆる「自己適合宣言」）が含まれること。

ウ　第２号のハの「同等以上の知識経験を有する者」とは、次に掲げる者が該当するものであること。

①　学校教育法による大学又は高等専門学校において理科系統以外の正規の課程を修めて卒業した者（大学改革支援・学位授与機構により学士の学位を授与された者（当該課程を修めた者に限る。）を含む。以下「大学等卒業者」という。）で、13 年以上適合自動制御装置等の研究、設計、製作若しくは検査又は適合性証明の業務に従事した経験を有する者

②　学校教育法による高等学校又は中等教育学校において理科系統以外の正規の課程を修めて卒業した者（以下「高等学校等卒業者」という。）で、17 年以上適合自動制御装置等の研究、設計、製作若しくは検査又は適合性証明の業務に従事した経験を有する者

③　ＩＳＯ・ＩＥＣの規格 17065 に基づき認定された製品認証機関において、ＩＳＯの規格 13849 又はＩＥＣの規格 61508（これと同等の国際規格を含む。）に係る認証の業務に従事した経験を有する者（以下「認証業務経験者」という。）であって、認証の業務の実施を管理する業務に従事した経験を有する者

エ　第３号ハの「同等以上の知識経験を有する者」とは、次に掲げる者が該当するものであること。

①　大学等卒業者で、５年以上適合自動制御装置等の研究、設計、製作若しくは検査又は適合性証明の業務に従事した経験を有する者

②　高等学校等卒業者で、７年以上適合自動制御装置等の研究、設計、製作若しくは検査又は適合性証明の業務に従事した経験を有する者

③　認証業務経験者

（登録の更新）

第一条の二の四十四の五　登録は、五年ごとにその更新を受けなければ、その期間の経過によつて、その効力を失う。

２　前三条の規定は、前項の登録の更新について準用する。

（実施義務）

第一条の二の四十四の六　登録を受けた者（以下この章において「登録適合性証明機関」という。）は、適合性証明申請書（様式第四号の三）の提出を受けて適合性証明を行うことを求められたときは、正当な理由がある場合を除き、遅滞なく、適合性証明を行わなければならない。

２　登録適合性証明機関は、適合性証明を行うときは、適合性証明員にこれを実施させなければならない。

３　登録適合性証明機関は、厚生労働大臣が定める技術上の指針に従つて適合性証明の実施方法を定め、これに従つて公正に適合性証明の業務を行わなければならない。

４　登録適合性証明機関は、適合性証明を行つた後遅滞なく、適合性証明を行うことを求めた者に対し、適合性証明を行つたことを証する書面（様式第四号の四。第一条の二の四十四の八第一項第五号及び第一条の二の四十四の十五第一項第六号において「適合証明書」という。）を交付しなければならない。

５　登録適合性証明機関は、毎事業年度において六月以内に一回、その期間内に行つた適合性証明の結果について、適合性証明実施結果報告書（様式第四号の五）を、厚生労働大臣に提出しなければならない。

（関係通達：平成 28 年９月 30 日付け基発 0930 第 32 号）

第２

３　登録適合性証明機関（登録省令第１章の６関係）

(3)　実施義務（第１条の２の 44 の６関係）

ア　第１項の適合性証明は、電子等制御に使用される部品、電子等制御に関連する部品を組み合わせた自動制御装置又は自動制御装置を備えた機械等のいずれに対しても実施可能とすること。

イ　第３項の「実施方法」には、原則として以下の事項が含まれること。

①　申請者からの安全確保に関する構想の聴取等

②　機械等による労働者の就業に係る危険性又は有害性の特定、要求安全機能の特定及び安全関連システムの要求安全度水準の決定等の妥当性の評価等

③　各種試験・検査等の実施、機械等の製造管理の体制等の監査及び報告書作成等

④　②と③の結果の整合性の確認及び適合証明書の発行等

ウ　第４項の適合証明申請書（様式第４号の３）及び適合証明書（第４号の４）の「使用条件」の欄には、ボイラーの自動制御装置の場合にあっては、当該自動制御装置の要求安全機能の特定及び要求安全度水準の決定の前提となっている、ボイラーの種類（丸ボイラー（炉筒煙管ボイラー等）、水管ボイラー（貫流ボイラー等）、鋳鉄ボイラー又は特殊ボイラー（廃熱ボイラー等））、燃料・熱源

の種類（油、ガス、バイオマス、廃熱等）、ボイラーの設置場所・条件、自動制御装置の点検方法・頻度等を記載する必要があること。

（変更の届出）
第一条の二の四十四の七　登録適合性証明機関は、第一条の二の四十四の四第二項第二号又は第三号の事項を変更しようとするときは、変更しようとする日の二週間前までに、登録適合性証明機関登録事項変更届出書（様式第一号の五）を厚生労働大臣に届け出なければならない。

（業務規程）
第一条の二の四十四の八　登録適合性証明機関は、適合性証明の業務の開始の日の二週間前までに、次の事項を記載した適合性証明の業務に関する規程を定め、業務規程届出書（様式第二号）に当該規程を添えて、厚生労働大臣に届け出なければならない。これを変更しようとするときも、同様とする。
一　適合性証明の実施方法
二　適合性証明に関する料金
三　前号の料金の収納の方法に関する事項
四　適合性証明の業務を行う時間及び休日に関する事項
五　適合証明書の発行に関する事項
六　適合性証明の業務に関する帳簿及び書類の保存に関する事項
七　第一条の二の四十四の十第二項第二号及び第四号の請求に係る費用に関する事項
八　前各号に掲げるもののほか、適合性証明の業務に関し必要な事項
２　登録適合性証明機関は、前項後段の規定により変更の届出をしようとするときは、業務規程変更届出書（様式第三号）を厚生労働大臣に提出しなければならない。

（業務の休廃止）
第一条の二の四十四の九　登録適合性証明機関は、適合性証明の業務の全部又は一部を休止し、又は廃止しようとするときは、あらかじめ、適合性証明業務休廃止届出書（様式第四号）を厚生労働大臣に届け出なければならない。

（財務諸表等の備付け及び閲覧等）

第一条の二の四十四の十　登録適合性証明機関は、毎事業年度経過後三月以内に、その事業年度の財産目録、貸借対照表及び損益計算書又は収支計算書並びに事業報告書（その作成に代えて電磁的記録の作成がされている場合における当該電磁的記録を含む。次項において「財務諸表等」という。）を作成し、五年間事務所に備えて置かなければならない。２　適合性証明の申込みをしようとする者その他の利害関係人は、登録適合性証明機関の業務時間内は、いつでも、次に掲げる請求をすることができる。ただし、第二号又は第四号の請求をするには、登録適合性証明機関の定めた費用を支払わなければならない。

一　財務諸表等が書面をもつて作成されているときは、当該書面の閲覧又は謄写の請求

二　前号の書面の謄本又は抄本の請求

三　財務諸表等が電磁的記録をもつて作成されているときは、当該電磁的記録に記録された事項を紙面又は出力装置の映像面に表示する方法により表示したものの閲覧又は謄写の請求

四　前号の電磁的記録に記録された事項を電磁的方法であつて次のいずれかのものにより提供することの請求又は当該事項を記載した書面の交付の請求

イ　送信者の使用に係る電子計算機と受信者の使用に係る電子計算機とを電気通信回線で接続した電子情報処理組織を使用する方法であつて、当該電気通信回線を通じて情報が送信され、受信者の使用に係る電子計算機に備えられたファイルに当該情報が記録されるもの

ロ　磁気ディスクその他これに準ずる方法により一定の情報を確実に記録しておくことができる物をもつて調製するファイルに情報を記録したものを交付する方法

３　登録適合性証明機関は、毎事業年度経過後三月以内に、第一項の規定により作成した損益計算書又は収支計算書及び事業報告書を厚生労働大臣に提出しなければならない。

（適合性証明員の選任等の届出）

第一条の二の四十四の十一　登録適合性証明機関は、適合性証明員を選任したときは、遅滞なく、適合性証明員選任届出書（様式第五号）に選任した者の経歴を記載した書面を添えて、厚生労働大臣に提出しなければならない。

２　登録適合性証明機関は、適合性証明員を解任したときは、遅滞なく、適合性証明員解任届出書（様式第六号）を厚生労働大臣に提出しなければならない。

（適合命令）

第一条の二の四十四の十二　厚生労働大臣は、登録適合性証明機関が第一条の二の四十四の四第一項各号のいずれかに適合しなくなつたと認めるときは、その登録適合性証明機関に対し、これらの規定に適合するため必要な措置を採るべきことを命ずることができる。

（改善命令）

第一条の二の四十四の十三　厚生労働大臣は、登録適合性証明機関が第一条の二の四十四の六第一項から第三項までの規定に違反していると認めるときは、その登録適合性証明機関に対し、適合性証明を行うべきこと又は適合性証明の実施方法その他の業務の改善に関し必要な措置を採るべきことを命ずることができる。

（登録の取消し等）

第一条の二の四十四の十四　厚生労働大臣は、登録適合性証明機関が次の各号のいずれかに該当するときは、その登録を取り消し、又は六月を超えない範囲内で期間を定めて適合性証明の業務の全部若しくは一部の停止を命ずることができる。

一　第一条の二の四十四の三第一号又は第三号に該当するに至つたとき。

二　第一条の二の四十四の六から第一条の二の四十四の九まで、第一条の二の四十四の十第一項若しくは第三項又は次条第一項の規定に違反したとき。

三　正当な理由がないのに第一条の二の四十四の十第二項各号の規定による請求を拒んだとき。

四　第一条の二の四十四の十一の規定による提出をせず、又は虚偽の提出をしたとき。

五　前二条の規定による命令に違反したとき。

六　不正の手段により登録を受けたとき。

（帳簿）

第一条の二の四十四の十五　登録適合性証明機関は、適合性証明を行つたときは、次の事項を記載した帳簿を備え、これを記載の日から一年間保存しなければならない。

一　適合性証明を行つた適合自動制御装置を所有する者の氏名又は名称及び住所

二　適合性証明を行つた適合自動制御装置の型式及び製造番号

三　適合性証明を行つた年月日

四　適合性証明を行つた適合性証明員の氏名

五　適合性証明の結果

六　適合証明書の番号

七　その他適合性証明に関し必要な事項

２　登録適合性証明機関は、適合性証明の業務を廃止した場合（登録を取り消された場合及び登録がその効力を失つた場合を含む。）には、前項の帳簿を厚生労働大臣に引き渡さなければならない。

（公示）

第一条の二の四十四の十六　厚生労働大臣は、次の表の上欄に掲げる場合には、同表の下欄に掲げる事項を官報で告示しなければならない。

＜表略＞

適合自動制御装置の認定実施要領

（平成 29 年 5 月 8 日付け基発 0508 第 2 号）

第１　趣旨等

１　趣旨

本実施要領は、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２項の規定に基づく所轄労働基準監督署長による自動制御装置の認定（以下単に「認定」という。）に係る基準、手続き等を定めるものである。

認定に当たっては、本要領に定めるところによるほか、「ボイラー及び圧力容器安全規則及び労働安全衛生法及びこれに基づく命令に係る登録及び指定に関する省令の一部改正（指定外国検査機関関係を除く。）等について」（平成 28 年９月 30 日付け基発 0930 第 32 号）に定めるところによる。

２　認定の対象

認定の対象となる自動制御装置は、次に掲げる条件の全てを満たすものとする。なお、認定の対象には、新たに設置するボイラーに備え付けられる自動制御装置のみならず、すでに設置されているボイラーを改修して新たに備え付けられるものも含まれる。

(1)　ボイラーの運転の状態に係る異常があった場合に当該ボイラーを安全に停止させることができる機能その他の機能を有する自動制御装置であって、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。以下「機能安全指針」という。）に適合しているもの（以下「適合自動制御装置」という。）。

(2)　適合自動制御装置が機能安全指針に適合していることを厚生労働大臣の登録を受けた者（以下「登録適合性証明機関」という。）が証明した書面（以下「適合証明書」という。）が添付されているもの。

３　認定の申請に必要な書類

認定の申請に当たっては、次に掲げる書類を所轄労働基準監督署長に提出させること。なお、新たに設置するボイラーに係る認定の申請に当たっては、ボイラー則第 10 条に定めるボイラー設置届（ボイラー則様式第 11 号）とその添付書類を同時に提出させるものとする。

(1)　適合自動制御ボイラー認定申請書（ボイラー則様式第 17 号）

(2)　適合証明書（労働安全衛生法及びこれに基づく命令に係る登録及び指定に関する省令（昭和 47 年労働省令第 44 号。以下「登録省令」という。）様式第４号の４）

(3)　適合自動制御ボイラー認定申請書及び適合証明書の内容を補足する書面（必要な場合のみ。）

４　認定の基準

(1)　認定を受けようとする適合自動制御装置に係る適合証明書の期限が設けられている場合、当該適合証明書が当該期限内であること。

(2)　認定を受けようとする適合自動制御装置を備えるボイラーに係る検査証が有効期間内であること。

(3)　認定を受けようとする適合自動制御装置を備えるボイラーの仕様や使用条件等が、当該適合自動制御装置により制御可能なボイラーの仕様や使用条件等の範囲内に含まれること。

第２　認定の審査

１　適合自動制御ボイラー認定申請書の審査基準

(1)　適合自動制御ボイラー認定申請書について、次に掲げる事項が当該申請に係るボイラーのボイラー設置届又はボイラー台帳（以下「設置届等」という。）に記載されている内容と合致するかどうか確認すること。

ア　事業場の名称及び所在地

イ　製造許可番号及び許可年月日

ウ　検査証番号

エ　種類

オ　伝熱面積又は内容積

カ　検査証の有効期間の満了日

(2)　適合自動制御ボイラー認定申請書について、適合証明書の証明書番号及び証明年月日の記載が、添付されている適合証明書と一致することを確認すること。

２　適合証明書の審査基準

添付された適合証明書について、以下の事項を審査すること。

(1)　適合証明書が登録適合性証明機関によって発行されたものであること。

(2)　証明書番号及び証明年月日が記載されていること。

(3)　製造者の名称及び住所が記載されていること。

(4)　品名及び型式欄に、適合性証明の対象となる適合自動制御装置を特定できる品名及び型式が記載されていること。

(5)　適用した規格等の欄に、適合性証明に当たって適用した日本工業規格又は国際規格等の名称が記載されていること。ボイラーの場合、機能安全に関する基本的な規格は、国際電気標準会議(IEC)規格 61508（日本工業(JIS)規格 C0508）であるが、国際標準化機構(ISO)規格 13849（日本工業(JIS)規格 B9706）も適用可能であることから、最低限、この２つの規格のいずれかが含まれていることを確認すること。その他の関連する国際規格としては、機械安全に関する ISO 規格（ISO 12100 等)、工業炉及び関連設備に関する ISO 規格（ISO 13577 等)、ボイラーに関する欧州規格（EN 50156、EN 12952、EN 12953 等）があるが、これらの規格への適合については登録適合性証明機関に委ねられること。

(6)　用途及び仕様欄に、適合自動制御装置の仕様等及び当該適合自動制御装置によって制御することが可能なボイラーの仕様等について、次に掲げる事項が記載されているか、これらを明らかにする書面が添付されていること。

ア　適合自動制御装置が適合する安全度水準（JIS C0508）若しくはカテゴリー及びパフォーマンスレベル（JIS B9705）が記載され、当該安全度水準等を機能安全指針に適合する方法で決定した旨が記載されていること。なお、ボイラーの自動制御装置については、安全度水準(SIL)によることが一般的であり、安全度水準(SIL)には、１から４までの段階があること。

イ　燃焼方式及び燃焼装置

バーナー燃焼、ストーカ燃焼等の別、バス専焼バーナー等

ウ　給水制御方式

比例制御方式等の制御方式

エ　自動制御方式

全自動制御、燃焼制御等の別、比例制御等の制御方式

オ　自動停止の機能

①　センサー（温度計、圧力計、火炎検出装置等）

②　論理部（プログラマブル・ロジック・コントロール（PLC)、リレー回路等）

③　アクチュエーター（燃料遮断弁、給水制御弁、圧力調整弁等）

④　①～③の組み合わせによる自動停止機能の概要

(7)　使用条件の欄に、当該適合自動制御装置によって制御されることが可能なボイラーの使用条件等について、次に掲げる事項が記載されているか、それらを明らかにする書面が添付されていること。なお、各事項は特定のボイラーに限定されている必要はなく、複数のボイラーに対応可能であっても差し支えないこと（例：伝熱面積は５から 10 平方メートルの範囲、複数の燃料に対応できる等)。

ア　ボイラーの種類

丸ボイラー（炉筒煙管ボイラー等)、水管ボイラー（貫流ボイラー等)、鋳鉄ボイラー又は特殊ボイラー（廃熱ボイラー等）等

イ　燃料・熱源の種類

灯油、重油、天然ガス、都市ガス、バイオマス、廃熱等

ウ　伝熱面積、定格蒸発量、蒸気温度等

エ　最高使用圧力、使用温度範囲

オ　使用電圧・電気容量

カ　ボイラー運転条件等

①　必要なボイラーの取扱資格（ボイラー技士の級別等）

②　１日あたりの運転時間等の運転条件

キ　ボイラー設置場所や設置環境

①　屋内・屋外の別

②　ボイラー設置場所でのボイラー取扱者の滞在時間

③　ボイラーの爆発等により影響を受ける範囲に常駐する労働者の人数等（適合自動制御装置の要求安全水準を決定する際、通常、ボイラーの爆発等により複数の作業者が被災することを前提とするが、仮に、被災労働者の人数が最大１人であることを前提としている場合、その人数を担保するための設置条件等（例：ボイラー設置場所の周囲に作業場所等がなく、爆発の影響を受ける範囲内にボイラー運転者以外の作業者等が立ち入らないこと等）について明示されていること。）

ク　保守点検に関する事項

①　ボイラーに係る保守点検の内容及び頻度（日常点検、定期自主検査、性能検査）

②　適合自動制御装置の点検項目、方法、頻度等

(8)　適合証明書の期限の末日欄に年月日の記載がある場合、労働基準監督署長が交付する様式第１号で定める適合自動制御ボイラー認定書（以下「認定書」という。）の認定日が適合証明書の期限の末日を過ぎないこと。

３　適合証明書と設置届等に記載されている事項の比較に係る審査基準

(1)　適合証明書の用途及び仕様欄に記載されている事項と、設置届等に記載された事項を比較し、表１に掲げる審査基準により、審査すること。

(2)　適合証明書の使用条件欄に記載されている事項と、設置届等に記載された事項を比較し、表２に掲げる審査基準により、審査すること。

第３　認定書の交付等

１　認定書の交付等

(1)　新規設置のボイラーに係る認定

新規設置のボイラーに係る認定については、当該ボイラーがボイラー則第59条の落成検査に合格し、検査証を交付する際に、認定書を併せて交付すること。

(2)　既設置のボイラーに係る認定

既設置のボイラーに係る認定に当たっては、以下の事項に留意すること。

ア　既設置のボイラーについて認定を申請するためには、既設置のボイラーの自動制御装置の交換等を行う必要があるが、これに伴い、燃焼装置や附属設備等ボイラー則第41条各号に掲げる部分又は設備についての変更を伴う場合は、ボイラー則第41条に基づく変更届の提出が必要であること。

イ　ボイラー則第41条各号に掲げる部分又は設備を変更しない場合であっても、ボイラー設置届又はボイラー明細書に記載された事項に変更が生じる場合、認定の申請時に、ボイラー設置届の変更事項について、任意様式（別紙ひな形参照）により報告を求めること。

ウ　認定の審査に当たっては、ア又はイにより提出又は報告された変更後のボイラーの仕様等に基づいて審査を行うこと。

エ　変更届が提出された場合には、ボイラー則第42条の変更検査に合格し、検査証の裏書をする際に、併せて認定書を交付すること。

(3)　認定後の処理

認定書を交付後、次に掲げる事項を実施すること。

ア　当該ボイラーに係るボイラー台帳の摘要欄に、認定書の交付年月日及び認定番号を記載すること。

イ　当面の間、労働局を通じて本省安全課あてに、認定書、認定申請書及び適合証明書の写しを送付すること。

2　変更の認定

(1)　変更の範囲

認定を受けた者が、次に該当する場合は、所轄労働基準監督署長に認定の変更を申請させること。

ア　認定を受けた適合自動制御装置を変更する場合

イ　認定を受けた適合自動制御装置を備えたボイラーについて、適合証明書の用途及び仕様欄又は使用条件の欄に記載されている仕様等に係る当該ボイラーの部分又は設備を変更しようとする場合

(2)　変更の認定の申請及び審査

変更の認定の申請及び審査は、新規の申請に係る事項を準用すること。

3　認定の廃止

認定を受けた者が、認定を廃止しようとするときには、所轄労働基準監督署長に対し、廃止申出書（様式任意）に認定書を添えて提出させること。

4　認定の取消し等

(1)　取消事由等

所轄労働基準監督署長は、認定を受けた者等について、次に掲げる事由のいずれかに該当するに至った場合は、認定を取り消すことができること。なお、当面の間、認定の取消しを行おうとする場合は、当該事案の概要、処分事由等について、あらかじめ労働局を通じて本省に協議すること。

ア　認定を受けた適合自動制御装置の機能が損なわれ、適合証明書の用途及び仕様欄又は使用条件欄に記載された仕様等に適合しなくなったとき。

イ　認定を受けた適合自動制御装置を備えたボイラーの検査証の有効期間が更新されなかったとき又は当該ボイラーが廃止されたとき。

ウ　認定を受けた適合自動制御装置を備えたボイラーの燃焼装置等が変更され、適合証明書の用途及び仕様欄又は使用条件欄に記載された仕様等に合致しなくなったとき。

エ　虚偽又は不正の手段で認定を受けたとき。

(2)　取消処分等に当たっての留意事項

取消処分又は不認定処分を行うに当たっては、行政手続法（平成５年法律第88号）、厚生労働省聴聞手続規則（平成12年厚生省・労働省令第２号）、「行政手続法の施行に伴う聴聞及び弁明の機会の付与の手続について」（平成６年９月30日付け基発第611号・婦発第272号）、「行政手続法等の施行について」（平成６年９月30日付け基発第612号）に留意し、聴聞、処分通知等を適切に行うとともに、処分通知に当たっては、行政不服審査法（平成26年法律第68号）及び行政事件訴訟法（昭和37年法律第139号）の規定による教示を行うこと。

表１　適合証明書の「用途及び仕様」欄の審査内容

適合証明書に記載すべき項目（例）	適合証明書に記載すべき内容（例）	設置届等の記載項目	設置届等の記載内容（例）	審査基準
安全度水準又はパフォーマンスレベル	安全度水準（SIL）:2 パフォーマンスレベル（PL）:d			適合証明書に安全度水準又はパフォーマンスレベルが記載されていること。また、当該安全度水準等が機能安全指針に適合する方法により決定された旨が記載されていること。
燃焼方式	ガス専焼バーナー	燃焼方式	手だき、ストーカ燃焼、バーナー燃焼	適合証明書の燃焼方式が設置届等の燃焼方式と一致すること。
給水制御方式	比例制御等	給水装置	種類、給水能力、数	適合証明書に制御方式が記載されていること。
自動制御方式	燃焼制御（比例制御等）	自動制御方式	全自動、燃焼系、その他	適合証明書の自動制御方式が設置届等の自動制御方式と一致すること。
自動停止の機能	センサー（温度計、圧力計、火炎検出装置等）、ロジック（PLC、リレー回路等）、アクチュエーター（燃料遮断装置、水位調整装置、圧力調整装置等）の組み合わせ	自動制御装置の概要	低水位遮断装置、燃焼安全装置、低水位警報装置、その他	適合証明書に記載されている自動停止機能が設置届等に記載されている自動制御装置を含んでいること。

表２　適合証明書の「使用条件」欄の審査内容

適合証明書に記載すべき項目（例）	適合証明書に記載すべき内容（例）	設置届等の記載項目	設置届等の記載内容（例）	審査基準
ボイラーの種類	炉筒煙管式蒸気ボイラー	種類		適合証明書に記載されているボイラーの種類に、設置届等の種類が含まれること。
燃料・熱源の種類、供給能力	灯油、重油、天然ガス、バイオマス、廃熱等	燃料	石油、微粉炭、重油、ガス、その他	適合証明書に記載されている燃料・熱源の種類に、設置届等の燃料の種類が含まれること。
伝熱面積 定格蒸発量 蒸気温度	●～●m^3 ●～●kg/h 飽和蒸気	伝熱面積 最大蒸発量		適合証明書の伝熱面積の範囲に、設置届等の伝熱面積が含まれること。
最高使用圧力 使用温度範囲	●～●MPa ●℃～●℃	最高使用圧力		適合証明書の最高使用圧力の範囲に設置届等の最高使用圧力が含まれること。
ボイラー設置場所・条件	ボイラー設置場所でのボイラー取扱者の滞在時間（12時間以下）、ボイラーの爆発等で影響を受ける周辺労働者の人数（●人程度）等	ボイラー室の位置	一階、地階、二階、その他	・実際の運用でのボイラー取扱者のボイラー室の滞在時間が、適合証明書の滞在時間の上限を超えないことを確認すること。 ・適合証明書の周辺労働者の人数が０人となっている場合、設置場所の周囲に労働者が常駐する作業場がないこ
		ボイラー施設の構造	木造・鉄骨等、鉄筋コンクリート造、その他	

				とを確認すること。（証明書の周辺労働者の人数が１人以上となっている場合は特段の審査事項なし。）
使用電圧・電気容量	AC●～●V, ●～●kw			適合証明書に使用電圧・電気容量が記載されていること。
自動制御装置の点検方法・頻度等	取扱説明書による。			適合証明書に自動制御装置の点検方法及び頻度が記載されていること。

様式第１号

適合自動制御ボイラー認定書

認定年月日		認定番号	
事業場の名称			
事業場の所在地			
認定された適合自動制御装置に係る適合証明書	適合性証明機関名		
	証明書番号		
	証明年月日		
当該適合自動制御装置を備えたボイラー	製造許可番号及び許可年月日		
	検査証番号		
	種類		
	伝熱面積又は内容積		

年　　月　　日

○○　労働基準監督署長

別紙

（所轄労働基準監督署長への設置届等の変更事項の報告のひな形）

○○労働基準監督署長　殿

事業者名

ボイラー設置届等記載事項の変更について

標記につきまして、下記のとおり報告します。

記

1　変更の対象となるボイラー
(1) 事業場の名称
(2) 事業場の所在地
(3) 製造許可番号
(4) 刻印番号
(5) 検査証番号
(6) 検査証の有効期限の満了日
(7) 変更前のボイラー設置届及びボイラー明細書の提出年月日※

2　ボイラー設置届又はボイラー明細書の変更事項

変更後	変更前	変更理由
（例） ・自動制御装置の概要 低水位警報装置及び燃料遮断装置 失火警報装置及び燃料遮断装置 圧力警報装置及び燃料遮断装置	（例） ・自動制御装置の概要 低水位警報装置 燃焼安全装置	（例） 適合自動制御装置の導入による。

3　変更年月日

※　可能であれば、写しを添付させること。

附録 B　機能安全の関連規格

本テキスト及びマニュアルで参照すべき規格一覧を表 B-1 に示す。表 2-1 の JIS C 0508 シリーズは、表 B-1 から除いている。また、規格番号の後に* 印をつけている規格は、翻訳版があることを示している。

表 B-1　機械安全規格体系におけるタイプ A 及び B 規格抜粋

JIS	ISO/IEC	標題または規格名称
タイプA規格およびA規格関連TR		
JIS B 9700	ISO 12100	機械類の安全性－設計のための一般原則－リスクアセスメント及びリスク低減
－	ISO/TR 22100-1	機械類の安全性－ISO 12100との関連－第1部：ISO 12100はどのようにタイプB及びタイプC規格に関連付いているか
－	ISO/TR 22100-2	機械類の安全性－ISO 12100との関連－第2部：ISO 12100はどのようにISO13849-1に関連付いているか
－	ISO/TR 22100-3	機械類の安全性－機械類の安全性－ISO 12100との関連－第3部：安全性規格への人間工学の導入
－	ISO/TR 14121-2*	機械類の安全性－リスクアセスメント－第2部：実践ガイド及び方法の例
タイプB規格：一般		
－	ISO 11161*	機械類の安全性－統合生産システム－基本的要求事項
JIS B 9705-1	ISO 13849-1	機械類の安全性－制御システムの安全関連部－ 第1部：設計のための一般原則
JIS B 9705-2 (2018年発行予定)	ISO 13849-2*	機械類の安全性－制御システムの安全関連部－ 第2部：妥当性確認
－	ISO/TR 23849	機械の安全関連制御システムの設計におけるISO 13849-1及びIEC 62061の適用の手引
JIS B 9703	ISO 13850	機械類の安全性－非常停止－設計原則
JIS B 9712	ISO 13851	機械類の安全性－両手操作制御装置－機能的側面及び設計原則
JIS B 9711	ISO 13854	機械類の安全性－人体が押しつぶされることを回避するための最小隙間
JIS B 9715	ISO 13855	機械類の安全性－人体の接近速度に基づく安全防護物の位置決め
JIS B 9717-1	ISO 13856-1	機械類の安全性－圧力検知保護装置－第1部：圧力検知マット及び圧力検知フロアの設計及び試験のための一般原則
－	ISO 13856-2	機械類の安全性－圧力検知保護装置－第2部：圧力検知エッジ及びバー設計及び試験のための一般原則
－	ISO 13856-3	機械類の安全性－圧力検知保護装置－第3部：圧力検知バンパ，プレート，ワイヤ及び類似の装置の設計及び試験のための一般原則
JIS B 9718	ISO 13857	機械類の安全性－危険区域に上肢及び下肢が到達することを防止するための安全距離
JIS B 9714	ISO 14118	機械類の安全性－予期しない起動の防止
JIS B 9710	ISO 14119	機械類の安全性－ガードと共同するインターロック装置－設計及び選択のための原則

JIS B 9716	ISO 14120	機械類の安全性－ガードー固定式及び可動式ガードの設計及び製作のための一般要求事項
JIS B 9713-1	ISO 14122-1	機械類の安全性－機械類への常設接近手段－第 1 部：高低差のある 2 箇所間の昇降設備の選択
JIS B 9713-2	ISO 14122-2	機械類の安全性－機械類への常設接近手段－第 2 部：作業用プラットフォーム及び通路
JIS B 9713-3	ISO 14122-3	機械類の安全性－機械類への常設接近手段－第 3 部：階段，段ばしご及び防護さく
JIS B 9713-4	ISO/FDIS14122?4	機械類の安全性－機械類への常設接近手段－第 4 部：固定はしご
JIS B 9709-1	ISO 14123-1	機械類の安全性－機械類から放出される危険物質による健康へのリスクの低減－第 1 部：機械類製造者のための原則及び仕様
JIS B 9709-2	ISO 14123-2	機械類の安全性－機械類から放出される危険物質による健康へのリスクの低減－第 2 部：検証手順に関する方法論
(JIS B 9650-2)	ISO 14159*	機械類の安全性－機械設計の衛生要求事項 注：JIS B 9650-2 と ISO14159 の関係については，表 5-3 の注参照。
－	ISO/TR 18569*	機械類の安全性－機械安全規格の理解及び使用のためのガイドライン
－	ISO 19353	機械類の安全性－防火及び保護
－	ISO 21469	機械類の安全性－製品との偶発的接触を伴う潤滑剤－衛生要求事項
－	ISO 29042-1	機械類の安全性－大気危険物質の放出の評価－第 1 部：試験方法の選択
－	ISO 29042-2	機械類の安全性－大気危険物質の放出の評価－第 2 部：特定の汚染物質の放出率－ガスの追跡方法
－	ISO 29042-3	機械類の安全性－大気危険物質の放出の評価－第 3 部：特定の汚染物質の放出率－実際の汚染物質を使用する台上試験
－	ISO 29042-4	機械類の安全性－大気危険物質の放出の評価－第 4 部：排気系統の補足効率－トレーサ試験
－	ISO 29042-5	機械類の安全性－浮遊危険物質の放出の評価－第 5 部：非ダクト式排気口をもつ空気清浄システムの大量分離効率の測定のためのテストベンチ法
－	ISO 29042-6	機械類の安全性－大気危険物質の放出の評価－第 6 部：質量による分離効率，非導管排出口
－	ISO 29042-7	機械類の安全性－大気危険物質の放出の評価－第 7 部：質量による分離効率，導管排出口
－	ISO 29042-8	機械類の安全性－大気危険物質の放出の評価－第 8 部：汚染物質濃度バラメタ，試験ベンチ法
－	ISO 29042-9	機械類の安全性－大気危険物質の放出の評価－第 9 部：汚染物質濃度バラメタ，室内法

タイプ B 規格：電気/制御		
JIS B 9960-1	IEC 60204-1	機械類の安全性－機械の電気装置－第 1 部：一般要求事項
JIS B 9960-11	IEC 60204-11	機械類の安全性－機械の電気装置－第 11 部：交流 1000V 又は直流 1500V を超え 36kV 以下の高電圧装置に対する要求事項
JIS B 9960-31	IEC 60204-31	機械類の安全性－機械の電気装置－第 31 部：縫製機械，縫製ユニット及び縫製システムの安全性と EMC に対する要求事項
JIS B 9960-32	IEC 60204-32	機械類の安全性－機械の電気装置－第 32 部：巻上機械に対する要求事項
JIS B 9960-33	IEC 60204-33	機械類の安全性－機械の電気装置－第 33 部：半導体製造装置に対する要求事項
JIS C 0920	IEC 60529	エンクロージャによる国際保護等級(IP コード)
JIS C 2812	IEC 60715	低電圧開閉装置及び制御装置の寸法。開閉装置及び制御装置設備の電気装置の機械的支持のための標準レール取付
JIS C 8201-1	IEC 60947-1	低電圧開閉装置及び制御装置－ 第 1 部：一般規則
JIS C 8201-2-1	IEC 60947-2	低圧開閉装置及び制御装置－ 第 2-1 部：回路遮断器（配線用遮断器及びその他の遮断器）
JIS C 8201-2-2	IEC 60947-2	低圧開閉装置及び制御装置－ 第 2-2 部：漏電遮断器
JIS C 8201-3	IEC 60947-3	低圧開閉装置及び制御装置－ 第 3 部：開閉器，断路器，断路用開閉器及びヒューズ組みユニット
JIS C 8201-4-1	IEC 60947-4-1	低圧開閉装置及び制御装置－ 第 4-1 部：接触器及びモータスタータ：電気機械式接触器及びモータスタータ
JIS C 8201-4-2	IEC 60947-4-2	低圧開閉装置及び制御装置－ 第 4-2 部：接触器及びモータスタータ：交流半導体モータ制御器及びスタータ
JIS C 8201-4-3	IEC 60947-4-3	低電圧開閉装置及び制御装置－ 第 4-3 部：接触器及びモータスタータ：非モータ負荷用交流半導体制御器及び接触器
JIS C 8201-5-1	IEC 60947-5-1	低電圧開閉装置及び制御装置－ 第 5 部：制御回路機器及び開閉素子－第 1 節：電気機械式制御回路機器
JIS C 8201-5-2	IEC 60947-5-2	低電圧開閉装置及び制御装置－ 第 5 部：制御回路機器及び開閉素子－第 2 節：近接スイッチ

―	IEC 60947-5-3	低電圧開閉装置及び制御装置－ 第 5-3 部：制御回路装置及び開閉要素－故障条件で定義された挙動を持つ近接装置の要求事項
―	IEC 60947-5-4	低電圧開閉装置及び制御装置－ 第 5-4 部：制御回路装置及び開閉素子－低電力接点の性能評価法－特殊試験
JIS C 8201-5-5	IEC 60947-5-5	低電圧開閉装置及び制御装置－ 第 5 部：制御回路機器及び開閉素子－第 5 節：機械的ラッチング機能をもつ電気的非常停止機器
―	IEC 60947-5-6	低電圧開閉装置及び制御装置－ 第 5-6 部：制御回路装置及び開閉要素－近接センサ及び開閉増幅器(NAMUR)のための直流インタフェース
―	IEC 60947-5-7	低電圧開閉装置及び制御装置－ 第 5-7 部：制御回路装置及び開閉素子－アナログ出力をもつ近接素子の要求事項
JIS C 8201-5-8	IEC 60947-5-8	低電圧開閉装置及び制御装置－ 第 5-8 部：制御回路機器及び開閉素子－3 ポジションイネーブルスイッチ
―	IEC 60947-5-9	低電圧開閉装置及び制御装置－ 第 5-9 部：制御回路装置及び開閉素子－流量スイッチ
JIS C 8201-5-101	IEC 60947-5-101	低電圧開閉装置及び制御装置－ 第 5 部：制御回路機器及び開閉素子－第 101 節：接触器形リレー及びスタータの補助接点
―	IEC 60947-6-1	低電圧開閉装置及び制御装置－ 第 6-1 部：多機能機器－自動切替え機器
―	IEC 60947-6-2	低電圧開閉装置及び制御装置－ 第 6-2 部：多機能機器－制御及び保護開閉装置(又は機器)
JIS C 8201-7-1	IEC 60947-7-1	低電圧開閉装置及び制御装置－ 第 7 部：補助装置－第 1 節：銅導体用端子台
JIS C 8201-7-2	IEC 60947-7-2	低電圧開閉装置及び制御装置－ 第 7-2 部：補助装置－銅導体用保護導体端子台
―	IEC 60947-7-3	低電圧開閉装置及び制御装置－ 第 7-3 部：補助機器－ヒューズ端子台の安全要求事項
―	IEC 60947-7-4	低電圧開閉装置及び制御装置－ 第 7-4 部：補助機器－銅導体用の PCB 端子ブロック
―	IEC 60947-8	低電圧開閉装置及び制御装置－ 第 8 部：回転電気機械の内蔵温度保護(PTC)の制御ユニット
JIS B 3501	IEC 61131-1	プログラマブルコントローラ－ 第 1 部:一般情報
JIS B 3502	IEC 61131-2	プログラマブルコントローラ－ 第 2 部：機器要求事項及び試験

JIS B 3503	IEC 61131-3	プログラマブルコントローラー 第3部：プログラム言語
―	IEC/TR 61131-4	プログラマブルコントローラー 第4部：使用者手引き
―	IEC 61131-5	プログラマブルコントローラー 第5部：通信
―	IEC 61131-6	プログラマブルコントローラー 第6部：機能安全
―	IEC 61131-7	プログラマブルコントローラー 第7部：ファジー制御プログラミング
―	IEC/TR 61131-8	プログラマブルコントローラー 第8部：プログラム言語の適用及び実施の指針
―	IEC 61131-9	プログラマブルコントローラー 第9部：小型センサ及びアクチュエータ(SDCI)のためのシングルドロップデジタル通信インタフェース
JIS B 9706-1	IEC 61310-1	機械類の安全性－表示，マーキング及び操作－ 第1部：視覚，聴覚及び触覚シグナルの要求事項
JIS B 9706-2	IEC 61310-2	機械類の安全性－表示，マーキング及び操作－ 第2部：マーキングの要求事項
JIS B 9706-3	IEC 61310-3	機械類の安全性－表示，マーキング及び操作－ 第3部：アクチュエータの配置及び操作に対する要求事項
JIS B 9704-1	IEC 61496-1	機械類の安全性－電気的検知保護設備－ 第1部：一般要求事項及び試験
JIS B 9704-2	IEC 61496-2	機械類の安全性－電気的検知保護設備－ 第2部：能動的光電保護装置を使う設備に対する要求事項
JIS B 9704-3	IEC 61496-3	機械類の安全性－電気的検知保護設備－第3部：拡散反射形能動的光電保護装置に対する要求事項
TR B 0025	IEC/TR 61496-4	機械類安全性－電気的検知保護設備－ 第4部：映像利用保護装置(VBPD)を用いる設備に対する要求事項
―	IEC/TS 61496-4-2	機械類の安全性－電気感光性保護機器－第4-2部：視覚的保護装置(VBPD)を用いる機器に関する特定要求事項－基準パターン技法(VBPDPP)を用いるときの追加要求事項
―	IEC/TS 61496-4-3	機械類の安全性－電気感光性保護機器－第4-3部：視覚的保護装置(VBPD)を用いる機器に関する特定要求事項－立体視覚技法(VBPDST)を用いるときの追加要求事項
―	IEC/TR 61508-0	電気/電子/プログラム可能電子安全関連システムの機能安全－第0部：機能安全及びIEC 61508
JIS C 0508-1	IEC 61508-1	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：一般要求事項

JIS C 0508-2	IEC 61508-2	電気・電子・プログラマブル電子安全関連系の機能安全－第2部：電気・電子・プログラマブル電子安全関連系の要求事項
JIS C 0508-3	IEC 61508-3	電気・電子・プログラマブル電子安全関連系の機能安全－第3部：ソフトウエア要求事項
-	IEC/TS 61508-3-1	電気・電子・プログラマブル電子安全関連系の機能安全－第3-1部：ソフトウエア要求事項－安全機能のすべて又は一部を実施するための既存のソフトウェア要素の再利用
JIS C 0508-4	IEC 61508-4	電気・電子・プログラマブル電子安全関連系の機能安全－第4部：用語の定義及び略語
JIS C 0508-5	IEC 61508-5	電気/電子/プログラマブル電子安全関連系の機能安全－第5部：安全度水準の決定方法の例
JIS C 0508-6	IEC 61508-6	電気/電子/プログラマブル電子安全関連系の機能安全－第6部：IEC 61508-2及び IEC 61508-3の適用の指針
JIS C 0508-7	IEC 61508-7	電気・電子・プログラマブル電子安全関連系の機能安全－第7部：技法及び措置の概要
－	IEC/TR 61511-0	機能安全－プロセス工業部門の安全計装システム－第0部：プロセス工業及びIEC 61511の機能安全
－	IEC 61511-1	機能安全－プロセス工業部門の安全計装システム－第1部：枠組み，定義，システム，ハードウェア及びソフトウェア要求事項
－	IEC 61511-2	機能安全－プロセス工業部門の安全計装システム－第2部：IEC 61511-1の適用の指針
－	IEC 61511-3	機能安全－プロセス工業部門の安全計装システム－第3部：安全度水準の決定のための指針
－	IEC 61511-SER	機能安全－プロセス工業部門の安全計装システム－すべての部
－	IEC/TR 62271-301	高電圧開閉装置及び制御装置－第301部：端子の寸法標準化
－	IEC/TR 62046	機械類の安全性－人を検出する保護設備の使用基準
JIS B 9961	IEC 62061	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
－	IEC/TR 62061-1	機械の安全関連制御システムの設計におけるISO 13849-1及びIEC 62061の適用の手引
－	IEC 62194	エンクロージャの耐熱性能の評価方法
TR B 0030	IEC/TR 62513	機械類の安全性－安全関連通信システムの使用指針
タイプB規格：流体動力		
JIS B 8361	ISO 4413	油圧－システム及びその機器の一般規則及び安全要求事項
JIS B 8370	ISO 4414	空気圧－システム及びその機器の一般規則及び安全要求事項

タイプB規格：光学及びフォトニクス		
―	ISO 11145	光学及びフォトニクスーレーザ及びレーザ関連機器ー用語及び記号
―	ISO 11554	光学及びフォトニクスーレーザ及びレーザ関連機器ーレーザビーム出力，エネルギー及び時間特性の試験方法
タイプB規格：振　動		
―	ISO 2017-1	機械振動及び衝撃ー弾性支持装置ー第1部：分離装置の適用のために交換すべき技術情報
―	ISO 2017-2	機械振動及び衝撃ー弾性支持システムー第2部：鉄道網に付随する振動絶縁の適用のために交換すべき情報
JIS B 0153	ISO 2041	機械振動・衝撃用語
JIS B 7760-2	ISO 2631-1	全身振動ー第2部：測定方法及び評価に関する基本的要求
―	ISO 2631-2*	機械振動及び衝撃ー人体の全身振動暴露の評価ー第2部：建物内の振動(1Hz～80Hz)
―	ISO 2631-4	械振動及び衝撃ー人体の全身振動暴露の評価ー第4部：固定案内走行路輸送システムにおいて振動及び回転運動が乗客並びに乗員の快適性に与える作用の評価に関する指針
―	ISO 2631-5	機械振動及び衝撃ー全身振動に暴露される人体の評価ー第5部：多重衝撃を含む振動の評価方法
―	ISO 3046-5	往復動機関ー性能ー第5部：ねじり振動
JIS B 7761-3	ISO 5349-1	手腕系振動ー第3部：測定及び評価に関する一般要求事項
JIS B 7761-2	ISO 5349-2	手腕系振動ー第2部：作業場における実務的測定方法
JIS Z 8131	ISO 5805	機械振動及び衝撃ー人体暴露―用語
JIS B 7760-1	ISO/DIS 8041	全身振動ー第1部：測定装置
JIS B 0906	ISO 10816-1	機械振動ー非回転部分における機械振動の測定と評価ー一般的指針
―	ISO 13753	機械振動及び衝撃ーハンドアーム振動ーハンドアーム装置によって負荷したときの弾性材料の振動透過率を測定する方法
―	ISO 20643	機械振動ー手持ち及び手案内機械ー振動伝達の評価の原理
タイプB規格：電磁両立性(EMC)		
―	IEC/TR 61000-1-1*	電磁両立性(EMC)ー第1部：一般ー第1部：基本定義及び用語の適用及び解釈
―	IEC 61000-1-2*	電磁両立性(EMC)ー第1-2部：一般ー機器を含む電気及び電子システムの電磁現象に対する機能安全実現のための方法論

―	IEC/TR 61000-1-3*	電磁両立性(EMC)－第 1-3 部：一般－民生用機器及びシステムへの高緯度 EMP (HEMP)の影響
―	IEC/TR 61000-1-4	電磁両立性(EMC)－第 1-4 部：一般－2 kHz 以下の周波数範囲における機器からの商用周波伝導高調波エミッションの制限に関する歴史的根拠
―	IEC/TR 61000-1-5	電磁両立性(EMC)－第 1-5 部：一般－民間系統における高出力電磁(HPEM)効果
―	IEC/TR 61000-1-6	電磁両立性(EMC)－第 1-6 部：一般－測定の不確かさの評価の手引
―	IEC/TR 61000-1-7	電磁両立性(EMC)－第 1-7 部：一般－非正弦条件下の単相システムの力率
―	IEC/TR 61000-2-1*	電磁両立性(EMC)－第 2 部：環境－第 1 部：環境の概要－一般電源における低周波伝導妨害及び信号発生の電磁環境
―	IEC 61000-2-2*	電磁両立性(EMC)－第 2-2 部：環境－第 2 章：公共低電圧電源系統における低周波伝導妨害及び信号発生の両立性レベル
―	IEC/TR 61000-2-3*	電磁両立性(EMC)－第 2 部：環境－第 3 章：環境の概要－放射及び非ネットワーク周波数関連伝導現象
―	IEC 61000-2-4*	電磁両立性(EMC)－第 2-4 部：環境－産業プラントにおける低周波伝導妨害の両立性
―	IEC/TR 61000-2-5	電磁両立性(EMC)－第 2-5 部：環境－電磁環境の概要及び分類
―	IEC/TR 61000-2-6*	電磁両立性(EMC)－第 2 部：環境－第 6 章：工場の電源における低周波伝導妨害の放射レベル評価
―	IEC/TR 61000-2-7*	電磁両立性(EMC)－第 2 部：環境－各種環境における低周波磁界
―	IEC/TR 61000-2-8*	電磁両立性(EMC)－第 2-8 部：環境－統計的測定結果を含む公共電源系統の電圧ディップ及び短時間停電
―	IEC 61000-2-9*	電磁両立性(EMC)－第 2 部：環境－第 9 章：HEMP 環境の概要－放射妨害－基本 EMC 出版物
―	IEC 61000-2-10*	電磁両立性(EMC)－第 2-10 部：環境－HEMP 環境の概要－伝導妨害
―	IEC 61000-2-11*	電磁両立性(EMC)－第 2-11 部：環境－HEMP 環境の分類
―	IEC 61000-2-12	電磁両立性(EMC)－第 2-12 部：環境－商用中電圧電源系統における低周波伝導妨害及び信号発生の両立性レベル
―	IEC 61000-2-13*	電磁両立性(EMC)－第 2-13 部：環境－高出力電磁(HPEM)環境－放射及び伝導
―	IEC/TR 61000-2-14	電磁両立性(EMC)－第 2-14 部：環境－公共配電網の過電圧

JIS C 61000-3-2	IEC 61000-3-2	電磁両立性（EMC）－第 3-2 部：限度値－高調波電流発生限度値（1 相当たりの入力電流が 20Ａ以下の機器）
－	IEC 61000-3-3*	電磁両立性(EMC)－第 3-3 部：限度値－1 相当り 16A 以下の定格電流を持ち，かつ，条件付接続に左右されない装置用の公共低電圧電源系統における電圧変化，電圧変動及びフリッカの限度
－	IEC/TS61000-3-4*	電磁両立性(EMC)－第 3-4 部：限度値－定格電流 16 A 超の機器の低電圧電源の調波電流放射限度値
－	IEC/TS610003-5	電磁両立性(EMC)－第 3-5 部：限度値－定格電流 75 A 超の機器の低電圧電源の電圧変動及びフリッカ限度値
－	IEC/TR 610003-6	電磁両立性(EMC)－第 3-6 部：限度値－MV，HV 及び EHV 電源の設備歪みの接続の放射限度値の評価
－	IEC/TR 61000-3-7	電磁両立性(EMC)－第 3-7 部：限度値－MV，HV 及び EHV 電源の変動設備の接続の放射限度値の評価
－	IEC 61000-3-8*	電磁両立性(EMC)－第 3 部：限度値－第 8 章：低電圧電気設備の信号発生－放射レベル，周波数帯及び電磁妨害レベル
－	IEC 61000-3-11*	電磁両立性(EMC)－第 3-11 部：限度値－一般低電圧電源における電圧変化，電圧変動及びフリッカの限度値－定格電流<=75A で，条件接続を受ける機器
－	IEC 61000-3-12*	電磁両立性(EMC)－第 3-12 部：限度値－商用低電圧系統に接続された相あたり 16 A 超 75 A 以下の入力電流をもつ機器によって生成される高調波電流の限度値
－	IEC/TR 61000-3-13	電磁両立性(EMC)－第 3-13 部：限度値－MV，HV 及び EHV 電源の非均衡設備の接続の放射限度値の評価
－	IEC/TR61000-3-14	電磁両立性(EMC)－第 3-14 部：低圧電源系統への擾乱設備の接続に関する高調波，時数間高調波，電圧変動及び不均衡に対するエミッション限度値の評価
－	IEC/TR 6100-3-15	電磁両立性(EMC)－第 3-15 部：限度値－低電圧網の分散発電系統に関する低周波電磁イミュニティの評価及びエミッション要求事項
－	IEC 61000-4-1*	電磁両立性(EMC)－第 4-1 部：試験及び測定技術－IEC 61000-4 シリーズの概観
JIS C 61000-4-2	IEC 61000-4-2	電磁両立性（EMC）－第 4-2 部：試験及び測定技術－静電気放電イミュニティ試験
JIS C 61000-4-3	IEC 61000-4-3	電磁両立性（EMC）－第 4-3 部：試験及び測定技術－放射無線周波電磁界イミュニティ試験
JIS C 61000-4-4	IEC 61000-4-4	電磁両立性(EMC)－第 4-4 部：試験及び測定技術－電気的ファストトランジェント/バーストイミュニティ試験
JIS C 61000-4-5	IEC 61000-4-5	電磁両立性(EMC)－第 4-5 部：試験及び測定技術－サージイミュニティ試験

JIS C 61000-4-6	IEC 61000-4-6	電磁両立性(EMC)－第 4-6 部：試験及び測定技術－無線周波数界によって誘導する伝導妨害に対するイミュニティ
JIS C 61000-4-7	IEC 61000-4-7	電磁両立性（EMC）－第 4-7 部：試験及び測定技術－電力供給システム及びこれに接続する機器のための高調波及び次数間高調波の測定方法及び計装に関する指針
JIS C 61000-4-8	IEC 61000-4-8	電磁両立性（EMC）－第 4 部：試験及び測定技術－第 8 節：電源周波数磁界イミュニティ試験
－	IEC 61000-4-9	電磁両立性(EMC)－第 4-9 部：試験及び測定技術－パルス磁界イミュニティ試験
－	IEC 61000-4-10*	電磁両立性(EMC)－第 4-10 部：試験及び測定技術－減衰振動磁界イミュニティ試験
JIS C 61000-4-11	IEC 61000-4-11	電磁両立性（EMC）－第 4-11 部：試験及び測定技術－電圧ディップ，短時間停電及び電圧変動に対するイミュニティ試験
－	IEC 61000-4-12*	電磁両立性(EMC)－第 4-12 部：試験及び測定技術－振動波イミュニティ試験
－	IEC 61000-4-13*	電磁両立性(EMC)－第 4-13 部：試験及び測定技術－交流電力ポートにおける電源線信号を含む高調波及び中間高調波の低周波イミュニティ試験
JIS C 61000-4-14	IEC 61000-4-14	電磁両立性－第 4 部：試験及び測定技術－第 14 節：電圧変動イミュニティ試験
－	IEC 61000-4-15*	電磁両立性(EMC)－第 4-15 部：試験及び測定技術－フリッカメーター機能及び設計仕様
JIS C 61000-4-16	IEC 61000-4-16	電磁両立性（EMC）－第 4 部：試験及び測定技術－第 16 節：直流から 150kHz までの伝導コモンモード妨害に対するイミュニティ試験
JIS C 61000-4-17	IEC 61000-4-17	電磁両立性（EMC）－第 4 部：試験及び測定技術－第 17 節：直流入力電源端子におけるリプルに対するイミュニティ試験
－	IEC 61000-4-18	電磁両立性(EMC)－第 4-18 部：試験及び測定技術－減衰振動波イミュニティ試験
－	IEC 61000-4-19	電磁両立性(EMC)－第 4-19 部：試験及び測定技術－AC 電力ポートでの周波数が 2 kHz～150kHz における伝導性，差動モード妨害及び信号伝達に対するイミュニティ試験
JIS C 61000-4-20	IEC 61000-4-20	電磁両立性（EMC）－第 4-20 部：試験及び測定技術－TEM（横方向電磁界）導波管のエミッション及びイミュニティ試験
－	IEC 61000-4-21*	電磁両立性(EMC)－第 4-21 部：試験及び測定技術－残響室試験方法
JIS C 61000-4-22	IEC 61000-4-22	電磁両立性－第 4-22 部：試験及び測定技術－全電波無響室（FAR）における放射エミッション及びイミュニティ試験

―	IEC 61000-4-23*	電磁両立性(EMC)－第 4-23 部：試験及び測定技術－HEMP 及び他の放射妨害に対する保護装置の試験方法
―	IEC 61000-4-24*	電磁両立性(EMC)－第 4 部：試験及び測定技術－第 24 章：HEMP 伝導妨害に対する保護装置の試験方法－基本 EMC 出版物
―	IEC 61000-4-25*	電磁両立性(EMC)－第 4-25 部：試験及び測定技術－機器及びシステムの HEMP イミュニティ試験方法
―	IEC 61000-4-27*	電磁両立性(EMC)－第 4-27 部：試験及び測定技術－入力電流が 16A/相以下の機器の非平衡イミュニティ試験
―	IEC 61000-4-28*	電磁両立性(EMC)－第 4-28 部：試験及び測定技術－入力電流が 16A/相以下の機器の電力周波数のばらつきのイミュニティ試験
―	IEC 61000-4-29*	電磁両立性(EMC)－第 4-29 部：試験及び測定技術－直流入力電力ポートの電圧降下，短期中断及び電圧変動イミュニティ試験
―	IEC 61000-4-30	電磁両立性(EMC)－第 4-30 部：試験及び測定技術－電力品質測定方法
―	IEC 61000-4-31	電磁両立性(EMC)－第 4-31 部：試験及び測定技術－AC 主電源ポート広帯域伝導妨害イミュニティ試験
―	IEC/TR 61000-4-32*	電磁両立性(EMC)－第 4-32 部：試験及び測定技術－高高度電磁パルス(HEMP)シミュレータの概要
―	IEC 61000-4-33*	電磁両立性(EMC)－第 4-33 部：試験及び測定技術－高電力過渡電圧パラメタの測定方法
JIS C 61000-4-34	IEC 61000-4-34	電磁両立性（EMC）－第 4-34 部：試験及び測定技術－1 相当たりの入力電流が 16A を超える電気機器の電圧ディップ，短時間停電及び電圧変動に対するイミュニティ試験
―	IEC/TR 61000-4-35	電磁両立性(EMC)－第 4-35 部：試験及び測定技術－HPEM シミュレータ概論
―	IEC 61000-4-36	電磁両立性(EMC)－第 4-36 部：試験及び測定技術－機器及びシステムの IEMI イミュニティ試験方法
―	IEC/TR 61000-4-37	電磁両立性(EMC)－高調波放射適合試験システムの校正及び検証
―	IEC/TR 61000-4-38	電磁両立性(EMC)－第 4-38 部：試験及び測定技術－電圧変動及びフリッカー適合試験システムのための試験，検証及び校正プロトコル
―	IEC 61000-4-39	電磁両立性(EMC)－第 4-39 部：試験及び測定技術－近接近の放射界－イミュニティ試験
―	IEC/TR 61000-5-1*	電磁両立性(EMC)－第 5 部：据付け及び軽減の指針－第 1 章：一般考慮事項－基本 EMC 出版物
―	IEC/TR 61000-5-2*	電磁両立性(EMC)－第 5 部：据付け及び軽減の指針－第 2 章：接地及びケーブル敷設

－	IEC/TR61000-5-3*	電磁両立性(EMC)－第 5-3 部：設置及び緩和の指針－HEMP 防護の概念
－	IEC/TS 61000-5-4*	電磁両立性(EMC)－第 5 部：据付け及び軽減の指針－第 4 章：HEMP に対するイミュニティ－HEMP 放射妨害に対する保護装置の仕様－基本 EMC 出版物
－	IEC 61000-5-5*	電磁両立性(EMC)－第 5 部：据付け及び軽減の指針－第 5 章：HEMP に対するイミュニティ－HEMP 伝導妨害に対する保護装置の仕様－基本 EMC 出版物
－	IEC/TR 61000-5-6*	電磁両立性(EMC)－第 5-6 部：設置及び緩和の指針－外部 EM の影響の緩和
－	IEC 61000-5-7*	電磁両立性(EMC)－第 5-7 部：据付け及び軽減の指針－エンクロージャによる電磁妨害に対する保護等級(EM コード)
－	IEC/TS 61000-5-8	電磁両立性(EMC)－第 5-8 部：据付け及び軽減の指針－分散型インフラストラクチャの HEMP 保護方法
－	IEC/TS 61000-5-9	電磁両立性(EMC)－第 5-9 部：据付け及び軽減の指針－HEMP 及び HPEN のシステムレベル感受性のアセスメント
－	IEC/TS 61000-5-10	電磁両立性(EMC)－第 5-10 部：据付け及び軽減の指針－HEMP 及び IEMI 対する施設の保護の手引
JIS C 61000-6-1	IEC 61000-6-1	電磁両立性（EMC）－第 6-1 部：共通規格－住宅，商業及び軽工業環境におけるイミュニティ
JIS C 61000-6-2	IEC 61000-6-2	電磁両立性(EMC)－第 6-2 部：共通規格－工業環境におけるイミュニティ
－	IEC 61000-6-3*	電磁両立性(EMC)－第 6-3 部：一般規格－住宅，商業及び軽工業環境のエミッション規格
－	IEC 61000-6-4*	電磁両立性(EMC)－第 6-4 部：一般規格－工業環境のエミッション規格
－	IEC 61000-6-5*	電磁両立性(EMC)－第 6-5 部：一般規格－発電所及び変電所環境のイミュニティ
－	IEC 61000-6-6*	電磁両立性（EMC)－第 6-6 部：一般規格－屋内機器の HEMP イミュニティ
－	IEC 61000-6-7	電磁両立性（EMC)－第 6-7 部：一般規格－工業環境において安全関連システムの機能(機能安全)を果たすように意図された機器のイミュニティ要求事項
タイプ B 規格：音　響		
－	ISO 3740	音響－騒音源の音響出力レベルの測定－基本規格の使用法指針
JIS Z 8734	ISO 3741	音響－音圧法による騒音源の音響パワーレベルの測定方法－残響室における精密測定方法
－	ISO 3743-1	音響－音圧を使用した騒音源の音響出力レベルの測定－残響音場における小移動音源での測定方法－第 1 部：壁面が硬い試験室での比較法

－	ISO 3743-2	音響－音圧を使用した騒音源の音響出力レベルの測定－残響音場における小移動音源での測定方法－第2部：特殊残響試験室での測定法
JIS Z 8733	ISO 3744	音響－音圧法による騒音源の音響パワーレベルの測定方法－反射面上の準自由音場における実用測定方法
JIS Z 8732	ISO 3745	音響－音圧法による騒音源の音響パワーレベルの測定方法－無響室及び半無響室における精密測定方法
－	ISO 3746	音響－音圧を使用した騒音源の音響出力レベルの測定－反射面の上に包囲測定面を設ける測定法
－	ISO 3747	音響－音圧を使用した騒音源の音響出力レベルの測定－現場での比較法
－	ISO 4871	音響－機械及び機器の騒音発生量の宣言及び検証
－	ISO 5136	音響－ファン及びその他の換気装置によってダクト内に放射される音響パワーの測定－インダクト法
JIS Z 8739	ISO 6920	音響－音響パワーレベル算出に使用される基準音源の性能及び校正に対する要求事項
－	ISO 7235	音響－ダクテッドサイレンサ及びエアターミナルユニットの試験所内測定手順－挿入損失，気流音及び全圧損失
JIS Z 8738	ISO 9613-1	屋外の音の伝搬における空気吸収の計算
－	ISO 9613-2	音響－屋外伝播中の音の減衰－第2部：一般計算方法
JIS Z 8736-1	ISO 9614-1	音響－音響インテンシティによる騒音源の音響パワーレベルの測定方法－第1部：離散点による測定
JIS Z 8736-2	ISO 9614-2	音響－音響インテンシティによる騒音源の音響パワーレベルの測定方法－第2部：スキャニングによる測定
JIS Z 8376-3	ISO 9614-3	音響－音響インテンシティによる騒音源の音響パワーレベルの測定方法－第3部：スキャニングによる精密測定
－	ISO 11200	音響－機械及び装置～放射された騒音－ワークステーション及び他の所定の位置における放射音圧レベルの計測に使用される基本的規格に対する指針
JIS Z 8737-1	ISO 11201	音響－作業位置及び他の指定位置における機械騒音の放射音圧レベルの測定方法－第1部：反射面上の準自由音場における実用測定方法
JIS Z 8737-2	ISO 11202	音響－作業位置及び他の指定位置における機械騒音の放射音圧レベルの測定方法－第2部：現場における簡易測定方法
－	ISO 11203	音響－機械及び装置～放射された騒音－音響パワーレベルによるワークステーション及び他の所定の位置における放射音圧レベルの計測

－	ISO 11204	音響－機械及び装置～放射された騒音－ワークステーション及び他の所定の位置における放射音圧レベルの計測－環境的相関を要求する方法
－	ISO 11205	音響－機械及び機器から放射される騒音－音響強度を用いた作業場及びその他の規定場所における現場の放射音圧レベルの測定のための工学的方法
－	ISO 11546-1	音響－エンクロージャの遮音性能の測定－第 1 部：試験所条件での測定(適合性宣言のため)
－	ISO 11546-2	音響－エンクロージャの遮音性能の測定－第 2 部：現地測定(受渡し及び検証のため)
－	ISO/TR 11688-1	音響学－低騒音機械及び機器の設計の推奨手順－第 1 部：計画
－	ISO/TR 11688-2	音響学－低騒音機械及び機器の設計の推奨手順－第 2 部：低騒音設計の物理学の概要
－	ISO 11690-1	音響学－防音機械室の設計のための推奨作業－第 1 部：防音戦略
－	ISO 11690-2	音響学－防音機械室の設計のための推奨作業－第 2 部：防音措置
－	ISO/TR 11690-3	音響学－機械を含む低騒音職場の設計の推奨手順－第 3 部：作業室における音の伝搬及び騒音予測
－	ISO 11691	音響学－流れなしのダクト接続形消音器の挿入損失の測定－試験室調査方法
－	ISO 11957	音響学－キャビンの防音性能の測定方法－試験室及び現場測定
－	ISO 12001	音響学－機械及び装置によって放出される雑音－雑音試験コードの原案作成及び提出に関する規則
タイプ B 規格：人間工学		
JIS Z 8907	ISO 1503	空間的方向性及び運動方向－人間工学的要求事項
JIS Z 8501	ISO 6385	人間工学－作業システム設計の原則
JIS Z 8504	ISO 7243	人間工学－WBGT（湿球黒球温度）指数に基づく作業者の熱ストレスの評価―暑熱環境
JIS Z 8500	ISO 7250	人間工学－設計のための基本人体測定項目
－	ISO 7726	温熱環境の人間工学－熱環境物理量測定のための機器と方法
－	ISO 7730	熱環境の人間工学－PMV 及び PPD 指標の計算及び局所快適温熱基準による快適温熱の分析的測定及び解釈
－	ISO 7731*	人間工学－公共の場所及び職場の危険信号－聴覚危険信号
－	ISO 7933*	温熱環境の人間工学－暑熱負担予測指標の計算による暑熱ストレスの解析
－	ISO 8996*	人間工学－代謝熱産生量の算定法

JIS Z 8511	ISO 9241-1	人間工学－視覚表示装置を用いるオフィス作業－通則
JIS Z 8512	ISO 9241-2	人間工学－視覚表示装置を用いるオフィス作業－仕事の要求事項についての指針
JIS Z 8513	ISO 9241-3	人間工学－視覚表示装置を用いるオフィス作業－視覚表示装置の要求事項
JIS Z 8514	ISO 9241-4	人間工学－視覚表示装置を用いるオフィス作業－キーボードの要求事項
JIS Z 8515	ISO 9241-5	人間工学－視覚表示装置を用いるオフィス作業－ワークステーションのレイアウト及び姿勢の要求事項
JIS Z 8516	ISO 9241-6	人間工学－視覚表示装置を用いるオフィス作業－作業環境に関する指針
JIS Z 8517	ISO 9241-7	人間工学－視覚表示装置を用いるオフィス作業－画面反射に関する表示装置の要求事項
JIS Z 8518	ISO 9241-8	人間工学－視覚表示装置を用いるオフィス作業－表示色の要求事項
JIS Z 8519	ISO 9241-9	人間工学－視覚表示装置を用いるオフィス作業－非キーボードの入力装置の要求事項
JIS Z 8521	ISO 9241-11	人間工学－視覚表示装置を用いるオフィス作業－使用性についての手引
JIS Z 8522	ISO 9241-12	人間工学－視覚表示装置を用いるオフィス作業－情報の提示
JIS Z 8523	ISO 9241-13	人間工学－視覚表示装置を用いるオフィス作業－ユーザー向け案内
JIS Z 8524	ISO 9241-14	人間工学－視覚表示装置を用いるオフィス作業－メニュー対話
JIS Z 8525	ISO 9241-15	人間工学－視覚表示装置を用いるオフィス作業－コマンド対話
JIS Z 8526	ISO 9241-16	人間工学－視覚表示装置を用いるオフィス作業―直接操作対話
JIS Z 8527	ISO 9241-17	人間工学－視覚表示装置を用いるオフィス作業－書式記入対話
JIS X 8341-1	ISO 9241-20	高齢者・障害者等配慮設計指針－情報通信における機器，ソフトウェア及びサービス－第１部：共通指針
－	ISO/TR 9241-100	人間工学－人とシステムとのインタラクション－第100部：ソフトウェア人間工学関連規格の手引
JIS Z 8520	ISO 9241-110	人間工学－人とシステムとのインタラクション－対話の原則
－	ISO 9241-129	人間工学－人とシステムとのインタラクション－第129部：ソフトウェア個別化の手引き
－	ISO 9241-143	人間工学－人とシステムとのインタラクション－第143部：形状

―	ISO 9241-151	人間工学－人とシステムとのインタラクション－第151部：ワールドワイドウェブのユーザインタフェースの手引
―	ISO 9241-154	人間工学－人とシステムとのインタラクション－第154部：自動音声応答装置(IVR)アプリケーション
JIS X 8341-6	ISO 9241-171	高齢者・障害者等配慮設計指針－情報通信における機器，ソフトウェア及びサービス－第6部：対話ソフトウェア
―	ISO 9241-210	人間工学－人とシステムとのインタラクション－第210部：対話型システムの人間中心設計
―	ISO 9241-300	人間工学－人とシステムとのインタラクション－第300部：電子視覚装置要求事項の手引
―	ISO 9241-302	人間工学－人とシステムとのインタラクション－第302部：電子視覚装置の用語
―	ISO 9241-303	人間工学－人とシステムとのインタラクション－第303部：電子視覚装置の要求事項
―	ISO 9241-304	人間工学－人とシステムとのインタラクション－第304部：電子視覚装置要求事項のユーザパフォーマンス試験方法
―	ISO 9241-305	人間工学－人とシステムとのインタラクション－第305部：電子視覚装置の光学試験所試験方法
―	ISO 9241-306	人間工学－人とシステムとのインタラクション－第306部：電子視覚装置の現場評価方法
―	ISO 9241-307	人間工学－人とシステムとのインタラクション－第307部：電子視覚装置の分析及び適合性試験方法
―	ISO/TR 9241-308	人間工学－人とシステムとのインタラクション－第308部：表面伝導型電子放出表示装置(SED)
―	ISO/TR 9241-309	人間工学－人とシステムとのインタラクション－第309部：有機発光ダイオード(OLED)表示装置
―	ISO/TR 9241-310	人間工学－人とシステムとのインタラクション－第310部：ピクセル欠陥の認性，美観及び人間工学
―	ISO/TR 9241-331	人間工学－人とシステムとのインタラクション－第331部：立体ディスプレイの光学的特性
―	ISO 9241-400	人間工学－人とシステムとのインタラクション－第400部：物理的入力装置の原理及び要求事項
―	ISO 9241-410	人間工学－人とシステムとのインタラクション－第410部：物理的入力装置の設計基準
―	ISO/TS 9241-411	人-システム相互作用の人間工学－第411部：物理的入力装置の設計の評価方法
―	ISO 9241-420	人間工学－人とシステムとのインタラクション－第420部：物理的入力装置の選択
―	ISO 9241-910	人間工学－人とシステムとのインタラクション－第910部：触知触覚のフレームワーク

－	ISO 9241-920	人間工学－人とシステムのインタラクション－第920部：触覚及び皮膚感覚のインタラクションの手引
－	ISO 9355-1	表示器及び制御作動器の設計における人間工学要求事項－第1部：表示器及び制御作動器と人間との相互作用
－	ISO 9355-2	表示器及び制御作動器の設計における人間工学必要条件－第2部：表示器
－	ISO 9355-3	表示器及び制御作動器の設計における人間工学要求事項－第3部：制御作動器
－	ISO/DIS 9355-4	表示器及び制御作動器の設計における人間工学要求事項－第4部：表示及制御アクチュエータの配置
－	ISO 9886	人間工学－生理的測定による熱ひずみの評価
－	ISO 9920	温熱環境の人間工学－被着衣の断熱性と透湿抵抗の評価
－	ISO 9921*	人間工学－言語伝達の評価
JIS Z 8502	ISO 10075	人間工学－精神的作業負荷に関する原則－用語及び定義
JIS Z 8503	ISO 10075-2	人間工学－精神的作業負荷に関する原則－設計の原則
－	ISO 10075-3	人間工学－精神的作業負荷に関する原則－第3部：精神的作業負荷の測定及び評価のための方法に関する原則及び要求事項
－	ISO 10551	温熱環境の人間工学－主観尺度による温熱環境評価
JIS Z 8503-1	ISO 11064-1	人間工学－コントロールセンターの設計－第1部：コントロールセンターの設計原則
JIS Z 8503-2	ISO 11064-2	人間工学－コントロールセンターの設計－第2部：コントロールスウィートの基本配置計画の原則
JIS Z 8503-3	ISO 11064-3	人間工学－コントロールセンターの設計－第3部：コントロールルームの配置計画
JIS Z 8503-4	ISO 11064-4	人間工学－コントロールセンターの設計－第4部：ワークステーションの配置及び寸法
JIS Z 8503-6	ISO 11064-6	人間工学－コントロールセンターの設計－第6部：コントロールセンターの環境
－	ISO 11064-7	人間工学－コントロールセンターの設計－第7部：コントロールセンターの評価のための原則
－	ISO 11079	寒冷環境の評価－必要衣服熱抵抗の算出
－	ISO 11226	人間工学－静的作業姿勢の評価
－	ISO 11228-1	人間工学－手動取扱い－第1部：巻き上げ及び運搬
－	ISO 11399	温熱環境の人間工学－国際規格の思想と適用原理
－	ISO 11428*	人間工学－視覚的な危険信号－一般的な必要条件，設計及び検査

－	ISO 11429*	人間工学－音及び光を用いた危険及び安全信号のシステム
－	ISO 12894	温熱環境の人間工学－著しい暑熱・寒冷環境に曝される者への事前健康審査
JIS Z 8528-1	ISO 13406-1	人間工学－フラットパネルディスプレイ（FPD）を用いる作業－第1部：通則
JIS Z 8528-2	ISO 13406-2	人間工学－フラットパネルディスプレイ（FPD）を用いる作業－第2部：FPDの人間工学的要求事項
JIS Z 8530	ISO 13407	人間工学－インタラクティブシステムの人間中心設計プロセス
－	ISO 13731	温熱環境の人間工学－用語とシンボル
－	ISO 13732-1*	機械類の安全性－接触表面の温度－熱い表面の温度限界値を定めるための人間工学的データ
－	ISO/TS 13732-2	温熱環境の人間工学－表面接触時の人体反応の評価法－第2部：中庸温域表面への人体接触
－	ISO 13732-3	温熱環境の人間工学－表面接触時の人体反応の評価法－第3部：低温表面
－	ISO 14738*	機械類の安全性－機械のワークステーションの設計に対する人体測定要求事項
JIS Z 8531-1	ISO 14915-1	人間工学－マルチメディアを用いるユーザインタフェースのソフトウェア－第1部：設計原則及び枠組み
JIS Z 8531-2	ISO 14915-2	人間工学－マルチメディアを用いるユーザインタフェースのソフトウェア－第2部：マルチメディアナビゲーション及び制御
JIS Z 8531-3	ISO 14915-3	人間工学－マルチメディアを用いるユーザインタフェースのソフトウェア－第3部：メディアの選択及び組合せ
－	ISO 15265	温熱環境の人間工学－温熱作業条件におけるストレス及び不快感を予防するためのリスクアセスメント戦略
－	ISO 15534-1*	機械類の安全のための人間工学的設計－第1部：身体全体で近づいて作業する場合の開口部寸法決定の原理
－	ISO 15534-2*	機械類の安全のための人間工学的設計－第2部：作業用開口部寸法決定の原理
－	ISO 15534-3*	機械類の安全のための人間工学的設計－第3部：人体測定データ
－	ISO 15535*	人体計測データを作成するための一般要求事項
－	ISO 15536-1	人間工学－コンピュータマネキン及び人体テンプレート
－	ISO 15537	工業製品及び設計の人体計測学的側面を試験するための試験要員の選定及び使用の原則
タイプB規格：機械の特定部の設計		

JIS B 0651	ISO 3274	製品の幾何特性仕様(GPS)－表面性状：輪郭曲線方式－触針式表面粗さ測定機の特性
JIS B 2401-1	ISO 3601-1	0 リング－第 1 部：0 リング
JIS B 2401-2	ISO 3601-2	0 リング－第 2 部：ハウジングの形状・寸法
JIS B 2401-3	ISO 3601-3	0 リング－第 3 部：外観品質基準
－	ISO 3601-5	流体動力システム－0 リング－第 5 部：産業用弾性材料の適切性
JIS B 0601	ISO 4287	製品の幾何特性仕様(GPS)－表面性状：輪郭曲線方式－用語，定義及び表面性状パラメータ
JIS B 0659-1	ISO 5436-1	製品の幾何特性仕様（GPS）－表面性状：輪郭曲線方式；測定標準－第 1 部：標準片
－	ISO 21469	機械類の安全性－潤滑油と製品との偶発接触－衛生要求事項
－	ISO 23550	ガスバーナ及びガス燃焼器具の安全性及び制御装置－一般要求事項
－	ISO 23551-1	ガスバーナ及びガス燃焼機器の安全性及び制御装置－特定要求事項－第 1 部：自動弁
－	ISO 23551-2	ガスバーナ及びガス燃焼機器の安全性及び制御装置－特定要求事項－第 2 部：圧力調節器
－	ISO 23551-3	ガスバーナ及びガス燃焼機器の安全性及び制御装置－特定要求事項－第 3 部：ガス/空気比制御，空気圧タイプ
－	ISO 23551-4	ガスバーナ及びガス燃焼機器の安全性及び制御装置－特定要求事項－第 4 部：自動遮断弁のためのバルブ試験システム
－	ISO 23551-5	ガスバーナ及びガス燃焼機器の安全性及び制御装置－特定要求事項－第 5 部：手動ガス弁
－	ISO 23551-6	ガスバーナ及びガス燃焼機器の安全性及び制御装置－特定要求事項－第 6 部：熱起電炎監視制御
－	IEC 60079 ｼﾘｰｽﾞ*	爆発性雰囲気（シリーズ規格） ＊シリーズのうち，翻訳版があるものは一部。
タイプ B 規格：表示・図記号・製品情報		
JIS Z 9101	ISO 3864-1	安全色及び安全標識－産業環境及び案内用安全標識のデザイン通則
－	ISO 3864-2*	図記号－安全色及び安全標識－第 2 部：製品安全ラベルの設計原則
－	ISO 3864-3	図記号－安全色及び安全標識－第 3 部：安全標識に使用する図記号のためのデザイン原則
－	ISO 3864-4	図記号－安全色及び安全標識－第 4 部：安全標識材料の比色及び光度特性
－	ISO 7000*	機器に用いる図記号－索引及び摘要

JIS Z 7253	ISO 11014	GHS に基づく化学品の危険有害性情報の伝達方法－ラベル，作業場内の表示及び安全データシート（SDS）
JIS Z 9103	－	安全色－一般的事項
JIS Z 9104	－	安全標識－一般的事項
JIS Z 9095	ISO 16069	安全標識－避難誘導システム（SWGS）－蓄光式
JIS Z 9096	–	床面に設置する蓄光式の安全標識及び誘導ライン
JIS Z 9107	ISO 17398	安全標識－性能の分類，性能基準及び試験方法
JIS C 0617 ｼﾘｰｽﾞ	IEC 60617 ｼﾘｰｽﾞ	図表用図記号
－	IEC 60073*	マンマシンインタフェース，マーキング及び識別の基本安全原則－表示装置及びアクチュエータのコーディング原則
－	IEC 60445*	マンマシンインタフェースの基本及び安全原則，表示及び識別－機器端子及び導体端子部の識別
－	IEC 60447*	マンマシンインタフェース，マーキング及び識別のための基本及び安全原則－アクチュエータの操作に関する原則
JIS B 9706-1	IEC 61310-1	機械類の安全性－指示，マーキング及び作動－第 1 部：視覚的，音響及び触覚信号
JIS B 9706-2	IEC 61310-2	機械類の安全性－指示，マーキング及び作動－第 2 部：マーキング要求事項
JIS B 9706-3	IEC 61310-3	機械類の安全性－指示，マーキング及び作動－第 3 部：アクチュエータの位置及び操作の要求事項
―	IEC 82079-1*	取扱説明書の作成－構造，内容及び表示方法－第 1 部：一般原則及び詳細な要求事項