機能安全を活用した機械設備の安全確保

平成 27 年度　厚生労働省委託

国内外における機械安全規格に関する調査事業

平成 28 年 3 月

中央労働災害防止協会

目　次

はしがき

我が国の機械設備による災害の死傷者数は、平成26年においては27,392人にのぼり全災害の死傷者数(119,535人)の22.9%に当たる。機械設備による災害は、人の命が奪われたり、取り返しのつかない障害を負ったり、悲惨な結果に結びつくことが少なくない。

このような不幸なことが起きないよう、国際的にISO12100(JISB9700)を頂点とする機械安全規格体系を活用して、機械の安全方策に取り組み、機械設備による災害の未然防止を進めている。

機械安全の取組の中で、「機能安全」という考え方が昨今しばしば聞かれるようになってきている。その具体的定義や解説については、本編を参照いただくこととするが、「本来の機能に付加して導入される保護装置等により安全を確保すること」という言い方がある。また、危険源そのものを除去・低減する「本質的安全」と対比して「機能安全」について語られることも多い。

この冊子は、中災防が受託した平成27年度厚生労働省委託事業「国内外における機械安全規格の調査事業」の報告書であり、同事業において設置された「機械安全規格に関する検討委員会」の検討結果である。

本検討委員会においては、機械安全規格の中でどのように「機能安全」が扱われているかを概観した上で、ボイラー、産業用ロボット、動力プレス機械を中心に各機械設備に要求される機能安全の水準、個別の機械設備への規制との関連、機能安全水準の第三者認証に関する現状と課題などを検討し、報告書として取りまとめた。

平成28年3月

中央労働災害防止協会技術支援部

機械安全規格に関する検討委員会委員　名簿

（学識経験者）

・向殿　政男　(座長)（明治大学名誉教授）
・石田　　豊　（前（公社）産業安全技術協会　技術支援部部長）
・福田　隆文　（長岡科学技術大学・システム安全専攻　教授）
・芳司　俊郎　（長岡技術科学大学・システム安全専攻　准教授）

（機械設備ユーザー）

・奥村　浩次　（トヨタ自動車（株）安全健康推進部安全衛生室技術グループ長）
・奈木　　勉　（労働安全コンサルタント/元日本軽金属(株)）
・野呂　武史　（キユーピー（株）生産本部グループ安全担当）
・水野　恒夫　（セーフティクラフト/元・(株)ブリヂストン）

（機械設備メーカー関係）

・大村　宏之　（(一社）日本食品機械工業会事業部長）
・畑　　幸男　（コマツ産機（株）事業企画部主査）
・宮崎　浩一　（(一社）日本機械工業連合会標準化推進部長）
・若井　博雄　（日本規格協会国際標準化ユニット副ユニット長）
・渡辺　　隆　（(一社）日本電気制御機器工業会・制御安全委員会委員）

(厚生労働省)

安井　省侍郎　厚生労働省労働基準局安全衛生部安全課副主任中央産業安全専門官
國澤　幸平　　厚生労働省労働基準局安全衛生部安全課業務２係

Ⅰ　機械安全規格に見る安全関連システム／制御システムの安全関連部の要求安全水準について（機能安全—SIL/PL に関する概要の説明）

1　機能安全とは

この節では、機能安全の基礎的な事項をまとめる。

(1)　機械の機能安全に関する規格とその概要

機能安全という用語がよく使われるようになってきた。機能安全に関する定義は1(2)で示すが、例えば、「安全のために、主として付加的に導入された、コンピュータ等の電子機器を含んだ装置が、正しく働くことによって実現される安全を"機能安全"と言います」[1]と説明されている。つまり、制御システムを用いて実現する安全という意味で使われている。したがって、機械分野だけでなく、化学プラント、ロボット、鉄道、自動車など多くの分野で使われる技術を示す術語である。また、この術語はIEC 61508によって広く知られる用語となった。一方、機械安全、労働安全等は、検討対象を示し、その領域での安全の意味で、技術（方法論）を示す用語ではない。機械安全の中は、機能安全による部分もあれば、構造計算を行って十分な強度を持たせることで実現する安全もある。

機械分野に関する機能安全を規定する規格としては、次の2規格が基礎的な規格である。

- 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

  ISO 12100をA規格とする機械安全規格の体系内のB規格として位置付けられている。制御システムで機能的安全を扱う際に参照される規格で、安全機能を達成する度合いをパフォーマンスレベル(Performance Level、以下PL)として、5段階（PL=a～e）に区分している。

- 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

  次に示すIEC 61508の傘下の機械安全分野のセクター規格で、機能安全の達成度合いを安全インテグリティレベルSIL(Safety Integrity Level、以下SIL)で3段階（SIL1～3）に区分している。上記の機械安全規格体系のB規格にも位置付けられている。

なお、ここで出てきたIEC61508の概要を次に示す。この規格はISO 13849においても、ソフトウェアーに関しては一部でIEC 61508を引用した規定がある。

- IEC 61508 電気・電子・プログラマブル電子安全関連系の機能安全

IEC 62061 の上位規格に位置付けられ、広い分野で使われる電気・電子・プログラマブル電子による機能安全の基礎を与えている。この規格は広範な分野で適用されるため、SIL を SIL1～4 の 4 段階に区分している。

これら規格を基礎として、光カーテンの規格などパフォーマンスレベル(PL)や安全度水準(SIL)を規定している B 規格を表 1 に示す。また、多くの機械の C 規格では安全要求で制御システムの安全関連部に機能を割り当てており、そこでは要求パフォーマンスレベル PLr あるいは要求 SIL を規定している（PLr, SIL については後述する。）。（表 2）

表 1　ISO 13849 あるいは IEC 62061 を引用している B 規格例

IEC 61496 機械類の安全性―電気的検知保護設備

表 2　ISO13849 あるいは IEC62061 を引用している C 規格例

ISO 10218-1 ロボット及びロボティックデバイス―産業用ロボットのための安全要求事項―第 1 部：ロボット
ISO 12643-1 印刷関連機器及びシステムに対する安全要求事項－第1部：一般要求事項
ISO 23125　工作機械―安全性―旋盤

C 規格における上記 PLr の規定として ISO 12643-1 の例を表 3 に示す。

表 3　ISO 12643-1 における PLr 及び要求 SIL の要求記載例

5.3.6 Hold-to-run controls ＜途中省略＞ b) with displacement limited to a maximum of 75 mm or with a maximum operating speed of 5 m/min where the measures defined in a) would reduce the ability of the machine to perform its function and where there would be no substantial increase in risk. Safety related parts of control systems of interlocking guard systems for the safety reduced speed/displacement limited condition shall comply with at least ISO 13849-1, PL d or IEC 62061, SIL 2. Safety related control systems (including selector switches relays and PLC circuits) that allow interlocked areas to be operated independently shall comply with at least ISO 13849-1, PL b or IEC 62061, SIL 1. ＜ISO 12643-1＞

つまり、ISO 13489 や IEC 62061 で、達成できるリスクの低減の度合いのレベル（PL や SIL）毎の技術要件と安全機能毎に求められるレベルの決め方（例えば、PLr

や要求 SIL をリスクグラフ法等で求めること。4参照。）を規定し、個別の機械の規格では、その機械で必要な安全機能毎に適切なレベル（PLr や要求 SIL）を規定している。

(2) 規格に見る機能安全の定義

機能安全という術語は IEC 61508 で次のように定義されている。

機能安全：EUC[1]と EUC 制御系[2]の全体に関する安全の内、E/E/PE[3]安全関連系[4]、他技術安全関連系及び外部リスク軽減施設の正常な機能に依存する部分

この定義から分かるように、機能安全には、他技術安全関連系及び外部リスク軽減施設の機能によるものも含まれるので、電気/電子/プログラマブル電子技術によるものだけではない。機械に当てはめて言い換えると、「機械自体と機械の制御装置全体に関する安全の内、電気回路/電子回路/プログラマブル電子回路(PLC など)の安全装置、リリーフ弁などの安全装置、周囲の柵の正常な機能に依存する部分」となる。

しかし、一般には、機械の電気/電子/プログラマブル電子の制御による安全を対象として使われている。また、機能安全は安全に関する規定であって、機械そのものの機能に関する制御に関する規定ではない。そこで、本報告書では次のように考えることとする。

機械の目的のための制御システム以外に付加される制御システムの部分で、安全を実現する部分で実現する安全機能を機能安全と呼んでいるようである。また、IEC 62061 を基に実装する安全を機能安全、ISO 13849 を基に実装する安全を制御安全と区別する例や、CPU やそれを用いた PLC（プログラム可能なロジックコントローラ）を用いたものを機能安全として、リレーなどを用いたものを除外する区分の例もあるが、この報告書では、適用規格、CPU や PLC 使用の有無による区別はせずに、機械の制御システムの一部（安全関連部）の機能で実現するものを機能安全と考えることにする。なお、ISO 13849 が扱う油空圧による制御システムも安全関連部の機能によるものも含む。

---

[1] 被制御系（EUC, Equipment under Control）：製造、プロセス、輸送、医療、その他の業務に供される機器、機械類、装置、プラントなど。

[2] EUC 制御系：プロセス及び/又は運転員からの入力信号に応答して、EUC を望ましい方法で運転するための出力信号を生成するシステム

[3] E/E/PE (Electric/Electronic/Programmable Electronic)：電気及び/又は電子及び/又はプログラマブル電子技術に基づく

[4] 安全関連系(Safety-related System, SRS)：次のようなシステム：—EUC を安全な状態に移行させるため、又は EUC の安全な状態を維持するために必要な安全機能を行い、かつ、—それ自体で、若しくは、その他の E/E/PE 安全関連系、他技術安全関連系、又は、外的リスク軽減施設と協調して、要求される安全機能に対して必要な安全度水準を達成する（図 1）。

ここまでに何回か出てきた用語「安全機能」は、「E/E/PE 安全関連系、他技術安全関連系又は外部リスク軽減施設によって遂行される機能。この機能は、特定の危険事象に対して EUC にかかわる安全な状態を達成又は保持する。」（IEC 61508）と定義されている。

なお、ISO 12100 と ISO 13849 では、機能安全という用語は使われていない[5]。安全機能は「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。」と定義されている。

(3) 制御システムの安全関連部

安全機能を担う制御システムの部分を、IEC 62061 においては安全関連電気制御システム（SRECS (Safety-related electrical control systems) ）と称し、ISO 13849 では制御システムの安全関連部（SRP/CS (safety-related parts of a control system) ）と称する。これらは、IEC61508 においては、**図 1** に示す安全関連系に相当する。これらの部分を以下、安全関連部と記述する。安全関連部は、機械の本来の機能（例えば生産のために機械の軸をある一定回転数で回転させる、あるいは増減速させる）から分離していることが基本である。プレスの前面の光カーテンにより、上型の下降中に作業者の身体の一部が侵入した場合に、これを検知して停止させる例は分離しているが、プレスの両手押しボタンのように運転機能と一体になっているものもある。いずれにしても、安全関連部の担う安全機能を明らかにし、安全関連部を特定することが大切である。また、PL あるいは SIL は機能安全にかかる部分にのみ適用されるもので、生産のための制御システムの評価には適用されない[6]。

2 保護方策の中の機能安全の位置付け

(1) リスクアセスメントから導かれる保護方策

---

[5] ISO 13849 内に一カ所「SRP/CS の機能安全に対しては，特に，イミュニティが関連する。製品規格が存在しない場合，少なくとも，JIS C 61000-6-2 のイミュニティの要求事項に従うことが望ましい。」と記述されている箇所がある。

[6] 機械の故障は点検作業を要するなどリスクを増大させる要因である。したがって、機械のコンポーネントの一つである制御システム（機械の運転にかかる部分、安全機能にかかる部分の両者とも）の信頼性の向上は、本質的安全設計方策の一つとして規定されている（ISO 12100，6.2.13）。

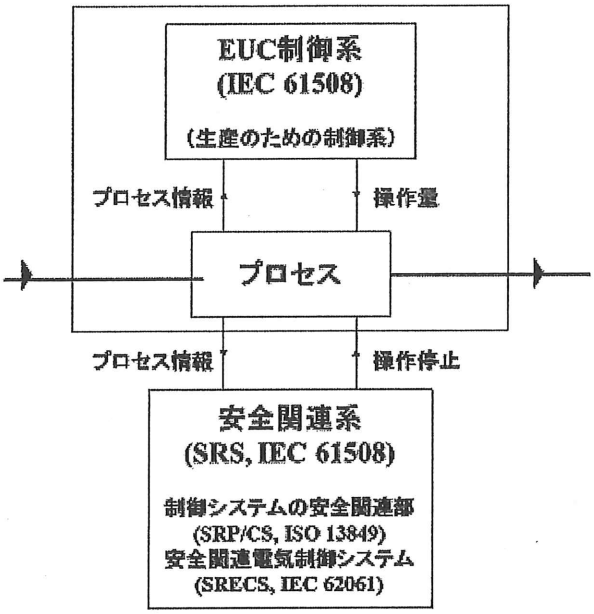


図１　IEC 61508 機能安全規格で示される安全関連部

番号	危険源(ISO14121附属書A参照)		危険箇所	据え付け時・通常使用時・点検保守時・交換時・廃棄時・その他( )													対策実施後の評価	残留リスク	備考
				作業内容	危険事象	使用形態	現状					対策実施後							
				(工程)			頻度	被害の大きさ	リスクレベル	対策の要否	対策	頻度	被害の大きさ	リスクレベル					
	危険源、危険状態及び危険現象																		
6	1.1	押しつぶしの危険源	本体	設置されている状態で、本体の周辺で他の機械による作業を行う	電源ケーブル、ホースなどが他の機械や自動車などに引っ掛かり、本体が転倒し、側にいた人が下敷きになる	通常	Ⅳ	B	Ⅱ		本装置のみの対応でない。							
7			本体	設置されている状態	設置面が傾斜しており、何らかの操作中に本体が転倒し、人が下敷きになる	誤使用	Ⅳ	B	Ⅱ	対策済み	仕様で水平に設置することを指示している。取扱説明書で、設置面の傾斜限度・設置方法及び、運搬中の傾斜限度(15°)を指定する。							重さ、重心の計算、吊り方について別紙(TCF_****_001)参照(TCF_0710_001)
8			フタ昇降部、取っ手で引く部分	食材出し入れ	指を挟む	通常	Ⅱ	C	Ⅰ	必要	投入口カバーが所定位置にないと、油圧ポンプに給電されないようにする(災安全機能(b、D'))	Ⅳ	C	Ⅱ				安全機能一覧及びPL計算書(TCF_****_005)
9			投入口カバー	投入口カバーを閉める	手で投入口カバーを閉める際に、指を挟む	通常	Ⅱ	D	Ⅰ	必要	投入口カバーに注意書き表示	Ⅱ	D	Ⅰ				投入口カバー回路(***)参照

図２　リスクアセスメント例(抜粋)

機械を設計する際にはリスクアセスメントを行い、その機械が内在する危険源を同定し、更にリスク低減方策を、本質的安全設計方策、安全防護及び付加保護方策、使用上の情報（の提供）の順で実施する。図 2 はある装置のリスクアセスメントの例であるが、まず危険源が同定され、それに伴う危険状態・危険事象が示され、安全方策をスリーステップメソッドの従って検討し、この例では制御システムの安全関連部で対処する方策が上げられている。その後、要求パフォーマンスレベル PLr がリスクグラフ法により決定され、回路が設計され、その回路のパフォーマンスレベル PL が PLr を満たしているか（PLr≧PL）の確認を行う（5 参照）。なお、PLC 等を用いた場合には、ソフトウェアについても検証を行う。

ここで注意しなければならないことは、リスクアセスメントで同定されない危険源・危険状態に対しては何ら保護方策が用意されず、無防備であるということこと、保護方策はスリーステップに従って検討を進めることである。つまり、初めから機能安全があるのではない。

3　機能安全の実例と基本構造

(1)　機能安全規格の適用事例

図 3[2)]は自動化されたダイカストマシンシステムに適用される機械安全規格を示している。この中で、インターロックガードの安全要求事項、両手操作起動装置、非常停止、セーフティ・ライトカーテン、圧力検知マットの安全要求事項、予期しない起動の防止、E/E/PE 安全関連系の機能安全、制御システムの安全関連部の規格は機能安全の規格である。

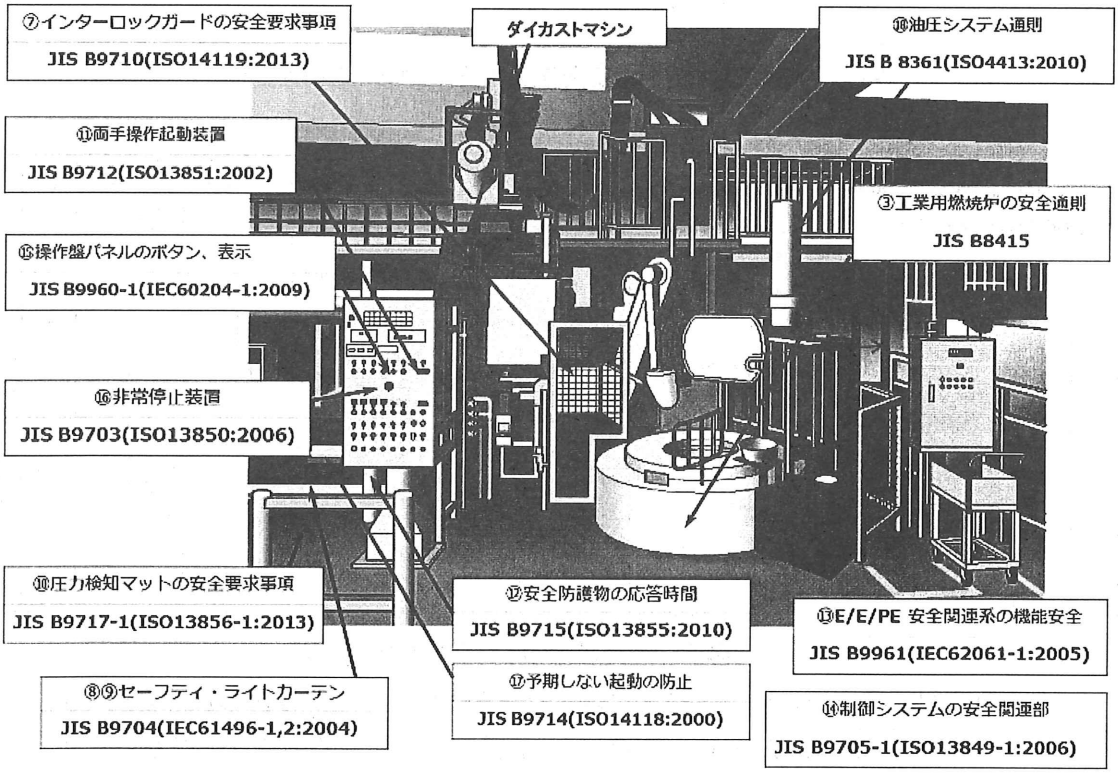


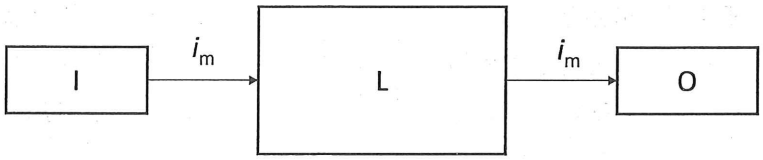
図３　機能安全の適用例　ダイカストマシンシステム

(2)　機能安全を担うハードウェアの基本的な構造

図 4 は ISO 13849 が示す制御システムの安全関連部の基本構造である。この構造は、IEC 62061 が示す安全関連電気制御システムにおいても同じである。入力装置をセンサ部、出力装置を最終要素と呼称している。入力装置は機械や人の状態を知るもので、ドアーに付いているスイッチ（ガードの開閉を検知している）、論理は機械の運転の可否を判断する部分で、PLC であることもリレーであることもあるし、コンタ

クタで次の出力装置の役割も担っていることもある。出力装置は、例えばモータへの動力を開閉するコンタクタである。実際には、I-L-O が冗長化されたり、試験装置が外付けされたりしている。

制御システムの安全関連部の例を ISO 13849-1 の附属書 I、図 I.3 に示されているインターロック付きガード装置で示す（図 5)。このインターロック付きガードの安全機能は、ガードが開状態では運転できないこと、機械が運転中にガードが開かれたら直ちにモータへの通電を断とすることである。



記号の説明
i_m　相互接続手段
I　入力装置，例えば，センサ
L　論理
O　出力装置，例えば，主接触器

IEC 61508 においても同じ構成であるが I をセンサ・入力インターフェース部(Sensor and Input Interface)、O を出力インターフェース・最終要素（Output Interface and Final Element）と呼称する。

図４　制御システムの安全関連部

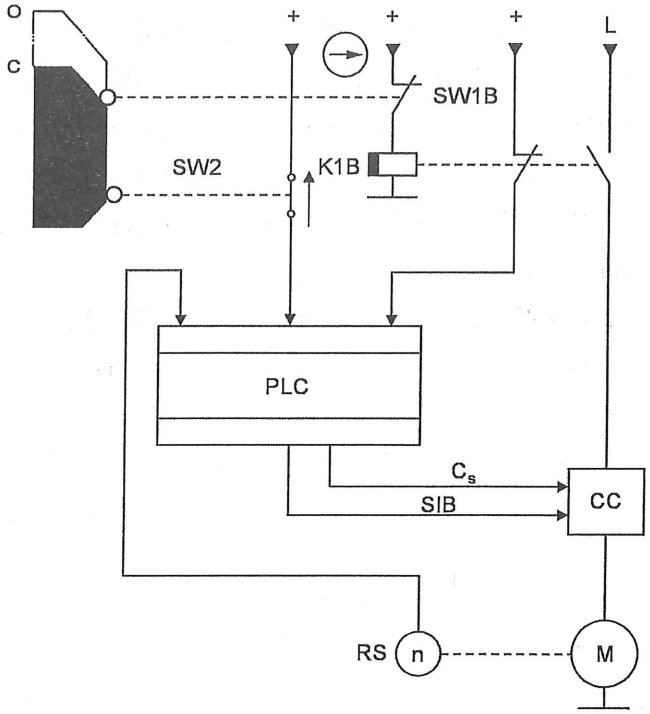


図５　インターロック付きガード

4　PL、SIL の定義

安全関連部の PL あるいは SIL は、安全機能の危険側故障確率で定義されている（表 4、表 5)。しかし、これ以外にも、PL であればアーキテクチャー、診断範囲、共通原因故障への配慮、SIL であれば安全側故障比率、共通原因故障、ハードウェアフォールトトレランスの評価・制約がある。実務における設計では、各規格を参照することが必須である。

表 4　PL の定義

PL	単位時間当たりの危険側故障発生の平均確率（PFH_d）　[1/h]
a	$10^{-5} \leqq PFH_d < 10^{-4}$
b	$3\times10^{-6} \leqq PFH_d < 10^{-5}$
c	$10^{-6} \leqq PFH_d < 3\times10^{-6}$
d	$10^{-7} \leqq PFH_d < 10^{-6}$
e	$10^{-8} \leqq PFH_d < 10^{-7}$

表 5　SIL の定義

安全インテグリティレベル	1 時間当たりの危険側故障確率（PFH_D）
SIL1	$10^{-6} \leqq PFH_D < 10^{-5}$
SIL2	$10^{-7} \leqq PFH_D < 10^{-6}$
SIL3	$10^{-8} \leqq PFH_D < 10^{-7}$

5　PLr、要求 SIL の決定法

安全関連部の PL あるいは SIL は、安全機能で防護しようとする危険事象のリスクの応じて決めることは合理的であるが、具体的にどの様に決定するかは、二つの場合がある。

第一の場合は、表 3 で示したように C 規格で規定があれば、それが設計する機械においても妥当か確認した上で、規格の規定の要求に従った PL あるいは SIL とする。ただし、C 規格はその規格のスコープの機械であっても、そのすべての危険源に対する保護方策を示したものではないこと、保護方策を示しているものであっても、それは「標準的な機械」に対する保護方策であることを理解し、その機械に対するリスクアセスメントを行うことは不可欠である。

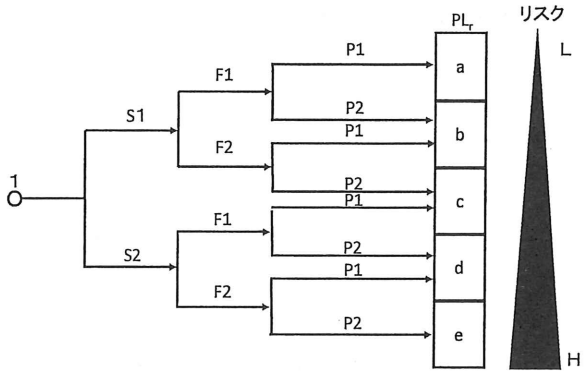
第二の場合は、リスクグラフ法等、規格が例示している手法により、適切な PL あるいは SIL を決め、それを満足する安全関連部を設計し、最後のその要求を満たしていることを確認・検証する。

ISO 13849-1 では、リスクグラフ法で PLr を求める手法を、”参考”として例示している。IEC 62061 では、ハイブリット法で要求 SIL を決定する方法を、同じく”参考”として例示している。

(1)　ISO 13849-1 に示されるリスクグラフ法

この規格では、附属書 A において安全関連部が有すべき PL である PLr の求め方としてリスクグラフ法を示している。図 6 の 1 を起点として、当該危険源が顕在化したとしたら想定される危害のひどさ、危険源への暴露の頻度及び/又は時間、危険源回

避又は危害の制限の可能性をそれぞれ選びながら右に進み、最後に PLr が求められる。



1 リスク低減に安全機能の寄与度を評価するための開始点

L リスク低減への寄与度“低”

H リスク低減への寄与度“高”

PLr 要求パフォーマンスレベル

S 傷害のひどさ

S1 軽症(通常，回復可能な傷害)

S2 重傷(通常，回復不可能又は死亡)

F 危険源への暴露の頻度及び／又は時間

F1 まれ～低頻度，及び／又はさらされる時間が短い

F2 高頻度～連続，及び／又はさらされる時間が長い

P 危険源回避又は危害の制限の可能性

P1 特定の条件下で可能

P2 ほとんど不可能

図６　リスクグラフ法による PLr の決定

(2)　IEC 62061 に示されるハイブリット法

この規格では、附属書 A において割り付けられるべき SIL の求め方として危害のひどさのポイント（表 6）と危害の発生確率に関するさ 3 要素のポイント（表 7、表 8、表 9）を加算した結果を用いて、表 10 のマトリクスで SIL を求める方法を示している。

表 6　危害のひどさ（*Se*）の分類

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

表 7　暴露レベル（*Fr*）の分類

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

表 8　発生確率（*Pr*）の分類

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

表 9　危険を回避又は限定できる確率（*Av*）の分類

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

表 10　SIL 割付けマトリクス

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

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

6　PL, SIL 計算法

回路設計を行った後、その安全関連部の PL あるいは SIL を決定しなければならない。それは大別して、計算による部分と管理による部分がある。後者はソフトの開発のプロセスの管理である。

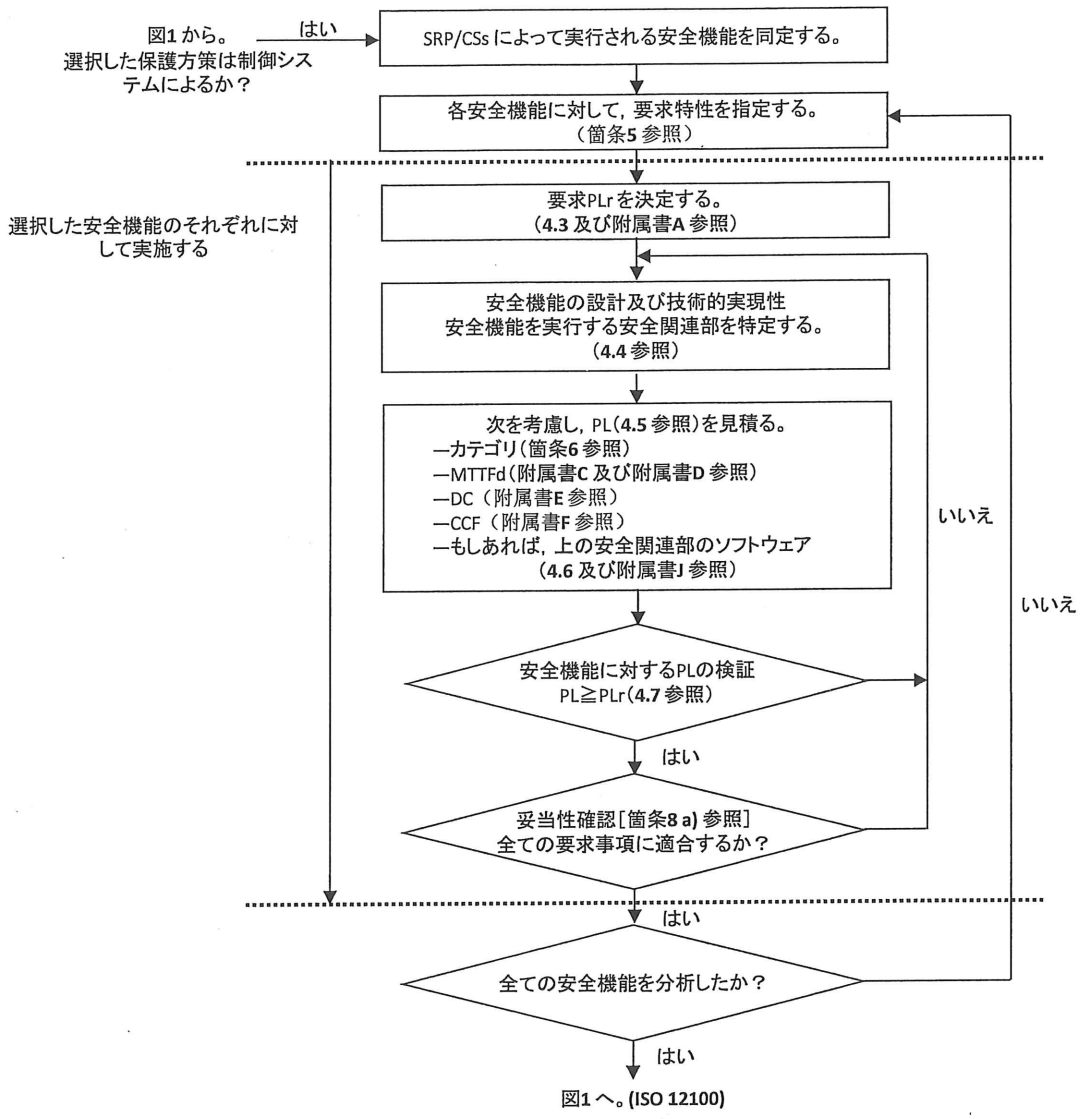
先ず、計算により危険側故障率の計算について、その流れを記述する。

(1)　PL の計算による求め方

図 7 に PL を求めるフローを示す。これは、ISO 13849-1 の図 3 として示されているものである。

アーキテクチャーは安全関連部の構成（構造）及びシステム挙動に対する要求事項で 5 カテゴリー、$MTTF_d$ は危険側平均危険側故障時間で表 11 に示す 3 段階、DC は診断範囲でこれの平均である DC_{avg} で表 12 に示す 4 段階に分けられ、図 8 の要件を満たすことが求められる。

CCF は共通原因故障に関するスコアーで、PL_d～PL_e では規定のポイント以上であることが求められる。



ISO 13849-2で，妥当性確認のための追加的支援策が示される。

図7　PLを求めるプロセス

表11　各チャネルの平均危険側故障間隔

$MTTF_d$	
各チャネルの指定表示	各チャネルの範囲
低	3年≦$MTTF_d$＜10年
中	10年≦$MTTF_d$＜30年
高	30年≦$MTTF_d$＜100年

表 12　診断範囲

DC	
*DC*の指定表示	*DC*の範囲
なし	*DC*＜60%
低	60%≦*DC*＜90%
中	90%≦*DC*＜99%
高	99%≦*DC*

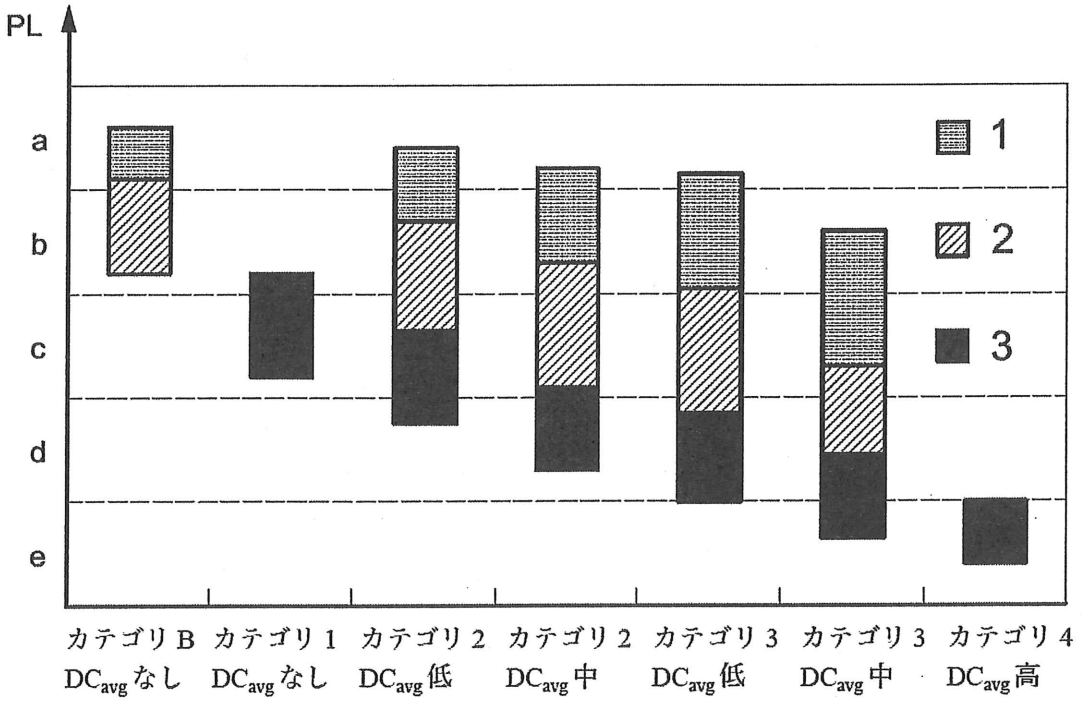


図８　カテゴリー、DCavg、各チャネルの MTTFd と PL の関係

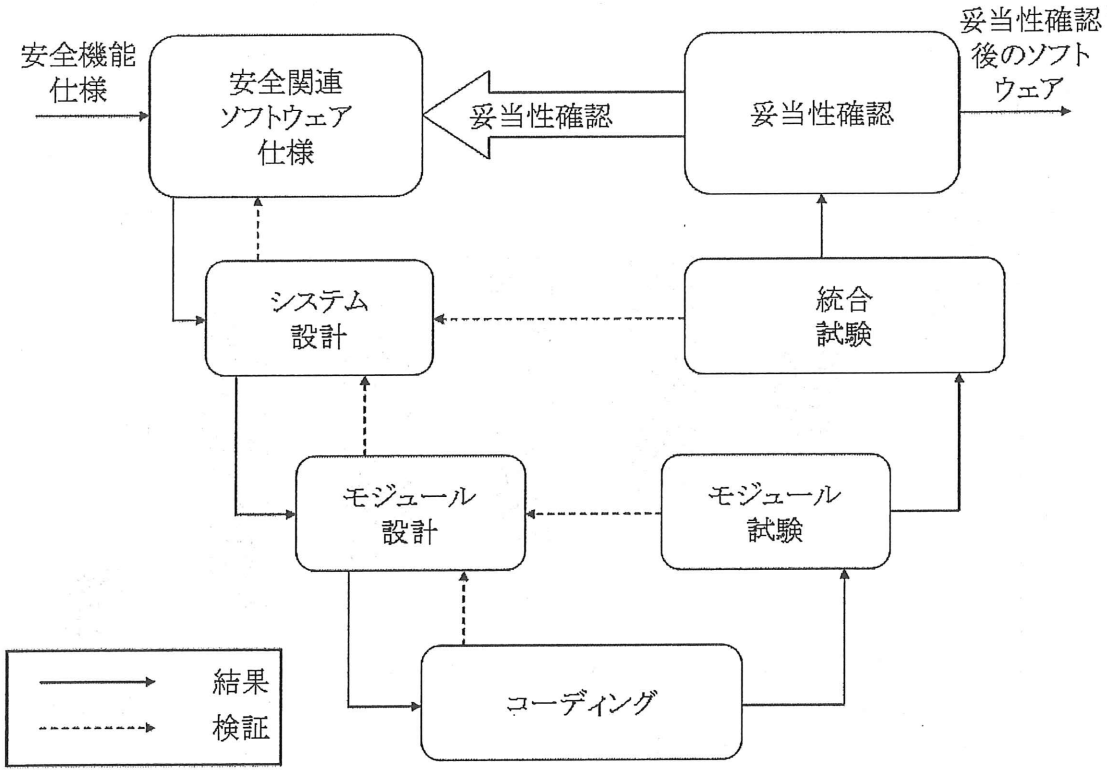
(2)　SIL の計算による求め方

ISO 13849 が簡単化した手法を提示しているのに対し、IEC 62061 の SIL の計算は、各要素の故障の発生が指数分に従うと仮定して、信頼性工学の理論から求めることを基礎としている。直列系アーキテクチャーの故障率は構成する各コンポーネントの故障率の和で求められる。並列系では、故障率λ_1とλ_2のコンポーネントが並列になると、系としての故障率は$\lambda_1\lambda_2 T$（Tはプルーフテスト間隔）となる。これに、更にプルーフテスト間隔、共通原因故障の発生、診断の効果を加味している。プルーフテストは定期的に行う機能試験で、すべての不具合が検出できると、規格の上では仮定している。

この点について、IEC 62061 の翻訳規格である JIS B 9961 の解説に詳しく記述されている。

(3)　ソフトウェアの管理

論理部にPLC等を用いる場合にはソフトウェアも安全担保の重要な要素となる。しかし、ソフトウェアの故障はハードウェアのようにランダム故障（ある分布に従って発生する故障）ではなく、ある条件がそろったときに不具合が顕在化するという系統的故障となる。そのため、故障率等の信頼性の指標では評価できない。一般には、図9に示すVモデルで進め、またソフトウェアの検証を行う個人、部署、組織をSILに応じて選択すること等で管理することを求めている。



注記　附属書Jに，ライフサイクル活動に対してより詳細な推奨事項を示す。

図9　ソフトウェア開発のVモデル

(注) 本章は，報告書を読む際に必要な基本的な事項をまとめたもので、この解説で機械の安全関連部の設計はできない。

参考文献

1) 日本規格協会：機能安全の導入と教育の進め－安全・安心とグローバル展開促進のために，日本規格協会パンフレット (2014)

2) 中央労働災害防止協会：機械安全規格を活用して労働災害を防ごう，中央労働災害防止協会パンフレット (2015)

Ⅱ　ボイラーの制御装置の安全関連システムの性能と取扱規制について
－欧州連合におけるボイラーの事例－

1　欧州における機能安全に関する法制度

(1) EU 事務局（EC）では、EU 加盟国に立法を指令する EC 指令を作成するが、その中に、ニューアプローチ指令がある。これは、EU 域内での規格や規制を整合化して、域内での技術的貿易障壁を撤廃することが目的となっており、EU 域内で流通する製品には、CE マーキング表示で指令への適合を示すこととされている。

(2) このニューアプローチ指令には、以下の指令など、22 の指令がある[1]。

ア　低電圧指令（2006/95/EC）

イ　EMC 指令（2004/108/EC）

ウ　機械指令（2006/42/EC）

エ　ガス機器指令（2009/142/EC）

オ　防爆機器指令（ATEX/ 94/9/EC）

カ　圧力機器指令（97/23/EC）（2014/68/EU により改正。2016 年７月より適用）

(3) 製品に CE マーキングするためには、製品が該当する全ての指令に適合することが必要であり、通常は、各指令に定められている製造規格（EN 規格）へ適合を確認する必要がある。適合確認の方法は、自らが規格への適合を宣言する方法（自己宣言）、認証機関（Notified Body）による基準適合の証明（第三者認証）などの方法があり、各指令にどのような確認を行う必要があるか規定されている。

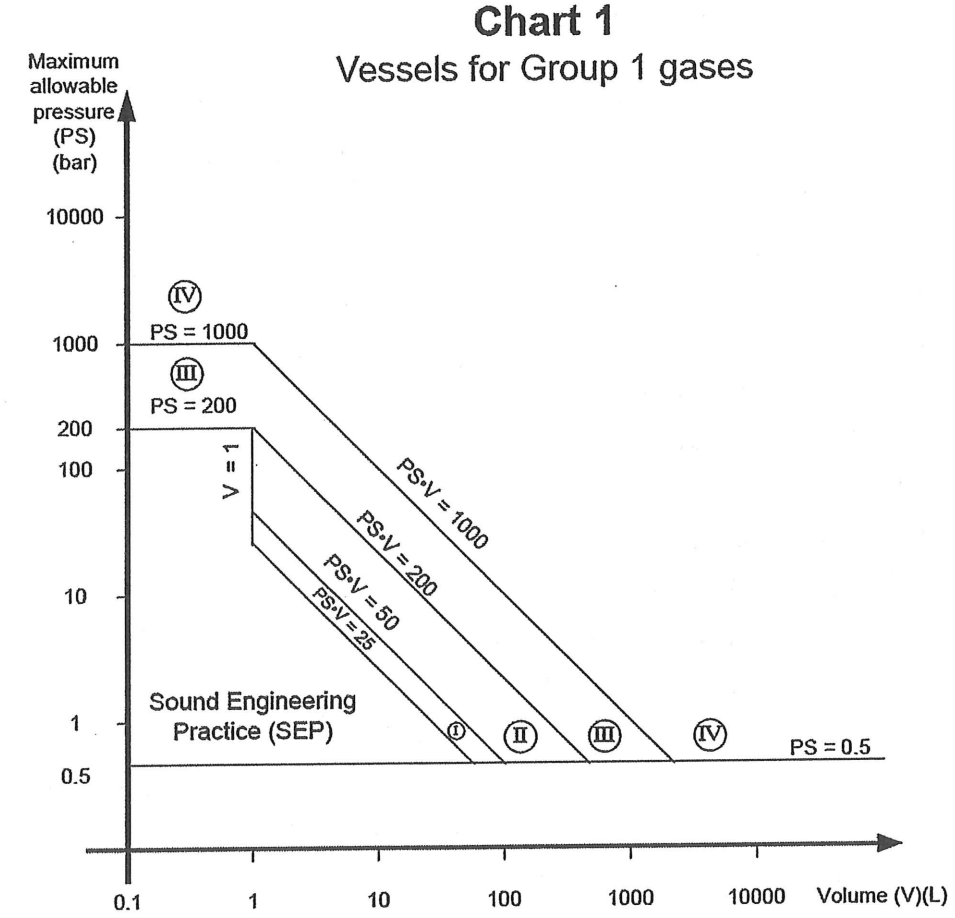
2　ボイラーに関する適合性評価の方法

(1) ボイラーの場合、圧力機器指令（Pressure Equipment Directive, PED）[2]第９条により、内包物の性状（グループ１が爆発物、グループ２がそれ以外）及び機器ごとの使用圧力や容積等に基づき、付属書 II に定める図に従い、機器ごとにⅠからⅣのカテゴリーに分類される。（**図１**参照。）

(2) さらに、PED 第 10 条に基づき、各カテゴリーで必要となる適合評価の方法が定められる。（**表１**、**表２**参照[3]。）カテゴリーⅠのみが自己認証によることが可能であり、カテゴリーⅡからⅣについては、認証機関（Notified Body）の認証が必要とされている。

(3) 各国政府は、カテゴリーⅡからⅣの圧力機器 PED 付属書Ⅰ（Essential Safety Requirements）のセクション 3.1.2 に定める溶接の方法及び溶接者、3.1.3 に定める非破壊検査の要員の承認（approval）のために、認定第三者機関(Recognized Third-party Organizations)を指定することができる。（PED 第 13 条）

(4) また、モジュールA1, C2, F, Gについては、ユーザー監督者(user inspectorates)が監査することができる（PED 第 14 条)。これは、設備の使用者（運用者）が作った団体の資格者が、設備の内部監査を行う趣旨のようである。



Exceptionally, vessels intended to contain an unstable gas and falling within categories I or II on the basis of Chart 1 must be classified in category III

図１　圧力機器のカテゴリー分けの図の例（PED 付属書Ⅱ Table. 1）

表１　カテゴリーごとの規格適合の確認方法のモジュール分類

Category I	Category II	Category III	Category IV
Module	Modules	Modules	Modules
A	A1	B1 + D	B + D
	D1	B1 + F	B + F
	E1	B + E	G
		B + C1	H1
		H	

表２　各モジュールの適合性評価方法

Module	Design	Production
A	Technical documentation	Internal production control
A1	Technical documentation	Internal production control with monitoring of the final assessment
B	Type examination	
B1	Design examination	
C1		Monitoring of final assessment
D		Quality assurance for production, final inspection and test
D1	Technical documentation	Quality assurance for production, final inspection and test
E		Quality assurance for final inspection and test
E1	Technical documentation	Quality assurance for final inspection and test
F		Product verification
G	Unit verification	Unit verification
H	Quality assurance for design,	manufacture, final inspection and test
H1	Quality assurance for design, with design examination and	manufacture, final inspection and test monitoring of final assessment

3　圧力容器指令と整合規格

(1) PED は、2002 年５月 29 日から施行されている（2014/68/EU により改正。2016 年７月より適用)。PED に適合することが求められる整合規格（EN 規格）は、官報でリストが公示されており、最新のリスト(2014/C 313/02)は、2014 年に更新された[4]。ボイラーについては、EN12952 シリーズ（水管ボイラー)、EN12953 シリーズ（丸ボイラー）が主なものである。（このリストには、電気系の機能安全に関する規格（CENELEC）は引用されていない。）

(2) 個別機械安全規格（C 規格）である EN12952, EN12953 いずれについても、安全保護システム(protective system)については、グループ安全規格（B 規格）である EN50156-1（炉と付帯設備のための電子機器）及び IEC/EN61508 に適合することが求められている。2015 年７月に EN50156-1 は改正され、同時に、EN50156-2 が新規制定された。

4　ボイラー関連 EN 規格における機能安全

(1)　EN50156-1:2015 では、安全関連システムの設計では、以下の要求事項がある（10.5.2）

ア　安全関連システムでは、故障アセスメントの手順に基づく故障解析を行う。

イ　安全装置の設計と型式認証は、EN50156-2 に従い、安全関連システムの設計で

は、EN50156-2 に従ったサブシステムや機器を使用する。

(2) EN50156-2:2015 では、安全関連システムの安全機器とサブシステムの要求事項は以下のとおり。

ア　安全関連システムの安全機能は、関連製品規格の要求事項に合致する必要がある。関連規格に合致すれば、SIL レベルの決定は要求されない（**図２**参照）。関連規格としては、C 規格である EN12592-11:2007（水管ボイラのリミット機器）、EN15953-9:2007（丸ボイラのリミット機器）などが含まれる。対応する C 規格がない場合は、機能安全については、B 規格である IEC/EN61508 シリーズに適合する必要があり、要求安全度水準（SIL）の設定が必要である。

イ　安全関連システム内の電気システムに接続される機械式、液圧、空圧機器は、関連 C 規格に適合する必要がある。関連 C 規格としては、EN12592-11:2007（水管ボイラのリミット機器）、EN15953-9:2007（丸ボイラのリミット機器）などが含まれる。C 規格の適用範囲からはずれている場合でも、可能な限り製品規格の安全要求を考慮することになっている。

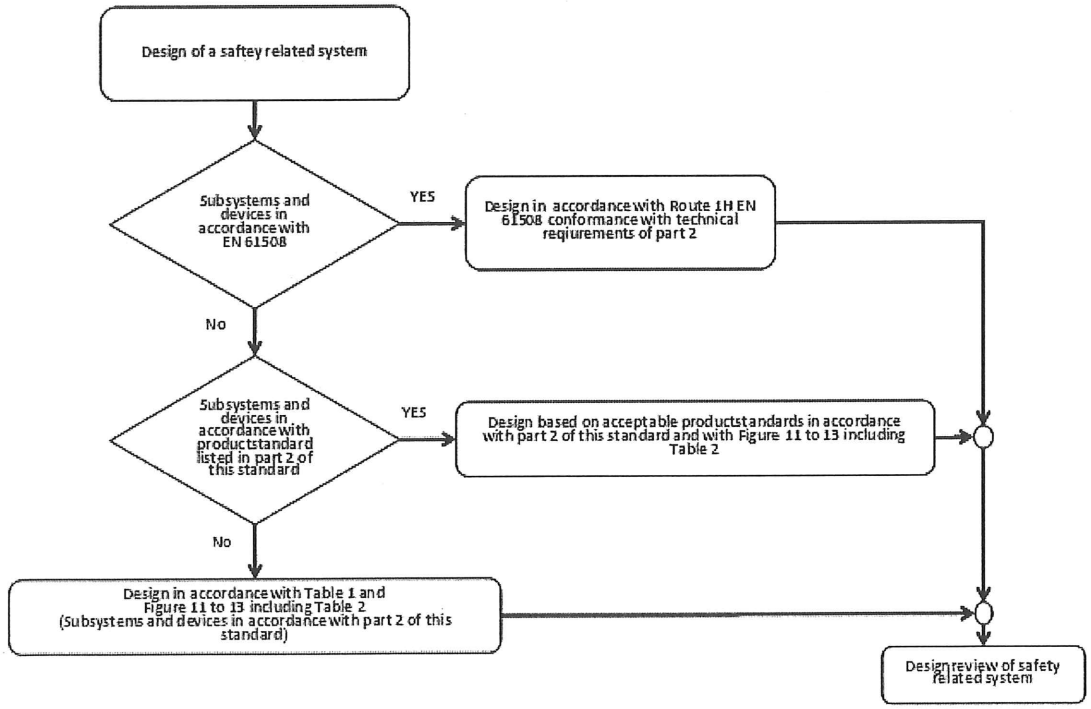


図２　設計原則の選択（EN 50156-1:2015 Figure.10）

５　取扱規制と機能安全の関係：英国におけるボイラー規制の事例

EN 規格は、ボイラーの製造上に満たすべき内容を定めたものであり、ボイラーの運転や点検といった取扱規制は、各国の労働安全衛生関係法令により、独自の規制がなさ

れている。ここでは、英国におけるボイラーの取扱規制について紹介する。

(1) 英国のボイラー取扱規制の法制度

ア　英国の労働安全衛生法（Health and Safety at Work Act 1974 (HASWA)）においては、事業者に対して、情報提供、指示、教育及び監督について、合理的に実施可能な範囲内で（so far as is reasonably practicable）、事業者に措置の実施を義務づけている。

イ　この「合理的に実施可能」の判断基準として、各種のガイドラインが定められており、ボイラーについては、CEA（Combustion Engineering Association）がHSE の承認を得て作成したガイドライン(BG01)[5]に定められた事項と同等以上の対応が求められる。

(2) 機能安全のレベルに応じた、ボイラーの監視・点検等のレベル分け

ア　BG01 では、自動化されたボイラーの制御配備（control arrangement）レベルを４つの配備（arrangement）に分けている。（**表３**参照）

イ　これをみるとわかるように、英国では、すでに使用されているボイラーについては、必ずしも EN 規格に適合することが求められておらず（適用除外）、規格への適合状況や、制御装置の安全度に応じて、資格者の配置場所、点検頻度などにレベル分けがなされている。具体的には、NE12953 に不適合の場合（配備１）については、資格者をオンサイトに常駐させることを求める一方、EN 12953 等の個別規格に適合している場合（配備３）や、EN61508 に基づく要求 SIL に適合している場合（配備４）については、自動運転を認めた上で、点検頻度は３日に１回とされている。

表３　英国におけるボイラーの取扱規制

（CEA2011, Guidance on Safe Operation of Boilers より作成）

配備	対象ボイラ	人員配置 (Attendance)	機器の安全度 (Equipment integrity)
配備1	最も低いレベルの自動化。EN12953に不適合。	ボイラ運転者をオンサイトに常駐（警報に対して直ちに対応可能）	制御機器はフェールセーフになっていること
配備2	● ボイラの警報を人員が常駐している警備員室等から遠隔パネルにより監視すること。 ● 新たな設置については、EN12953に適合するべきであり、追加のリミット機器が装備されること。	● 適切に教育・指示された者オンサイトに常駐（警報に対応できること）。 ● この者は、最低限、ボイラが安全に運転されているかを確認でき、異常をボイラ運転者に知らせることができること。 ● ボイラ運転者は、最低限、毎日ボイラをチェックすること。	● 高い信頼度の最低水位検出機器を装備。 ● 全ての制御機器がフェールセーフであること。
配備3	● 最高レベルの自動化（例：オンサイトにボイラ運転者が非常駐であり、運転状況が遠隔監視室又はテレメトリーシステム（遠隔監視機器）により監視。 ● 新たな設置については、EN12953に適合するべきであり、追加のリミット機器が装備されること。 ● 追加機器が装備されていない場合、リスクアセスメントを実施し、必要な他の制御手法によりサポートされていなければならない。	● 少なくとも3日に1回（リスクアセスメントにより別途指定される場合を除く）、ボイラ運転者によって点検を受けること。 ● ボイラの運転状況は、オンサイト又はオフサイトで監視される。	● ボイラの制御及び機器について、最も高い信頼性(greatest degree of confidence)を要求される最も高いレベルの自動化であること。 ● 低水位レベル検出機器は高い信頼度(high-integrity)であること。 ● 全ての制御機器がフェールセーフであること。
配備4	● 外部に圧力発生器を装備した温水システム。 ● 新たな機器については、人員配置や遠隔監視のレベルに関する情報をサプライヤーに伝達すること。 ● 複雑な電気制御システムについては、それぞれの安全機能(safety function)に割り当てられたSILにより、安全機能に貢献するために使用されるモニタリングのデバイスやシステムの選択やそれをどのように適用して運用、試験するのかについて決定すること。	● 少なくとも3日に1回（リスクアセスメントにより別途指定される場合を除く）、ボイラ運転者によって点検を受けること。 ● ボイラの運転状況は、オンサイト又はオフサイトで監視される。	● （リスクアセスメントによって別途指定されていない限り） ● 全ての制御機器がフェールセーフであること。 ● 低水位リミッターは、高い信頼度であり、手動の試験施設により自己モニタリング(self-monitoring)されていること。

６　取扱規制と機能安全の関係：ドイツにおけるボイラー規制の事例

(1)　ドイツのボイラー取扱規制の法制度

ア　ドイツにおいては、製造物責任法（ProdSG）に基づく規則として、作業用機械使用規則（BetrSichV）がある。その具体的な内容を規定した技術基準（義務規定ではなく、指針としての位置づけ。）として、機器使用安全技術規則（TRBS）が定められている。

イ　TRBS のうち、蒸気ボイラーと圧力装置の危険に関する規則（TRBS 2141）の Part. 1 に詳細な規定がある。ここでは、最近の改正により、無人運転可能な期間（点検頻度）を 72 時間と規定している。

(2)　既存のボイラーに対する TRBS の適用

ア　昨年実施された厚生労働省からのドイツの規制当局へのヒアリングによると、TRBS 2141 においては、最先端（state of the art）の基準に合致することが求められているが、TRBS はそもそも、運転時の規制であることから EN 規格に適合することは求められていないこと、さらに、TRBS が規定しているのは機械的安全性であり、制御システムや安全関連システムについて詳細な規定があるわけではないため、安全関連システムに最新の EN 規格に適合することを求める趣旨ではないとのことであった。

イ　制御システムの安全機能も含めて、72 時間の無人運転が可能かどうかについては、性能検査代行機関（ZUS）が、個別のボイラーごとに判断するとのことであった。

7　機能安全の適合性評価について

(1) 認証機関による認証の必要性について

ア　IEC 61508-1 の 8.2.18 の Table 5 に規定されているとおり、SIL2 までであれば、自社の独立した部局による認証が原則であるが、SIL3 以上については、独立組織が原則（SIL3 については、複雑性が低いシステムについては自社認証（独立部門）も認められている。）となっている。

(2) 適合性評価の単位について

ア　EN 規格適合性（CE マーキング）は、市場に出るものに付される。このため、制御装置等の部品メーカーは、部品を販売するのであれば、その部品に CE の認証を受けてから販売し、最終メーカーは、それらの部品を組み立てた上で、最終製品としてリスクアセスメントを行った上で CE 認証を受ける。

イ　既存のボイラーに別売りの CE 認証された制御装置を装着する場合は、ドイツの場合、作業用機械使用規則（BetrSichV）の Appendix 2, Section 4.4.2 の規定により、”significant change”に該当する場合は、リスクアセスメントを再度実施することが求められる。該当するかどうかの判断は、検査機関（ZUS）による個別判断となる。

[1] 山田哲也：工業炉／燃焼装置における機能安全. 工業加熱. Vol. 50, No. 1. pp.29-34

[2] DIRECTIVE 97/23/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 29 May 1997 on the approximation of the laws of the Member States concerning pressure equipment. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31997L0023&from=EN

[3] HSE: Pressure Equipment, Guidance Note on the UK Regulations April 2005, URN 05/1074. Available at : https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/293935/05-1074-product-standards-pressure-equipment.pdf

[4] Publication of titles and references of harmonised standards under Union harmonisation legislation (2014/C 313/02) : Commission communication in the framework of the implementation of Directive 97/23/EC of the European Parliament and of the Council of 29 May 1997 on the approximation of the laws of the Member States concerning pressure equipment. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=uriserv:OJ.C_.2014.313.01.0053.01.ENG

[5] Safety Assessment Federation (SAFed) and Combustion Engineering Association (CEA) 2011, "Guidance on Safe Operation of Boilers" Ref: BG01

Ⅲ　産業用ロボットの安全方策における機能安全の活用
-協働作業を中心として-

1　産業用ロボットの登場　その光と影

我が国では、1980年を産業用ロボット普及元年として、急速に普及が進み大企業から中小企業まで多くの工場で用いられるようになっている。しかし、その当初から、ロボットアームに押しつぶされる死亡災害が発生するなど、安全方策の不備が国会等で指摘され、1983年に、「隔離と停止の原則」による安全方策を基本とする労働安全衛生規則の改正が行われた。「隔離と停止の原則」による安全方策とは、具体的には、ロボットの周囲に柵等を設け、自動運転中は原則として柵内に立ち入らないこと、保守作業等で柵内に入る際にはロボットを停止することなど、「ロボットと人を隔離するか、隔離できない場合にはロボットを停止する」ことによる安全方策をいう。

教示作業（ロボットに作業のための動作を教える作業）においても、柵の外から行う、駆動源を落とした状態で行うなどにより、「隔離と停止の原則」による安全方策を用いることができる場合にはこれを用いる。ただし、ロボットアームの先端に近づいて溶接点を確認しなければならない場合など、「隔離と停止の原則」に従えないときには、作業者にイネーブルスイッチを持たせ、ロボットが仮に誤動作しても、ぶつかる前に止まるようにする「隔離と停止の原則」に準じた方策が講じられる。

これらに関する労働安全衛生規則の条文（第150条の3～第151条）を表1に示す。

なお、労働安全衛生規則の改正と併せて「産業用ロボットの使用等の安全基準に関する技術上の指針（昭58.9.1公示第13号）」が作成されている。これは世界に先立って作られたロボットの技術指針であり、これを参考に国際規格ISO10218が制定されている。

表1　産業用ロボットに関する労働安全衛生規則

第一章 機械による危険の防止　第9節　産業用ロボット
（教示等） 第150条の3　事業者は、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について教示等の作業を行うときは、当該産業用ロボツトの不意の作動による危険又は当該産業用ロボツトの誤操作による危険を防止するため、次の措置を講じなければならない。ただし、第1号及び第2号の措置については、産業用ロボツトの駆動源を遮断して作業を行うときは、この限りでない。 一　次の事項について規程を定め、これにより作業を行わせること。 イ　産業用ロボツトの操作の方法及び手順 ロ　作業中のマニプレータの速度 ハ　複数の労働者に作業を行わせる場合における合図の方法 ニ　異常時における措置 ホ　異常時に産業用ロボツトの運転を停止した後、これを再起動させるときの措置

へ　その他産業用ロボツトの不意の作動による危険又は産業用ロボツトの誤操作による危険を防止するために必要な措置

二　作業に従事している労働者又は当該労働者を監視する者が異常時に直ちに産業用ロボツトの運転を停止することができるようにするための措置を講ずること。

三　作業を行つている間産業用ロボツトの起動スイツチ等に作業中である旨を表示する等作業に従事している労働者以外の者が当該起動スイツチ等を操作することを防止するための措置を講ずること。

（運転中の危険の防止）

第150条の4　事業者は、産業用ロボツトを運転する場合（教示等のために産業用ロボツトを運転する場合及び産業用ロボツ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ツトを運転するときを除く。）において、当該産業用ロボツ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。

（検査等）

第150条の5　事業者は、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、修理、調整（教示等に該当するものを除く。）、掃除若しくは給油又はこれらの結果の確認の作業を行うときは、当該産業用ロボツトの運転を停止するとともに、当該作業を行つている間当該産業用ロボツトの起動スイツチに錠をかけ、当該産業用ロボツトの起動スイツチに作業中である旨を表示する等当該作業に従事している労働者以外の者が当該起動スイツチを操作することを防止するための措置を講じなければならない。ただし、産業用ロボツトの運転中に作業を行わなければならない場合において、当該産業用ロボツトの不意の作動による危険又は当該産業用ロボツトの誤操作による危険を防止するため、次の措置を講じたときは、この限りでない。

一　次の事項について規程を定め、これにより作業を行わせること。

イ　産業用ロボツトの操作の方法及び手順

ロ　複数の労働者に作業を行わせる場合における合図の方法

ハ　異常時における措置

ニ　異常時に産業用ロボツトの運転を停止した後、これを再起動させるときの措置

ホ　その他産業用ロボツトの不意の作動による危険又は産業用ロボツトの誤操作による危険を防止するために必要な措置

二　作業に従事している労働者又は当該労働者を監視する者が異常時に直ちに産業用ロボツトの運転を停止することができるようにするための措置を講ずること。

三　作業を行つている間産業用ロボツトの運転状態を切り替えるためのスイツチ等に作業中である旨を表示する等作業に従事している労働者以外の者が当該スイツチ等を操作することを防止するための措置を講ずること。

（点検）

第151条　事業者は、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について教示等（産業用ロボツトの駆動源を遮断して行うものを除く。）の作業を行うときは、その作業を開始する前に、次の事項について点検し、異常を認めたときは、直ちに補修その他必要な措置を講じなければならない。

一　外部電線の被覆又は外装の損傷の有無

二　マニプレータの作動の異常の有無

三　制動装置及び非常停止装置の機能

2　産業機械としてのロボットの特徴

1つの製品が完成するまでには、様々な工程を要する。生産ラインにおいて、ロボットは

さまざまな工程で用いられ、周辺機器または他のロボットと連携してワークを加工する。この際、ロボットは、ロボット自体が切削や鍛圧などの加工を行うのではなく、人の代わりにワークを把んで搬送したり、他の工作機械（周辺機器）にワークをセットする用途（pick & place）に用いられることが多い。場合によっては、ロボットとロボットが協調して作業する（例えば、前工程の pick & place ロボットと、次工程の pick & place ロボットが連動してワークの移送をするなど）こともある。さらに、最近では、この連携相手の１つとして人間（作業者）が考えられている。ロボットには得意な作業と不得意な作業がある。ロボットが不得意な作業や人の方が得意な作業は人が行い、人とロボットが連携して作業を行おうという研究が実証段階に入っている。例えば、重量物のワークをロボットが人の作業スペースに搬送し、ロボットがワークを保持した状態で作業者が加工を行うといったことが考えられている。このように、人とロボットが同じ空間を共有して連携して作業を行うことを協働運転（collaborative operation）といっている。（ISO10218-1(JIS B 8433-1)では「特別の目的で設計したロボットが、定義した作業空間内で人間と直接協働して動く状態」と定義している）

この新たなロボットの研究開発の進展と併せて、国際規格の改正が審議され、協働運転に必要となる安全要求事項が ISO10218-1,2（JIS では B8433-1,2）に規定された。あらかじめ安全規格を規定してものづくりを促進することは国際的には当然のことであり、我が国でも、平成 25 年に協働運転を行う場合の規定が示された（平成 25 年 12 月 24 日基発 1224 第 2 号）。我が国では、大きな事故が起きてからでないと安全対策が示されないことが多い中で、あらかじめ安全要求事項が示されたことは、今後の行政施策の良い前例となると思われる。その内容は、国際標準化機構による産業用ロボットの規格（ISO10218-1,2:2011）により設計製造された産業用ロボットをその使用条件に基づき適切に使用することなどを要件とするものである。

３　産業ロボットの安全規格

産業ロボットの安全規格である ISO 10218-1、及び ISO 10218-2 による主な安全要求事項を紹介する。この２つの規格は JIS B 8433-1,2 として日本工業規格になっているので、これをもとにその概要を紹介する。（主な事項に限っているので、実際に設計等を行う際には、改めて規格書を参照すること。）

（１）ISO10218-1:2011（JIS B 8433-1:2014）

ISO10218-1「ロボット及びロボティックデバイス－産業用ロボットのための安全要求事項－第１部：ロボット」は、ISO12100 に示されるタイプ C 規格（個別安全規格）であり、ロボットの設計及び製造上の安全の保証のための手引きである。

この規格は、産業用ロボットの本質的安全設計、保護方策及び使用上の情報についての要求事項及び指針について規定している。また、ロボットに関連する基本的な危険源を記述し、危険源に関連するリスクを除去し、または適切に低減するための要求事項に

ついて規定しているものである。なお、この規格は非産業用ロボット（軍事ロボット、宇宙ロボットなど）には適用されない。

まず、ロボットは関連する危険源に対してISO12100（JIS B 9700）に従って設計しなければならないと明記している。そのあとに産業用ロボットに関する安全要求事項が示されているが、そのうち、機能安全に関する部分としては以下のものがある。

ア　一般要求事項

（ア）動力伝達構成品（略）

（イ）動力の消失または変化（略）

（ウ）エネルギー源（略）

（エ）作動制御装置（略）

（オ）安全関連制御システム性能（ハードウェア及びソフトウェア）

制御システムの安全関連部は、ISO13849-1(JIS B 9705-1)で規定するカテゴリ3のアーキテクチャでのPL=d、又はIEC62061(JIS B 9961)で規定するプルーフテスト間隔が20年以上で、ハードウェアフォールトトレランスが1のSIL2に適合するように設計しなければならないこと。

これは、特に次のことを意味する。

a)いずれの部分に単一の障害が生じても安全機能の喪失にはつながらない。

b)合理的に実行可能な場合は常に、単一の障害は安全機能の次の作動要求時又はその前に検出できなければならない。

c)単一の障害発生時に、安全機能を常に実行し、検出した障害が修復されるまで安全状態を維持しなければならない。

d)合理的に予見可能な障害は、全て検出できなければならない。

ロボット及びその意図したアプリケーションに対して行われる包括的リスクアセスメントの結果に基づき、上記以外の安全関連制御システム性能を適切であると決定してもよい。

（カ）ロボット停止機能

ロボットは、一つ以上の非常停止機能をもたなければならないこと(IEC60204-1（JIS B 9960-1の停止カテゴリ0又は1)。

ロボット動作又は他の危険な状態を始動することのできる各制御ステーションは、手動で開始できる次の非常停止機能をそなえなければならないこと。

a)（オ）及びIEC60204-1(JIS B 9960-1)の要求事項に適合する。

b)ロボットの他の全ての制御に優先する。

c)全ての危険源を停止する。

d)ロボットアクチュエータから駆動用動力を除去する。

e)ロボットシステムによって制御される危険源の制御の能力を備える。

f)リセットするまで維持する。

g)手動動作によってだけリセットでき、リセット後は再起動を引き起こしてはならない。リセットは、再起動を可能にすることだけでなければならない。

非常停止装置は、IEC60204-1(JIS B 9960-1)及びISO13850(JIS B 9703)に適合しなければならないこと。

ロボットは、外部の保護装置に接続するために設計した一つ以上の保護停止機能を持たなければならないこと。保護停止機能性能は、(オ)の要求事項に適合しなければならないこと。

この停止機能は、全てのロボット動作を停止し、ロボット駆動用アクチュエータへの動力を除去又は制御し、かつ、ロボットが制御する他のあらゆる危険源の制御を可能にしなければならない。この停止は、手動又は制御論理によって開始してもよい。

少なくとも一つの保護停止機能はIEC60204-1(JIS B 9960-1)で規定している停止カテゴリ0又は1でなければならないこと。

(キ) 速度制御(略)

(ク) 運転モード(略)

(ケ) ペンダント制御装置(略)

(コ) 協働運転要求事項

協働運転のために設計されたロボットは、協働運転中であることを示す視覚表示を備えなければならず、更に以下の①から④の一つ以上の要求事項に適合しなければならないこと。

①安全適合の監視停止

人間が協働作業空間内に存在するときは、ロボットは停止しなければならない。停止機能は、(オ)及び(カ)に適合しなければならないこと。人間が協働作業空間から離れると、ロボットは自動運転に復帰してもよい。

又は、ロボットは、IEC60204-1(JIS B 9960-1)に従った停止カテゴリ2としてもよい。この停止は、一旦停止したら、(オ)で規定する安全関連制御システムによって監視しなければならないこと。安全適合の監視停止機能の障害は、停止カテゴリ0としなければならないこと。

②ハンドガイド(略)

③速度及び間隔の監視(略)

④本質的設計又は制御による動力及び力の制限

ロボットの動力または力を制御する機能は、(オ)に従わなければならないこと。いずれの制限値を超えた場合も保護停止としなければならないこと。

ロボットは単に最終的な協働ロボットシステムの中の構成品であり、そ

れ単体だけでは安全な協働運転に対しては十分ではない。協働運転のアプリケーションは、アプリケーションシステム設計で実施されたリスクアセスメントによって決定しなければならないこと。使用上の情報には、制御されたロボットにおける制限値の設定について詳細を含めなければならないこと。JIS B 8433-2 は、協働運転を設計するために使用すること。

（サ）特異点保護（略）

（シ）軸制限（略）

イ　安全要求事項及び保護方策の検証及び妥当性確認

ロボット製造者は、適切な安全保護装置を含めた設計及び製造の検証及び妥当性確認をしなければならないこと。

ウ　使用上の情報

表示（例えば、標識、記号）及び指示資料（例えば、運転及び保全のマニュアル）は、ISO12100(JIS B 9700)及びIEC60204(IS B 9960-1)に従って、製造業者が提供しなければならないこと。

各ロボットには、次の事項を含む取扱説明書又は適切なメディアを附属しなければならないこと。

（2）ISO 10218-2:2011（JIS B 8433-2:2014）

ISO 10218-2「ロボット及びロボテイックデバイス－産業用ロボットのための安全要求事項－第2部：ロボットシステム及びインテグレーション」は、産業用ロボットセル及びラインに統合され、設置された産業用ロボットシステムによってもたらされる特定の危険源を認識して規定されたものである。主な安全要求事項のうち、機能安全に関係するものを次に示す。

ア　一般（略）

イ　安全関連制御システムの性能（ハードウェア及びソフトウェア）

安全関連制御システム（電気、油圧、空圧及びソフトウェア）は、リスクアセスメントの結果によって代替の性能基準が適切であると決定しない限り、制御システムの安全関連部品は、ISO13849-1(JIS B 9705-1)で規定するカテゴリ3のアーキテクチャでのPL=d、又はIEC62061(JIS B 9961)で規定する、プルーフテスト間隔が20年以上で、ハードウェアフォールトトレランスが1のSIL2に適合するように設計しなければならないこと。

これは、特に次のことを意味する。

a)いずれの部分に単一の障害が生じても安全機能の喪失にはつながらない。

b)合理的に実行可能な場合は常に、単一の障害は、安全機能の次の作動要求時又は

その前に検出できなければならない。

c)単一の障害発生時に、安全機能を常に実行し、検出した障害が修復されるまで安全状態を維持しなければならない。

d)合理的に予見可能な障害は、全て検出できなければならない。

要求事項 a)～d)は、ISO13849-1(JIS B 9705-1)で規定するカテゴリ 3 と同等であることを考慮する。

ウ　ロボットシステム及びセルの停止機能（略）

エ　ロボット動作の制限（略）

オ　ロボットシステム運転モードアプリケーション（略）

カ　ペンダント（略）

キ　保全及び修理（略）

ク　安全防護（略）

ケ　協働ロボットの運転

協働とは、人とロボットが共通の作業空間を共有する特別な運転である。

①　あらかじめ決めたタスクに使われること、

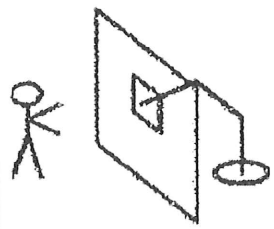
②　全ての必要な保護方策が作動中のときだけ協働可能なこと、

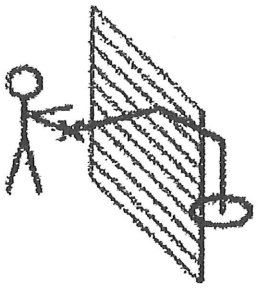
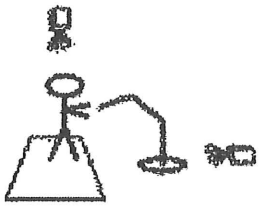
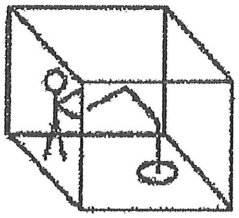
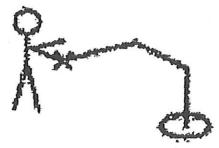
③　JIS B 8433-1 に適合する協働運転のために特別に設計された特性を持つロボットであること。

が全て満たされた場合だけに限られる。

アプリケーションの例を**表 2** に示す。

表 2　協働ロボットの概念的アプリケーション

アプリケーションの種類		説明	安全防護物	目的
	受渡し窓口	－安全防護空間内の自律した自動運転 －ロボットは窓口に移動する。 －接近中に自動運転の中断なし	－作業空間周囲の固定式又は検知式ガード －窓口付近の低減速度及び縮小作業空間 －窓口の外側にロボット作業空間なし －窓口の下端が 1000mm 未満の場合、5.10.3 による安全防護物	－ロード、アンロード －試験、手仕上げ、清掃 －点検

	インタフェース窓口	－安全防護空間内の自律した自動運転 －ロボットはインターフェース窓口で停止し、その後、手動でインターフェースの外側から動かすことができる。	－作業空間周囲の固定式又は検知式ガード －窓口の外及び付近の低減速度及び縮小作業空間 －ガイド動作のためのホールド・ツウ・ラン制御	－自動スタッキング／デスタッキング －ガイド組立 －ガイド補充／撤去 －試験、手仕上げ、清掃 －点検
	協働作業空間	－共有（協働）作業空間内の自律した自動運転 －人が共有（協働）作業空間に侵入したとき、ロボットは減速及び／又は停止する。	－一つ以上のセンタを使用した人検出システム －距離に応じた低減速度（5.11.5.4） －立入禁止空間に侵入した場合、ロボットは安全に停止し、空隙が適切に安全防護された後に自動再起動が可能になる。	－共有の組立 －共有のハンドリング －試験、手仕上げ、清掃 －点検
	検査	－安全防護空間内の自律した自動運転 －ロボットが低減速度及び移動制限下で運転を継続している間に、人が協働作業空間に侵入する。	－作業空間の周辺の固定式又は検知式ガード －人検出システム又はイネーブル装置 －作業空間侵入後の低減速度及び作業空間の縮小 －誤使用に対する方策	－検査及びプロセスの調整。例えば溶接のアプリケーション
	ハンドガイドロボット	－用途特有の作業空間 －ハンドガイドによる移動 －経路に沿うハンドガイドによる移動	－低減速度 －ホールド・ツウ・ラン制御 －用途の危険源に応じた協働作業空間	－ハンドガイドによる組立、塗装など

インテグレータは、協働運転に求められる安全防護物及びモード選択を使用上の情報に含めなければならないこと。

協働ロボットの運転に必要な安全要求事項を（ア）（イ）に示す。

（ア）一般

協働作業空間内の人とロボットとの間の空間的分離が、潜在的に減少することによって、運転中に人とロボットとの物理的接触を引き起こす可能性がある。保護方策は、常にオペレータの安全を確実にするよう講じなければならないこと。

次の要求事項は全て満たさなければならないこと。

a)インテグレータは、リスクアセスメントを実施しなければならないこと。リスクアセスメントは、協働タスク及び作業空間全体を考慮しなければならないこと。少なくとも、次を含めなければならないこと。

1)ロボット特性（例えば、負荷、速度、力、動力）

2)ワークピースを含めてのエンドエフェクタの危険源（例えば、人間工学的設計、鋭利なエッジ、突起物、ツール交換装置を使用しての作業）

3)ロボットシステムのレイアウト

4)ロボットアームの近くでは、オペレータの位置

5)部品の位置、構造物の配置（例えば、取付具、建造物の支持具、壁）及び取付具上の危険源の位置に対するオペレータの位置及び経路

6)取付具の設計、クランプの位置取り及び動作、その他関連する危険源

7)手動制御ロボットのガイド装置の設計及び配置（例えば、接近性、人間工学など）

8)アプリケーション特有の危険源（例えば、温度、放出部品、溶接火花）

9)必要な保護具の使用によって生じる制限

10)環境への配慮（例えば、化学物質、無線周波数（RF）、放射など）

11)関連する安全機能の性能基準

b)協働作業空間に統合されているロボットは、JIS B 8433-1 の要求事項を満足していなければならないこと。

c)存在検知に使用されている保護装置は、イの要求事項を満足していなければならないこと。

d)協働作業空間内で使用されている追加の保護装置は、イの要求事項を満足していなければならないこと。

e)安全防護は、協働作業空間を越えて安全防護空間に侵入してくる人を阻止するか、又は検出するように設計されなければならないこと。協働作業空間を越えた安全防護空間への侵入には、ロボットを停止し、かつ、全ての危険源をなくさなければならないこと。

f)周囲の安全防護は、安全防護空間の協働していない場所に侵入してくる人を阻止するか、又は検出するものでなければならないこと。

g)ロボットシステムに接続されているか、又は装着されており、潜在的危険源をもっている機械が、協働作業空間内にある場合には、これらの機械の安全関連機能は、少なくともイの要求事項に適合していなければならないこと。

協働運転を構成しているロボットは、**図 1** に示すシンボルのラベルを貼付するのが望ましい。

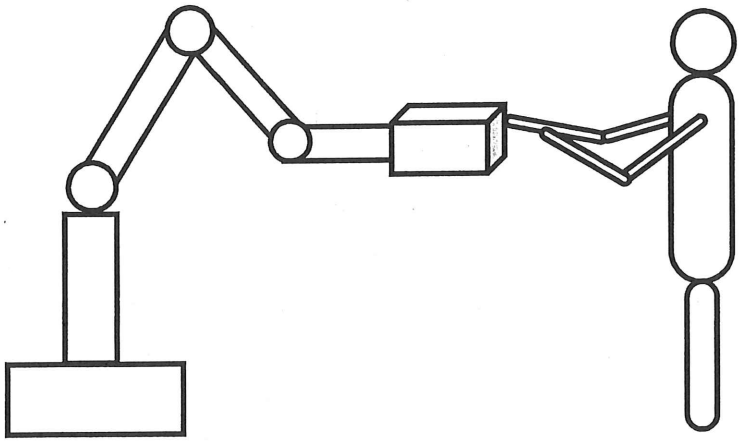


図 1－ラベルの推奨デザイン

（イ）協働作業空間内での運転

協働運転を設計するとき、全ての要員が作業セル内で潜在的危険源に暴露されない安全な作業環境を確保するように、①～④にある一つ以上の安全特性を適切に選択しなければならないこと。

協働運転の選択された安全特性で検出された故障は全て保護停止にならなければならないこと。非協働運転は、そのような停止後、協働作業空間の外側からの意図的な再起動操作によるリセットまで再開してはならないこと。

①安全適合の監視停止

協働作業空間に人がいない場合、ロボットは非協働で動作する。協働作業空間に人が侵入した場合、オペレータとロボットとが直接的に関わること（例えば、エンドエフェクタへの部品の搬入）を可能にするために、ロボットは動作を停止し、JIS B 8433-1に従った安全適合の監視停止を維持しなければならないこと。

②ハンドガイド（hand guide）

ハンドガイドの操作は、次の要求事項を満足した上で、許可されること。

a)ロボットがハンドガイド開始位置に到達したとき、JIS B 8433-1 に従った安全適合の監視停止となる。

b)オペレータは、JIS B 8433-1 の要求事項を満足するガイド装置（意図した位置にロボットを動かすための）をもっていなければならないこと。

c)オペレータは、協働作業空間全体を明確に視認できなければならないこと。

d)オペレータがガイド装置を離したとき、JIS B 8433-1 に従った安全適合の監視停止となる。

③速度及び間隔の監視

動的な動きをしている（状態にある）ロボットとオペレータとの間を安全な間隔に保つように設計されたロボットシステムには、JIS B 8433-1 の要求事項に適合するロボットを使用しなければならないこと。

ロボットの速度、最小の隔離距離及びその他のパラメータは、リスクアセスメントによって決定しなければならないこと。

④設計又は制御による動力及び力の制限

動力又は力の制限によって危険源を制御するように設計されたロボットシステムには、JIS B 8433-1 に適合するロボットを使用しなければならないこと。

動力、力及び人間工学のパラメータは、リスクアセスメントで決定しなければならないこと。

コ　安全要求事項及び保護方策の検証及び妥当性確認

ロボットシステムの製造者又はインテグレータは、ここに規定した原則に従って適切な安全防護装置を含めてロボットシステムの設計及び製作の検証及び妥当性確認をしなければならないこと。

サ　使用上の情報（略）

Ⅳ　動力プレス機械リスク低減と機能安全、規制緩和への可能性－機能安全のプレス機械への適用事例

1　動力プレス機械に関する法令と規格

(1) 国内の法令

日本国内の動力プレス機械の安全に関する主な法令，規格として以下がある。JIS B6410:2009 は，日本独自のサーボプレスに関する安全要求事項に関する規格であり ISO13849-1(JIS B9705-1)で示される制御システムの安全関連部の機能安全の性能要求レベルであるパフォーマンスレベルでサーボプレス機械の各制御機能の安全関連部の性能要求レベルが示されている。

ア　労働安全衛生法

イ　労働安全衛生規則　第 131 条~137 条

ウ　動力プレス機械構造規格

エ　プレス機械又はシャーの安全装置構造規格

オ　JIS B6410:2009「プレス機械－サーボプレスの安全要求事項」

(2) 欧州の規制

欧州においては，EU 加盟国に立法を指令するニューアプローチ指令の中の機械指令（2006/42/EC）がある。機械指令では，機械類に適用しなければならない規格（整合規格）があり，動力プレス機械関連の規格として C 規格（個別製品規格）に以下が示されている。これらの規格においても制御システムの安全関連部の機能安全は，機械類の機能安全規格である EN ISO13849-1 を参照している。

ア　EN 692:2005+A1:2009　：機械プレスの安全

イ　EN 693:2001+A2:2011　：液圧プレスの安全

ウ　EN 13736:2003+A1:2009　：空気圧プレスの安全

(3) 米国の規制

米国内の動力プレス機械の安全に関する主な法令，規格として以下がある。

ア　OSHA 1910.217　：労働安全衛生庁　労働安全衛生規格　機械式動力プレス

イ　ANSI B11.1:2009：機械式動力プレスの安全要求事項

ウ　ANSI B11.19:2010：安全防護の性能要求事項

エ　ANSI B11.TR6-2010：機械の安全制御システム

オ　NFPA79:2015：産業機械の電気規格

OSHA1910.217 の規定には，動力プレス機械の安全要求事項の要求性能が示されているが，詳細な機能安全の要求事項は示されていない。機能安全要求事項は，国家規格 ANSI B11（機械安全）シリーズや NFPA79 に IEC62061,ISO13849-1 の制御システムの安全関連の適用規格としての記載があると共に,ISO13849-2，IEC61508,IEC61800-5-2 等の機能安全規格の適用が示されている。特に動力プレス

機械の米国規格 ANSI B11.1 では，設計者・使用者・使用者（作業者）の責任とそこで適用される国家規格体系が示されている。参考として**図１**に各責任（メーカー・使用者・作業者）で使用する国家規格体系を示す。

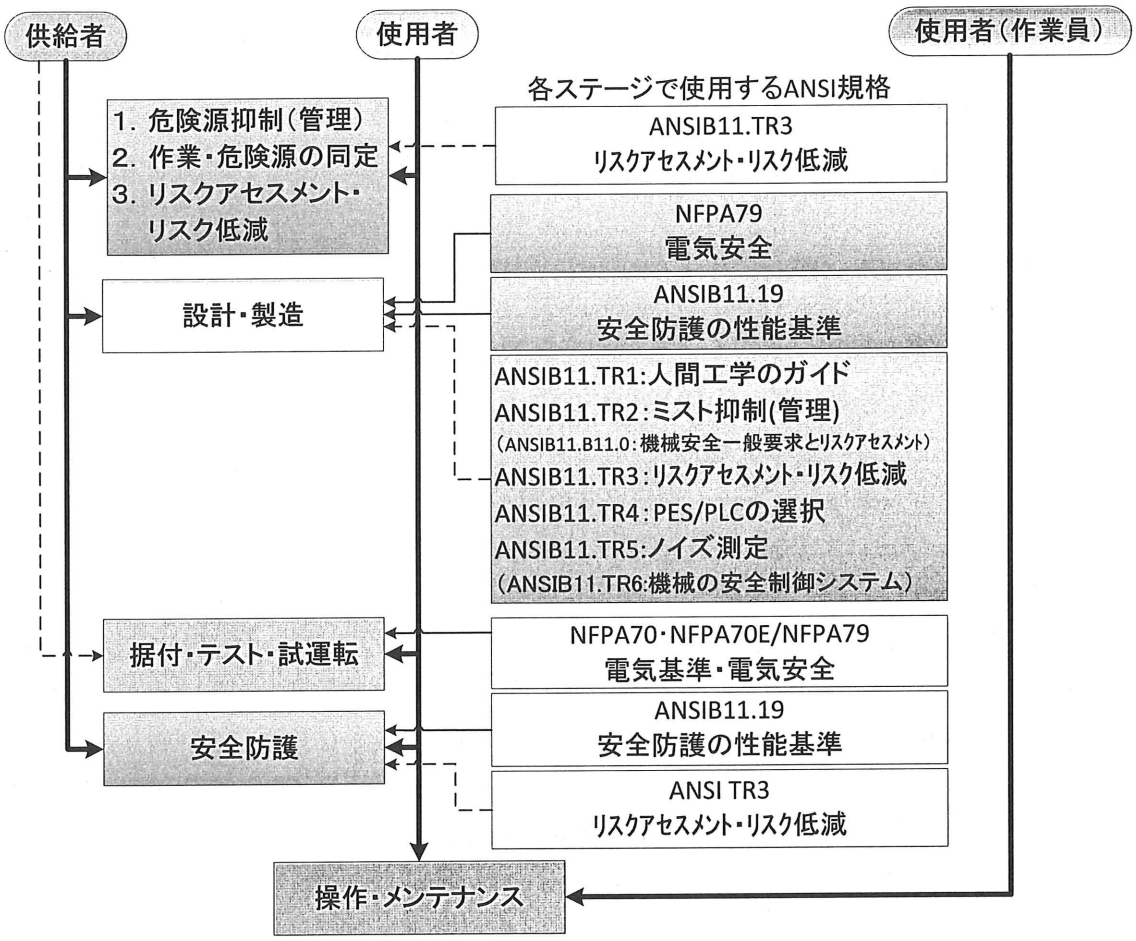


図１．各責任（メーカー・使用者・作業者）で使用する国家規格

(4) 制御システムの安全関連部の規制

各国の動力プレス機械の制御システムの安全関連部は，その技術に関する国家規格を参照することが基本である。また，各国の機械安全の国家規格は，各国においてWTO/TBT 協定のもとで機械安全の国際規格（ISO/IEC）と整合した国家規格が発行されている。以下に日本国内で発行されている動力プレス機械の制御システムの安全関連部で確認，使用できる主要な機能安全規格及びガイドを示す。以下では、国内で国家規格として発行されていない重要規格に関しては，国際規格で示してある。特に動力プレス機械に機能安全を適用する場合は，JIS B9700、ISO/TR22100-2、ISO13849-1，ISO13849-2, IEC 62061, ISO/TR23849(IEC/TR62061-1）を理解して設計を進めることが必要である。

ア　JIS B9700:2013　:設計の一般原則—リスアセスメントとリスク低減

イ　ISO/TR22100-2:2013　：ISO 12100 と ISO13849-1 との関係

ウ　JIS B9705-1:2011　：制御システムの安全関連部―設計のための一般原則

エ　ISO13849-1:2015　：制御システムの安全関連部―設計のための一般原則
(JIS B9705-1:2011 の元規格である ISO 13849-1:2006 の最新版)

オ　ISO13849-2:2012　：制御システムの安全関連部―妥当性確認

カ　JIS B9961:2008　：電気・電子・プログラマブル電子制御系の機能安全

キ　IEC 62061:2012　：電気・電子・プログラマブル電子制御系の機能安全
(JIS B9961:2008 の元規格である IEC 62061:2005 の最新改訂版)

ク　ISO/TR23849(IEC/TR62061-1):2010　：安全関連制御における ISO 13849-1 と IEC 62061 の適用に関するガイドライン

ケ　IEC 61508-1~7:2010　：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

(5) 動力プレス機械の制御システムの規制

現在進められている動力プレス機械の国際規格の安全関連の制御システムの要求事項では，従来欧州規格 EN692 で示されていた制御システム構造要件から機能安全の適用が検討されている。**図２**に EN692 と現在検討が進められている動力プレス機械の国際規格で検討されている制御システムの安全関連部の機能安全要求事項との比較事例を示す。動力プレス機械の C 規格では，安全機能において要求される PLr（要求パファーマンスレベル）に加え，制御システムのカテゴリも要求事項として規定されているのが特徴である。この考えは，リスクが大きな危険源に対する制御システムによる保護方策に対しては冗長設計構造の必要性を示している。

EN692 ：手作業の一行程生産モードでの作業者安全防護の要求事項（光線式安全装置部の抜粋）

作業者安全システム	サイクル始動	クラッチ・ブレーキ制御システム		オーバーラン監視	ミューティング	一行程	備考
		電気	バルブ				
光線式安全装置による保護方策	ガード以外	冗長システムと監視	冗長システムと監視	必要（単一システムと監視）	監視	冗長システムと監視	要求される安全距離の確保

動力プレス機械国際規格案：手作業の一行程生産モードでの作業者安全防護の要求事項（光線式安全装置部の抜粋）

主要安全システム	危険動作	安全機能	要求性能PLr決定のためのリスク評価			安全機能の最低要求 PL	安全機能の入力・処理（制御）・出力の設計の基準			
			S	F	P		制御システムのカテゴリ要求	入力	処理（制御）	出力
光線式安全装置による保護方策	スライド下降行程	光線以外の始動	S1	F1	P1	PLa	Cat.B	光線以外の入力	あらゆる制御	電気制御システムの適切な動作
		光線による始動	S2	F2	P2	PLe	Cat.4	AOPD (TYPE4)	安全関連論理制御	
		安全装置による停止	S2	F2	P2	PLe	Cat.4			空圧システム（バルブ）

図２．動力プレス機械への機能安全適用動向

(6)　動力プレス機械のリスク低減における主要な機能安全の規格

図３は，動力プレス機械及び一般の機械の機能安全設計のための主要な国際規格の歴史と関係を示した。機械安全における機能安全の規格は，1996 年に発行された EN954-1 が始まりで，それ以前の Pr-EN954 の時代から制御システムの安全要求レベルとして制御システムの故障に対する耐性レベルとしてリスクレベルに応じたカテゴリ B，１，２，３，４の 5 段階の性能レベルが指定されていた。動力プレス機械では 1980 年代後半からこれらの概念が使用されている。機能安全の国際規格の始まりは，この EN954-1 をもとに 1999 年に制定された ISO13849-1 である。この ISO13849-1:1999 が，機械製造者，機械設計者の制御システムの設計者のための制御システムの安全関連部を設計するための基準となった。

その後，IEC61508 が，プログラム（ソフトウエア）を含めた電子・電気機器製造，設計者のための規格が 2000 年に発行されている。この IEC61508 が，産業界のプログラム（ソフトウエア）を含めた電子・電気機器製造，設計者のための基本規格になっている。その後 IEC61508 から機械安全に特化した規格として IEC62061 が 2005 年に発行されている。一方 ISO13849-1 も従来の制御システムのカテゴリに IEC61508 の信頼性の概念を取り入れた制御システムの安全性能レベルであるパフォーマンスレベル（PL）が，機械安全の制御システムの設計に導入された。

この流れで機械安全に制御システムの安全関連部の設計においては ISO13849-1（ISO13849-2 含む）と IEC62061 が存在することになった。そこで 2010 年にこれらの規格を使用して制御システムの設計を行うためのガイドラインが ISO/IEC 双方から ISO/TR23849，IEC/TR62061-1 として発行されている。この２つのガイドラインの内容は同一である。制御システムの安全関連部の設計を進める上では非常に有益なガイドラインであるので「３ 動力プレス機械のリスク低減における機能安全適用事例」で設計使用例の概要を示す。

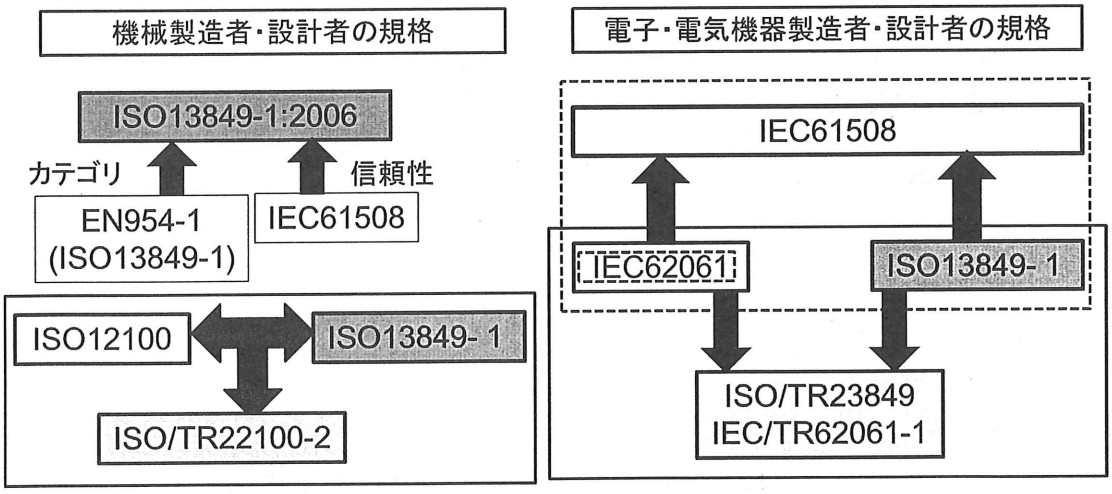


図３．リスク低減における主要な機能安全の規格

2 リスク低減方策への機能安全の役割

ここでは動力プレス機械のリスク低減を行う手順と機能安全の役割について示す。

(1) 動力プレス機械のリスクアセスメント手順

動力プレス機械においても構造規格をはじめ各国には国家規格はあるが，実際の機械を設計する際は一般の機械同様に JIS B9700 に示された手順で行う。**図４**には JISB9705-1 で示されている JISB9700 に基づくリスクアセスメント手順と適切なリスク低減後のリスクアセスメント，リスク低減の反復作業と保護方策での制御システムの関わりの流れを示した。JIS B9700 で示されるリスクアセスメント手順によりリスクを洗い出し各リスクについてのリスクレベルを見積もり評価し，その評価結果でリスク低減を行い，更にリスクが本当に適切か，他の危険源が生じていないか，リスクを低減する方策を現状の技術レベルで実施されたかを再評価する。リスク低減方策の中で制御システムが使用される場合の，JISB9705-1 を使用して制御システムの安全関連部の設計を行う手順を図４に示した。リスクの再評価の結果でリスクが現状の技術レベルで適切に低減されたと場合，機械使用者に対して残留リスクの開示のための文書化を行う。

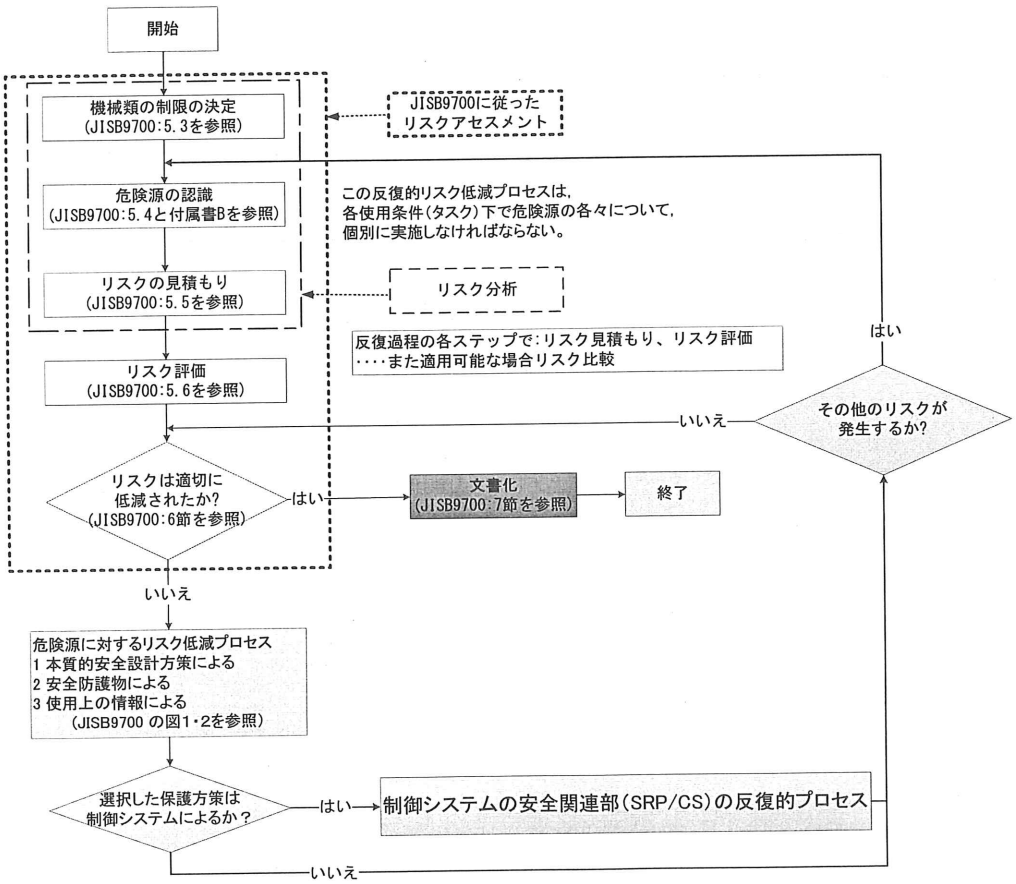


図４．機械のリスクアセスメント

(2) リスク低減手順の中での機能安全の概要

動力プレス機械におけるリスク低減も一般の機械同様にJIS B9700に示された手順で行う。リスクアセスメントの結果に基づく適切なリスク低減の機能安全設計概要フローチャートを**図５**に示す。機能安全の関わりは，安全防護の保護方策又は付加的な保護方策によるリスク低減方策を制御装置等により制御システムの安全関連部を制御する際に機能安全が使用される。図５で示した機能安全との関わりのある「ISO13849-1でのPLr見積り・機能安全設計」の実施事項の概略を以下に示す。

ア　リスクアセスメントの結果より各制御システムの安全関連部を明確にする。

イ　各制御システムの安全関連部の要求事項（機械の耐用年数，安全関連部の使用頻度等の制限仕様を明確にする）

ウ　各安全関連部の安全レベルの要求性能（PLｒ：要求パフォーマンスレベル）をISO13849-1に示されているリスクグラフにより見積もる

エ　機能安全設計の中でカテゴリ，MTTFｄ，DC，CCF，T10d，ソフトウエアがあればPLにあったソフトウエア設計と文書化を行う

オ　PLｒ以上の機能安全設計とその妥当性確認を行う

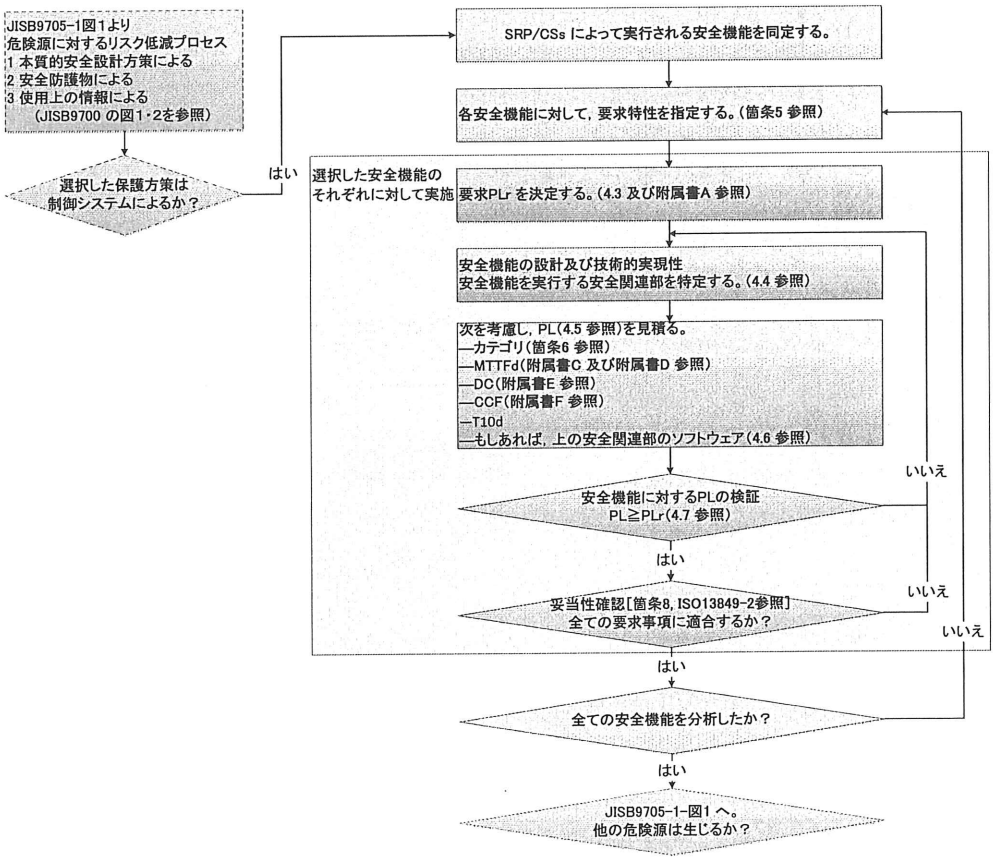


図５．リスクアセスメントの結果に基づくリスク低減フローと機能安全

(3) 機械のリスク低減における機能安全の役割

図６は，光線式安全装置を保護装置とした動力プレス機械と災害発生のプロセスと機能安全の関わりを示したものである。この動力プレス機械の主要な危険源は，下降中のスライド（金型間）による挟まれ，押し潰し，切断等の災害が想定される危険源である。この危険源による危険状態は，作業者の手が下降中のスライド（金型間）進入した状態である。この危険状態からの安全確保のための代表的な保護方策が，光線式安全装置の設置による人の手が危険源に到達する前に機械を停止させることである。この保護方策は，図２で示した光線式安全装置による停止機能で制御システムの安全関連部である。この制御システムの設計に機能安全が使用される。図５では保護方策の不具合と危険事象の発生の関係を示した。つまり，機能安全の不具合が危険事象の発生につながることを示している。「リスク」は，「危害の酷さ」とその「発生確率」の組合せ（関数）である。したがって機械安全における機能安全の役割は，危害の「発生確率」の構成要素である危険事象の発生確率を機能安全の安全性能レベルに応じて低減させることにより危害全体の発生確率の低減に寄与することにある。

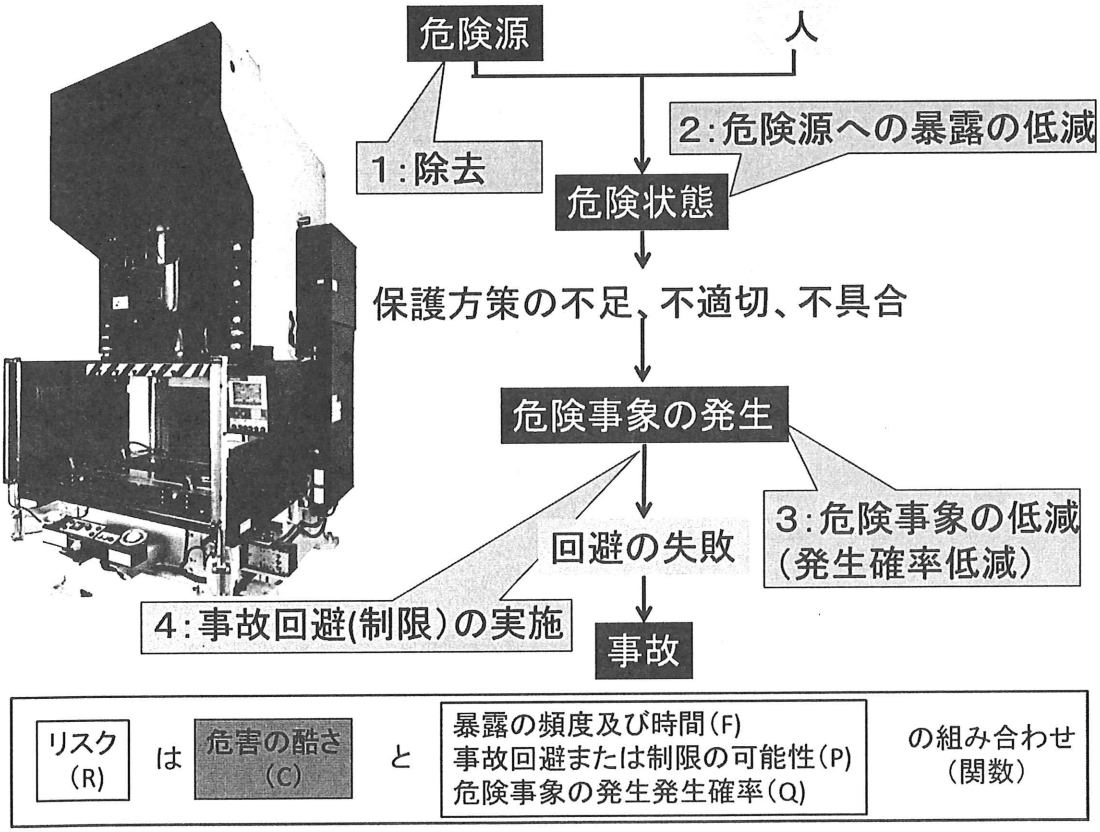


図６．動力プレス機械の危害発生のプロセスと機能安全の役割

3　動力プレス機械のリスク低減における機能安全適用事例

(1) 制御システムの安全関連部の設計及び確認事項

制御システムの安全関連部の設計を行うための手順について**図７**に示す。制御システムの安全関連部の設計を着手する場合，機械の制限仕様から決定する使用期間は，重要な要素である。ISO13849-1:2015 に附属書Ｉの事例においても機械の使命期間（ミッションタイム）に基づく制御システムの安全関連部を制御する機器の寿命からその機器の交換周期を明確にすることが示されるようになった。この図７の手順５に示した T10d を明確にして機器の寿命，交換により制御システムの安全維持の正常性を保つ考え方は，機能安全の設計を行う上で重要である。

また，近年は，機械の制御システムを扱う時に機械的な機器と安全 PLC や安全制御ユニット等の電子制御装置との組合せを行わなければならない場合が多々ある。この場合，ISO13849-1:2015，ISO/TR23829（IEC/62061-1）を使用して制御システムの安全性能レベルを評価する場合に PFHD（単位時間当たりのシステムの危険側故障確率）が，評価レベルを判断するための重要なパラメータになる。ISO13849-1:2015 では，評価パラメータとして PFHD が附属書Ｉで追加されている。

動力プレス機械のリスク低減における機能安全の使用について事例で図７に従って説明を加える。

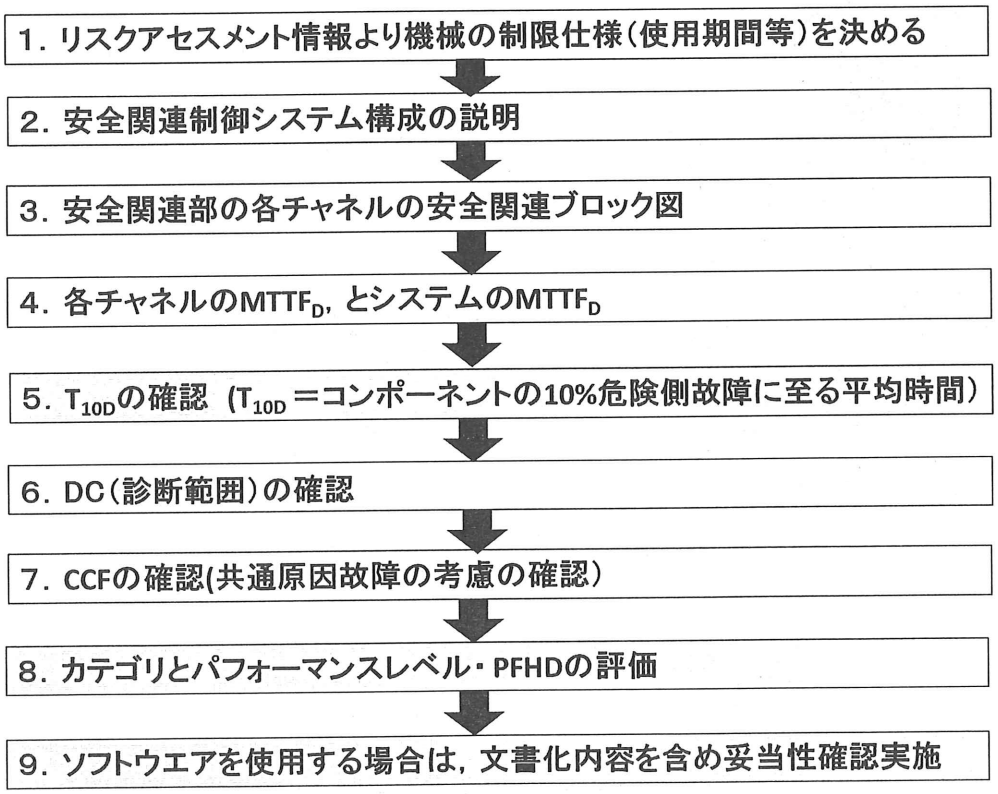


図７．制御システムの安全関連部の設計を行うための手順

(2) 事例１：動力プレス機械のガードシステム事例

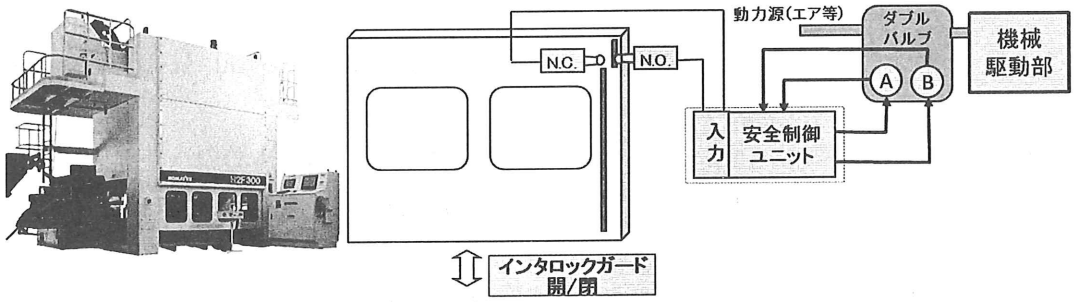


図８．動力プレス機械のインタロック式ガードによる保護方策

図８に動力プレス機械のインタロック式ガードによる保護方策の制御システムを示した。図８に示された機能安全設計についてその手順を以下に示す。

① 機械の制限仕様（使用期間等）及びリスク評価（PLｒ）を決める

- 本動力プレス機械の使用期間は，３０年とする。
- 作業は，年間３００日，１日２０時間稼働する。
- ガード開閉操作頻度は 30 分に１回･機械内部作業は，1 回 20 秒程度の作業。

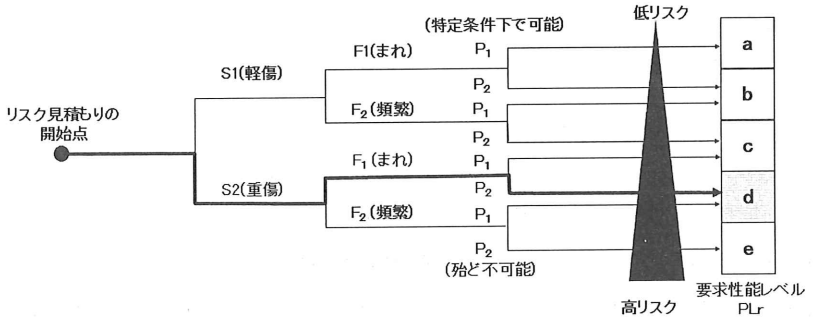


図９．JIBB9505-1：要求パフォーマンスレベルの見積もり（事例１）

- 使用条件による制御システムの安全性能要求レベルは，図 9 より PL d
- 運転操作によるダブルバルブの作動頻度は，10 秒に１回操作を行う。

② 安全関連制御システム構成の説明

- 冗長チャンネル（電気機械機構＋安全関連制御用電気制御機器）を使用
- 位置スイッチ NC は，「機械的強制乖離機構の接点」，機械的機構のスイッチは，メーカーより１０%故障回数値 B10 を入手しその値の半分を B10d とする。メーカーが B10d 値データを持っている場合は，その値を使用する。メーカーがデータを持っていない場合は，JISB9705-1 の附属書 C に記載されている B10d の値を設計データとして使用する。
- 位置スイッチ NC の B10d メーカー 確認データは，B10d(NC)＝2,000,000

回

- 位置スイッチ NO の B10d メーカー 確認データは，B10d(NO)＝1,500,000 回
- ダブルバルブ（ダイレクトモニタリング機構）の B10d メーカー 確認データは，B10d(DV)＝2,000,000 回
- 安全制御ユニット：Kは，メーカーより制御システムの安全性能連レベルが，PLe で　危険側故障確率 PFHD(K)＝2.5×10^{-9}/h が、確認が取れている。

③ 安全関連部の各チャネルの安全関連ブロック図

図８の制御システムの安全関連部のブロック図と簡略化した図を**図１０**に示す。

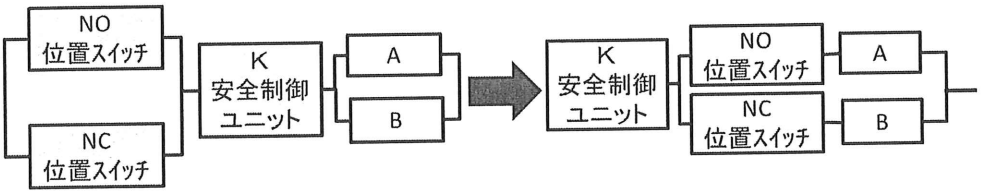


図１０．事例２の安全関連ブロック図

④ 各機器，チャネルの MTTFd とシステムの MTTFd および T10d の確認

②の情報より B10d(NC)＝2,000,000 回, B10d(NO)＝1,500,000 回

NO/NC 年間作動回数 nop（回/年）は，

nop=300 日×20H×2 回(1H/30 分)＝12,000 回/年

10%危険側故障に至る平均年数 T10d（年）は，

T10d(NC)= B10d(NC)/nop＝2,000,000/12,000=166.67 (約１６５年)

T10d(NO)= B10d(NC)/nop＝1,500,000/12,000=125 (約１２５年)

平均危険側故障間隔時間 MTTF d＝B10d/(0.1 × nop)=T10d/0.1（時間）は，

MTTF d （NC）＝165/0.1=1,650 年

MTTF d （NO）＝125/0.1=1,250 年

同様にダブルバルブについて B10d(DV)＝5,000,000 回

NO/NC 年間作動回数 nop（回/年）は，

nop=300 日×20H×720 回(1H/10 秒)＝2,160,000 回/年

10%危険側故障に至る平均年数 T10d（年）は，

T10d(DV)= B10d(DV)/nop＝5,000,000/2,160,000=2.3 (約２年)

平均危険側故障間隔時間 MTTF d＝B10d/(0.1 × nop)=T10d/0.1(時間)は，

MTTF d （DV）=2.3/0.1=23 年

図１０で示された MTTF d （NC）と MTTF d （DV）で構成されるチャンネル１の MTTF d （CH1）は，

$$\text{MTTF d (CH1)} = \frac{\{MTTFd(NC) \times MTTF(DV)\}}{\{MTTFd(NC) + MTTF(DV)\}} = 22.\ 8(年)$$

同様にMTTF d （NO）とMTTF d （DV）で構成されるチャンネル２のMTTF d （CH2）は，

$$\text{MTTF d (CH2)} = \frac{\{MTTFd(NO) \times MTTF(DV)\}}{\{MTTFd(NO) + MTTF(DV)\}} = 22.\ 7(年)$$

CH1とＣＨ２の合成MTTFd(CH1/CH2)は，冗長系の場合，次式で計算され

$$\text{MTTFd}(CH1 \cdot CH2) = \frac{2}{3} \times \left[MTTFd(CH1) + MTTFd(CH2) - \frac{1}{\left\{\frac{1}{MTTFd(CH1)} + \frac{1}{MTTFd(CH2)}\right\}} \right]$$

$$\text{MTTFd}(CH1 \cdot CH2) = \frac{2}{3} \times \left[22.8 + 22.7 - \frac{1}{\left\{\frac{1}{22.8} + \frac{1}{22.7}\right\}} \right] = 22.\ 8(年)$$

⑤ DC（診断範囲）・DCavg(平均診断範囲)の確認

DCavg(平均診断範囲)は，JISB9705-1では，４つのレベルに分類されている。このパラメータは，制御システムが故障した場合の不具合の検出機能を示し，値が高いほど制御システム内の故障が検出され，システムの危険側故障回避する機能に優れている。DCavg(平均診断範囲)が，60%未満の制御システムは安全関連部の制御システムとして使用できない。

ア　DCavg=99%以上　（high レベル）

イ　DCavg=90%以上,99%未満（medium レベル）

ウ　DCavg=60%以上,90%未満（low レベル）

エ　DCavg=60%未満（安全関連部使用不可レベル）

位置センサーNO/NC の接点は，安全制御ユニットにて監視されている。JIS B9705-1 の附属書 E.1 で示されている NC 接点・NO 接点による監視に方策を実施することで NO/NC 接点の診断範囲 DC(NO/NC)=99%にできる。

また，ダブルバルブの動作は安全制御ユニットにてダブルバルブのダイレクトモニタ接点による状態監視を毎サイクルの起動前に監視されているのでダブルバルブの診断範囲 DC(DV)=99%にできる。

従ってチャンネル１・チャンネル２全体の平均診断範囲 DCavg は，以下となる。DCavg=99% (High)

$$\text{DCavg} = \frac{\frac{DC(NC)}{MTTFd(NC)} + \frac{DC(NO)}{MTTFd(NO)} + \frac{DC(DV)}{MTTFd(DV)}}{\frac{1}{MTTFd(CH1)} + \frac{1}{MTTFd(CH2)} + \frac{1}{MTTTFd(DV)}} = \frac{\frac{0.99}{22.8} + \frac{0.99}{22.7} + \frac{0.99}{23.1}}{\frac{1}{22.8} + \frac{1}{22.7} + \frac{1}{23.1}}$$

$$= 0.99 = 99(\%)$$

⑥ CCF の確認(共通原因故障の考慮の確認)

CCF は，【Common Caused Failure】の略で，制御システムの安全関連部

が共通原因故障に対して対応方策が考慮されているかを確認する目的である。実際にはJIS B9705-1の附属書Fに示されている共通原因故障に対する方策リストで点数を付けて６５点以上であれば安全関連部の制御システムとして共通原因故障に対する方策が取られていると判定できる。表１にＪＩSB9705-1で示されている共通原因故障に対する方策の良否の判定リストで，本システムここでは同じ結果で判定したとする。（実際は，各考慮事項の確認が必要）

表１．共通原因故障に対する方策の良否判定リスト

No.	CCFに対する方策	制御システムのスコア	最大値
1	**分離／隔離**		
	信号経路間の物理的な分離	15	15
	・配線・配管の分離		
	・プリント回路基板における十分な空間距離と沿面距離		
2	**多様性**		
	異なる技術や物理原則が使用されている ・第一系統:プログラマブル電子機器と第二系統:ハードワイヤード ・起動の種類 ・圧力と温度 距離と圧力の方策 ・デジタルとアナログ ・異なるメーカの部品	20	20
3	**設計/アプリケーション/経験**		
3.1	過電圧、過圧力、過電流などの保護	なし	15
3.2	十分に吟味された部品が使用されている	5	5
4	**アセスメント／分析**		
	故障モードと影響分析の結果が、共通故障の防止に設計上考慮されているか	5	5
5	**能力/訓練**		
	設計者/保守作業者は共通故障の原因と結果を理解するための訓練を受けているか	なし	5
6	**環境**		
6.1	・適切な規格に準じたCCFに対する汚染の防止と電磁両立性(EMC)	25	25

	・液体システム:圧媒体のろ過作用、汚れ吸気の防止、圧縮空気の排出 ・電気システム:システムは電磁環境耐性に対してチェックされたものであるか ・液体系と電気系システムの組み合わせの場合は、両方の側面で考慮されていなければならない		
6.2	その他の影響 温度，衝撃，振動，湿度（例えば，関連の規格で規定されるように）のような環境関連の影響の全てに対してイミュニティの要求事項を考慮しているか？	10	10
	合計	80	Max100

合計値	CCF を回避する方策の判定
65 点以上	80 点：要求事項に満足している
65 点未満	プロセスに問題あり→追加手段を選択

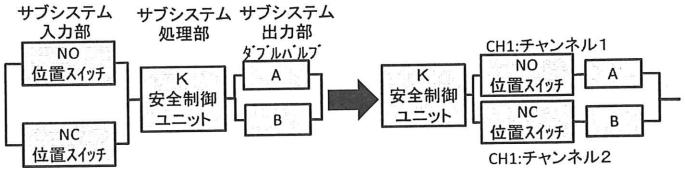
⑦ カテゴリとパフォーマンスレベル・ PFHD の評価（総合評価）

以下のこれまでの冗長部分（入力＋出力）の設計確認結果をまとめる

- ＣＣＦは，８５点（＞６５点）より，ＣＣＦの要求事項を満足している。
- どの部品の単一故障による安全機能に喪失に至らないことからカテゴリ３の特性と判定できる。
- 平均診断範囲 DC avg は，DC avg = 99% :High（高）レベル
- MFFTd(CH1/CH2)=22.8 （年） : Medium（中）レベル
- JISB9705-1 附属書 K 表 K.1 より MTTF d ＝18 年，Cat.3 を選択すると PLd / PFHd=4.21×10^{-7}(/h) となる。
- 安全制御装置 K の PLe で 危険側故障確率 PFHD(K)＝2.5×10^{-9}/h と PFHd を加算し，附属書 K で評価すると PLd / PFHd=4.24×10^{-7}(/h)
- 本システムは，要求パフォーマンスレベル PLd に対して同等であり，本機能に対して制御システムの安全関連部として妥当である。
- 但し，ダブルバルブの T10d(DV)=2.3 年であるので２年ごとの交換が必要。

これまで示した「事例１：動力プレス機械のガードシステム事例」の制御システム設計の要求パフォーマンスレベル PLr=d に対する設計検証のまとめの事例を表２に示す。

表２．事例１：動力プレス機械のガードシステム事例　設計検証事例

	機械仕様		単位	備考
1	機械の使用期間	30	年	
2	年間稼働日	300	日/ 年	
3	一日の作業時間	20	時間/日	
	安全機能（インタロック式ガード）：要求仕様		単位	備考
1	PLr：要求パフォーマンスレベル	d	PL	JISB9705-1:リスク評価より
2	PFHd:平均危険側故障率	–	SIL	
3	設計制御ハード構成	3	Cat.	設計方針：PLdをカテゴリ3で構築
4	安全関連ブロック図			
	入力部（安全関連：サブシステム）仕様		単位	備考
1	位置スイッチNC：B10d(NC)	2,000,000	回	メーカーカタログ値
2	位置スイッチNO：B10d(NO)	1,500,000	回	メーカーカタログ値
3	安全機能：ガード使用頻度	2	回/時間	使用頻度　30分/回
	処理部（安全関連：サブシステム）仕様		単位	備考
1	パフォーマンスレベルPL：安全制御ユニット:K	e	PL	メーカーカタログ値
2	危険側故障確率PFHd(K)：安全制御ユニット:K	$2.5x10^{-9}$	1/h	メーカー提供値
	出力部（安全関連：サブシステム）仕様		単位	備考
1	ダブルバルブ：B10d(DV)	5,000,000	回	メーカーカタログ値
2	安全機能：バルブ使用頻度	360	回/時間	使用頻度　10秒/回
	入力部（安全関連：サブシステム）：MTTFd評価		単位	備考
1	位置スイッチNC/NO年間作動回数：Nop(NC/NO)	12,000	回/年	
2	**位置スイッチNO：T10d(NC)＝B10d(NC)/Nop**	**166.7**	年	
3	**位置スイッチNO：T10d(NO)＝B10d(NO)/Nop**	**125.0**	年	
4	**位置スイッチNO：MTTFd(NC)＝T10d(NC)/0.1**	**1,667**	年	
5	**位置スイッチNO：MTTFd(NO)＝T10d(NO)/0.1**	**1,250**	年	
	出力部（安全関連：サブシステム）：MTTFd評価		単位	備考
1	ダブルバルブ年間作動回数：Nop(DV)	2,160,000	回/年	
2	**ダブルバルブ：T10d(DV)＝B10d(DV)/Nop**	**2.3**	年	**交換周期:2年とする。**
3	**位置スイッチNO：MTTFd(NO)＝T10d(NO)/0.1**	**23.1**	年	
	安全関連ブロック図　入力・出力冗長合成　MTTFd評価		単位	備考
1	安全関連ブロック図　CH1　MTTFd(CH1)	22.8	年	MTTFd(NC)とMTTFd(DV)直列計算
2	安全関連ブロック図　CH2　MTTFd(CH2)	22.7	年	MTTFd(NO)とMTTFd(DV)直列計算
3	安全関連ブロック図　入力・出力合成MTTFd(CH1/CH2)	22.8	年	MTTFd(CH1)とMTTFd(CH2)冗長計算
	安全関連ブロック図　入力・出力冗長合成　平均診断範囲DCavg評価		単位	備考
1	安全関連ブロック図　NO/NC診断範囲　DC(NC/NO)	99	%	JISB9705-1の附属書E.1
2	安全関連ブロック図　ダブルバルブ診断範囲　DC(DV)	99	%	
3	安全関連ブロック図　入力・出力合成　平均診断範囲DCavg	99	%	(NC),(NO),(DV)の全診断範囲の平均
	CCF(共通原因故障)スコア確認		単位	備考
1	安全関連ブロック図　入力・出力合成　CCF	85.0	点	65点以上合格：詳細はCCF確認表
	総合評価		単位	備考
1	安全関連ブロック図　入力・出力合成　PFHd(CH1/CH2)	$4.21x10^{-7}$	1/h	JISB9705-1:表K.1 MTTFd=22年/Cat.3/DCavg-High より
2	安全関連ブロック図　入力・出力合成　PL(CH1/CH2)	d	PL	
設計確認結果	安全関連ブロック図　入力・処理・出力合成　PFHd(Total)	$4.24x10^{-7}$	1/h	各PFHd加算結果
	安全関連ブロック図　入力・出力合成　PL(Total)	d	PL	JISB9705-1:表K.1 PFHd＝4.24x10-7より
	ダブルバルブ：T10d(DV)＝B10d(DV)/Nop	2.3	年	交換周期:2年とする。

(3) 事例２：動力プレス機械の光線式安全装置による保護方策事例

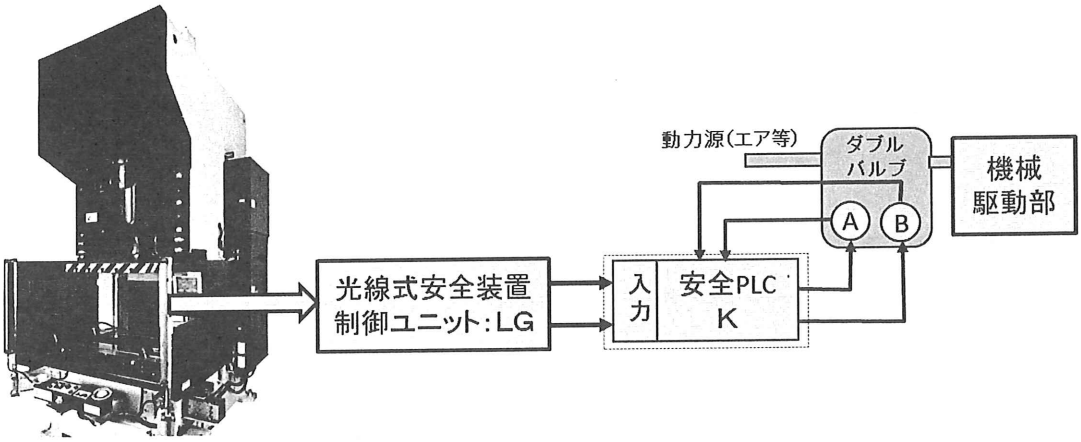


図１１．動力プレス機械の光線式安全装置による保護方策事例

図１１に動力プレス機械の光線式安全装置による保護方策の制御システムを示した。図１１に示された機能安全設計についてその手順を以下に示す。

① 機械の制限仕様（使用期間等）及びリスク評価（PLｒ）を決める

- 本動力プレス機械の使用期間は，３０年とする。
- 作業は，年間３００日，１日２０時間稼働する。
- 光線式安全装置作動頻度は平均１０秒に１回・機械内部作業は，１回１秒程度の作業。

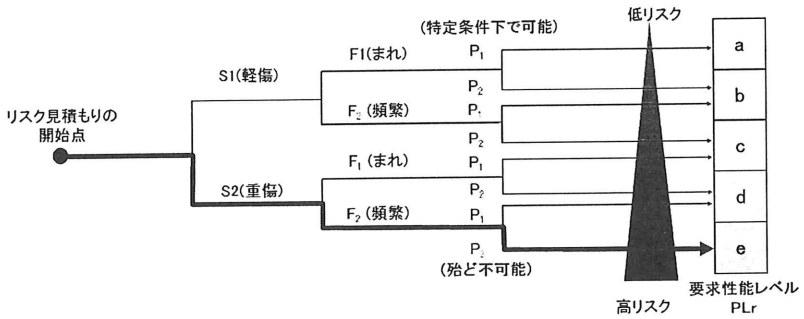


図１２．JIBB9505-1：要求パフォーマンスレベルの見積もり（事例２）

- 使用条件による制御システムの安全性能要求レベルは，図１２より PLe
- 運転操作によるダブルバルブの作動頻度は，10 秒に１回操作を行う。

② 安全関連制御システム構成の説明

- 冗長チャンネル（電気機械機構＋安全関連制御用電気制御機器を使用）
- 光線式安全装置制御ユニット：ＬＧは，メーカーより制御システムの安全性能連レベルが，PLe で　危険側故障確率 $PFHd(LG)=3.0\times10^{-9}/h$ が、確認

が取れている。

- ダブルバルブ（ダイレクトモニタリング機構内臓）の B10d メーカー確認データは，B10d(DV)＝10,000,000 回
- 安全制御 PLC：Kは，メーカーより制御システムの安全性能連レベルが，PLe で　危険側故障確率 PFHD(K)＝2.5×10^{-9}/h が確認が取れている。

③ 安全関連部の各チャネルの安全関連ブロック図

図１１の制御システムの安全関連部のブロック図を**図１３**に示す。

図１３．事例１の安全関連ブロック図

④ 各チャネルの MTTFd とシステムの MTTFd および T10d の確認

②の情報よりここではダブルバルブ以外の確認が取れているのでダブルバルブについて MTTFd と T10d の確認を行う。

- B10d(DV)＝10,000,000 回
- ダブルバルブの年間作動回数 nop（年），
  nop=300 日×20H×720 回(1H/10 秒)＝2,160,000 回/年
- 10%危険側故障に至る平均年数 T10d（年）は，
  T10d(DV)= B10d(DV)/nop＝10,000,000/2,160,000=4.6 (約４年)
- 平均危険側故障間隔時間 MTTF d = B10d/(0.1 × nop)=T10d/0.1 は，
  MTTF d （DV）=4.6 /0.1=46 年

⑤ DC（診断範囲）・DCavg(平均診断範囲)の確認

ダブルバルブの動作は安全制御ユニットにてダブルバルブのダイレクトモニタ接点による状態監視を毎サイクルの起動前に監視されているのでダブルバルブの診断範囲 DC(DV)=99%にできる。(LG/K は,PLe より簡易的に評価から外した。)

従って平均診断範囲 DCavg はバルブのみの評価として DCavg=99% (High)

⑥ CCF の確認(共通原因故障の考慮の確認)

CCF は，事例１同様に実施記録すれば良い。

⑦ カテゴリとパフォーマンスレベル・ PFHD の評価（総合評価）

以下のこれまでの冗長部分（入力＋出力）の設計確認結果をまとめる

- ＣＣＦは，８５点（＞６５点）より，ＣＣＦの要求事項を満足している。

- どの部品の単一故障による安全機能に喪失に至らないことからカテゴリ３の特性と判定できる。
- 平均診断範囲 DC avg は，DC avg = 99% :High（高）レベル
- MFFTd(DV)=46 （年） : High（高）レベル
- JISB9705-1 附属書 K 表 K.1 より MTTF d ＝43 年，Cat.4 を選択すると PLd / PFHd=6.37×10^{-8}(/h) となる。
- 光線式安全装置ＬＧの危険側故障確率 PFHD(K)＝2.5×10^{-9}/h と危険側故障確率 PFHD(K)＝2.5×10^{-9}/h 及び附属書Kの表 K.1 から決定したダブルバルブ 危険側故障確率 PFHD(K)＝6.37×10^{-8}(/h)を加算した値 PFHD(K)＝6.87×10^{-8}(/h)を附属書 K で評価すると PLe / PFHd=6.87×10^{-8}(/h)
- 本システムは，要求パフォーマンスレベル PLe に対して同等であり，本機能に対して制御システムの安全関連部として妥当である。
- 但し，ダブルバルブの T10d(DV)=4.6 年なので４年ごとの交換が必要。

表３．事例２：動力プレス機械の光線式安全装置保護方策　設計検証事例

機械仕様			単位	備考
1	機械の使用期間	30	年	
2	年間稼働日	300	日/ 年	
3	一日の作業時間	20	時間/日	
安全機能（インタロック式ガード）：要求仕様			単位	備考
1	PLr：要求パフォーマンスレベル	e	PL	JISB9705-1:リスク評価より
2	PFHd:平均危険側故障率	–	SIL	
3	設計制御ハード構成	4	Cat.	設計方針：PLeをカテゴリ4で構築
4	安全関連ブロック図	サブシステム 入力部：LG 光線式安全装置 制御ユニット／サブシステム 処理部：K 安全制御 ユニット／サブシステム 出力部：A, B ﾀﾞﾌﾞﾙﾊﾞﾙﾌﾞ		
入力部（安全関連：サブシステム）仕様			単位	備考
1	パフォーマンスレベルPL(LG):光線式安全装置	e	PL	メーカーカタログ値
2	危険側故障確率PFHd(LG)：光線式安全装置	3.0x10^{-9}	1/h	メーカー提供値
3	安全機能：安全装置使用頻度	360	回/時間	使用頻度 10秒/回
処理部（安全関連：サブシステム）仕様			単位	備考
1	パフォーマンスレベルPL(K)：安全PLC	e	PL	メーカーカタログ値
2	危険側故障確率PFHd(K)：安全PLC	2.5x10^{-9}	1/h	メーカー提供値
出力部（安全関連：サブシステム）仕様			単位	備考
1	ダブルバルブ：B10d(DV)	10,000,000	回	メーカーカタログ値
2	安全機能：バルブ使用頻度	360	回/時間	使用頻度 10秒/回
出力部（安全関連：サブシステム）：MTTFd評価			単位	備考
1	ﾀﾞﾌﾞﾙﾊﾞﾙﾌﾞ年間作動回数：Nop(DV)	2,160,000	回/年	
2	ﾀﾞﾌﾞﾙﾊﾞﾙﾌﾞ：T10d(DV)＝B10d(DV)/Nop	4.6	年	交換周期:4年とする。
3	ﾀﾞﾌﾞﾙﾊﾞﾙﾌﾞ：MTTFd(DV)＝T10d(NO)/0.1	46.3	年	
安全関連ブロック図 入力・出力冗長合成 平均診断範囲DCavg評価			単位	備考
2	安全関連ブロック図 ﾀﾞﾌﾞﾙﾊﾞﾙﾌﾞ診断範囲 DC(DV)	99	%	
CCF(共通原因故障)スコア確認			単位	備考
1	安全関連ブロック図 入力・出力合成 CCF	85.0	点	65点以上合格：詳細はCCF確認表
総合評価			単位	備考
1	安全関連ブロック図 PFHd(DV2)	6.37x10^{-9}	1/h	MTTFd=43年/Cat.4/DCavg-High より
設計確認結果	安全関連ブロック図 入力・処理・出力合成 PFHd(Total)	6.87x10-9	1/h	各PFHd加算結果
	安全関連ブロック図 入力・出力合成 PL(Total)	e	PL	JISB9705-1:表K.1 PFHd＝6.87x10-9より
	ﾀﾞﾌﾞﾙﾊﾞﾙﾌﾞ：T10d(DV)＝B10d(DV)/Nop	4.6	年	交換周期:4年とする。

表４．JISB9705-1 附属書 K の表 K.1 評価テーブル

危険側故障の平均確率:PFHd(1/h)及び対応のパフォーマンスレベルPL																
カテゴリ	B		1		2		2		3		3		4			
Dcavg	NONE		NONE		LOW		MEDIUM		LOW		MEDIUM		HIGH			
MTTFd (年)	CCF:65%以上で要求事項を満足															
3	3.800E-05	a			2.580E-05	a	1.990E-05	a	1.260E-05	a	6.090E-06	b				
3.3	3.460E-05	a			2.330E-05	a	1.790E-05	a	1.130E-05	a	5.410E-06	b				
3.6	3.170E-05	a			2.130E-05	a	1.620E-05	a	1.030E-05	a	4.860E-06	b				
3.9	2.930E-05	a			1.950E-05	a	1.480E-05	a	9.370E-06	b	4.400E-06	b				
4.3	2.650E-05	a			1.760E-05	a	1.330E-05	a	8.390E-06	b	3.890E-06	b				
4.7	2.430E-05	a			1.600E-05	a	1.200E-05	a	7.580E-06	b	3.480E-06	b				
5.1	2.240E-05	a			1.470E-05	a	1.100E-05	a	6.910E-06	b	3.150E-06	b				
5.6	2.040E-05	a			1.330E-05	a	9.870E-06	b	6.210E-06	b	2.800E-06	c				
6.2	1.840E-05	a			1.190E-05	a	8.800E-06	b	5.530E-06	b	2.470E-06	c				
6.8	1.680E-05	a			1.080E-05	a	7.930E-06	b	4.980E-06	b	2.200E-06	c				
7.5	1.520E-05	a			9.750E-06	b	7.100E-06	b	4.450E-06	b	1.950E-06	c				
8.3	1.390E-05	a			8.870E-06	b	6.430E-06	b	4.020E-06	b	1.740E-06	c				
9.1	1.250E-05	a			7.940E-06	b	5.710E-06	b	3.570E-06	b	1.530E-06	c				
10	1.140E-05	a			7.180E-06	b	5.140E-06	b	3.210E-06	b	1.360E-06	c				
11	1.040E-05	a			6.440E-06	b	4.530E-06	b	2.810E-06	c	1.180E-06	c				
12	9.510E-06	b			5.840E-06	b	4.040E-06	b	2.490E-06	c	1.040E-06	c				
13	8.780E-06	b			5.330E-06	b	3.640E-06	b	2.430E-06	c	9.210E-07	d				
15	7.610E-06	b			4.538E-06	b	3.010E-06	b	1.820E-06	c	7.440E-07	d				
16	7.130E-06	b			4.210E-06	b	2.770E-06	c	1.670E-06	c	6.760E-07	d				
18	6.340E-06	b			3.680E-06	b	2.370E-06	c	1.410E-06	c	5.670E-07	d				
20	5.710E-06	b			3.260E-06	b	2.060E-06	c	1.220E-06	c	4.850E-07	d				
22	5.190E-06	b			2.930E-06	c	1.820E-06	c	1.070E-06	c	4.210E-07	d				
24	4.760E-06	b			2.650E-06	c	1.620E-06	c	9.470E-07	d	3.700E-07	d				
27	4.230E-06	b			2.320E-06	c	1.390E-06	c	8.040E-07	d	3.100E-07	d				
30			3.800E-06	b	2.060E-06	c	1.210E-06	c	6.940E-07	d	2.650E-07	d	9.540E-08	e		
33			3.460E-06	b	1.850E-06	c	1.060E-06	c	5.940E-07	d	2.300E-07	d	8.570E-08	e		
36			3.170E-06	b	1.670E-06	c	9.390E-07	d	5.160E-07	d	2.010E-07	d	7.770E-08	e		
39			2.930E-06	c	1.530E-06	c	8.400E-07	d	4.530E-07	d	1.780E-07	d	7.110E-08	e		
43			2.650E-06	c	1.370E-06	c	7.340E-07	d	3.870E-07	d	1.540E-07	d	6.370E-08	e		
47			2.430E-06	c	1.240E-06	c	6.490E-07	d	3.350E-07	d	1.340E-07	d	5.760E-08	e		
51			2.240E-06	c	1.130E-06	c	5.800E-07	d	2.930E-07	d	1.190E-07	d	5.260E-08	e		
56			2.040E-06	c	1.020E-06	c	5.100E-07	d	2.520E-07	d	1.030E-07	d	4.730E-08	e		
62			1.840E-06	c	9.060E-07	d	4.430E-07	d	2.130E-07	d	8.840E-08	e	4.220E-08	e		
68			1.680E-06	c	8.170E-07	d	3.900E-07	d	1.840E-07	d	7.680E-08	e	3.800E-08	e		
75			1.520E-06	c	7.310E-07	d	3.400E-07	d	1.570E-07	d	6.620E-08	e	3.410E-08	e		
82			1.390E-06	c	6.610E-07	d	3.010E-07	d	1.350E-07	d	5.790E-08	e	3.080E-08	e		
91			1.250E-06	c	5.880E-07	d	2.610E-07	d	1.140E-07	d	4.940E-08	e	2.740E-08	e		
100			1.140E-06	c	5.280E-07	d	2.290E-07	d	1.010E-07	d	4.290E-08	e	2.470E-08	e		

⑧　ソフトウエアの評価

カテゴリとパフォーマンスレベル・ PFHD の評価は，PLe として満足しているが，動力プレス機械を含め全ての機械において安全 PLC を使用した場合はソフトウエアの妥当性も機能安全の妥当性確認として必要である。機械安全の制御システムの安全関連部のソフトウエア設計の選択について JISB9705-1 をもとに図１４に示した。安全 PLC のソフトウエアは，一般にラダー言語，ファンクションブロック図などＬＶＬ（制約可変言語）に分類されるソフトウエア言語で記述される。

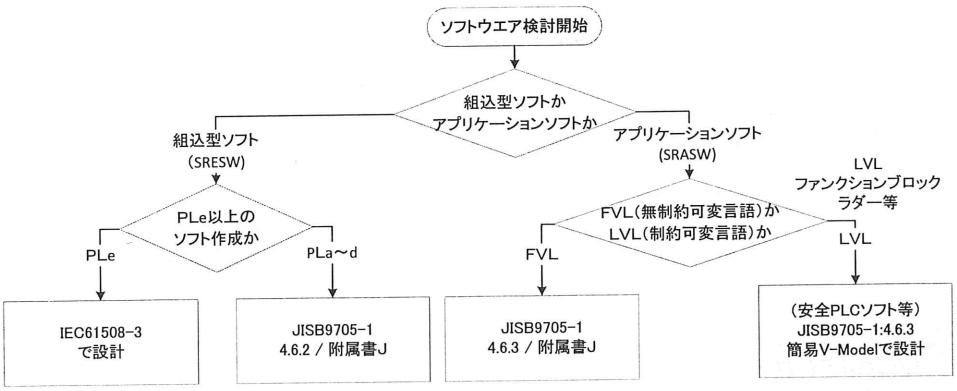


図１４．制御システムの安全関連部のソフトウエア設計の選択

図１４で示されている安全 PLC による機械における制御システムの安全関連部のソフトウエア設計についてその設計検証手順として簡易 V-Model が示されている。この簡易 V-Model は，現在も機械安全における機能安全の国際規格でも審議されているが，機械の制御システムの安全関連部のソフトウエア設計を行うのに有益な内容であるので図１５に示す。

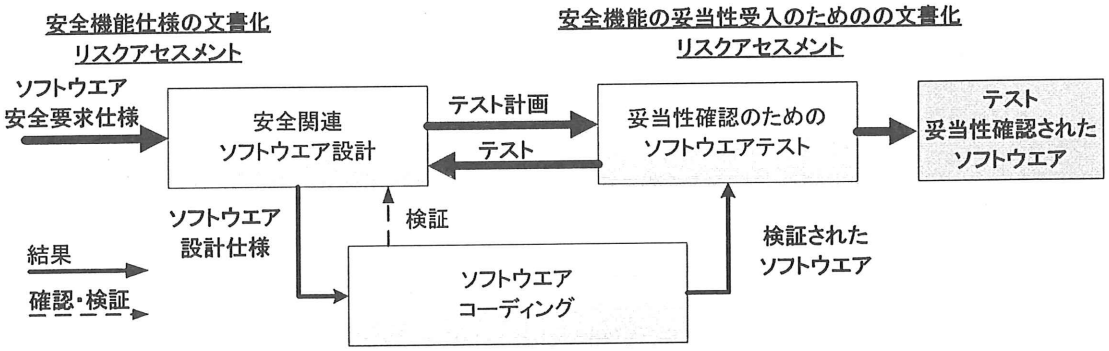


図１５．安全ＰＬＣ(SRASW)ソフトウエアの開発手順（簡易 V-Model）

一般的な安全 PLC のソフトウエアは，機械設計者が簡単に使用できるアプリケーションソフトウエア作成のためのツールが各安全 PLC メーカーで準備されている。そしてそのツールは，制御システムの安全関連部のソフトウエアを作成に適切であることの証明がなされていることが大前提で安全 PLC が構成されている。ソフトウエアの設計者は，ソフトウエア作成前にまず制御システムの安全関連部のソフトウエアを作成に適切なソフトウエアか確認することが重要である。ここでは安全 PLC を使用した時の妥当性確認に必要な作業と文書化の項目について以下に示す。

機械の制御システムの安全関連部のソフトウエア設計を行う機械設計者，製造者は，安全関連部のソフトウエアを作成した際は，図 15 に示した流れでソフトウエアの機能テストを実施必要がある。ソフトウエア安全要求仕様書，ソフトウエア設計仕様書に示された機能が達成されているかを保証するのが機能テストである。以下に安全 PLC で機械の制御システムの安全関連部のソフトウエアを構築する際に一般的に必要と思われる文書を示す。

ア　リスクアセスメント
イ　ハード構成
ウ　ソフトウエア要求仕様書
エ　テスト計画書
オ　設計仕様書
カ　機械の制御システムの安全関連部のソフトウエアの記述（コーデング）

キ　テスト結果（テストレポート）

安全 PLC ソフトの妥当性説明のために上記以外にも設計，検証過程を記録として残すことが推奨される。

参考として，図 16 に現在 JISB9705-1 で示されている一般的なソフトウエア開発のための V—Model を示す。

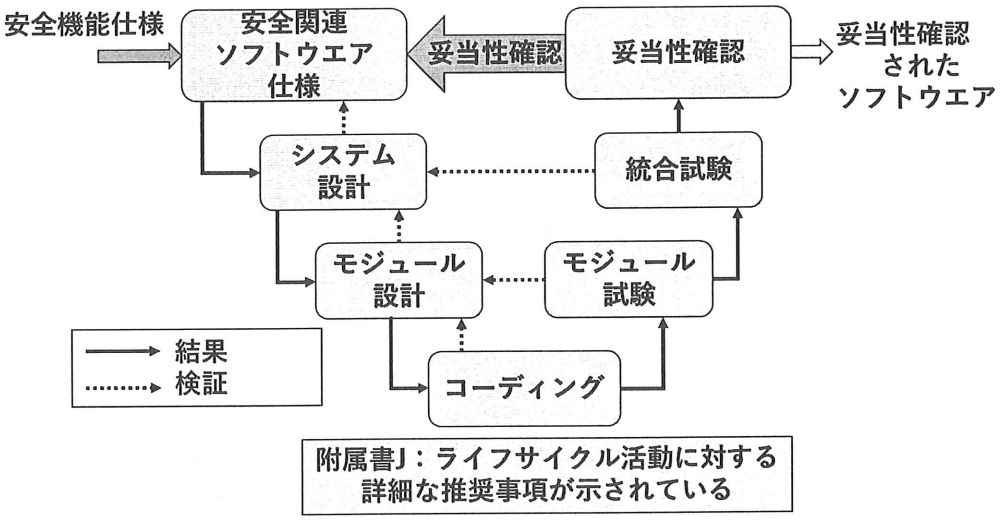


図１６．ソフトウェア安全ライフサイクルの単純化 V モデル

4　動力プレス機械リスクへの機能安全の適用による規制緩和の可能性

(1)　機能安全の適用による規制緩和の可能性

動力プレス機械に関する機能安全が適用できる方策として以下への適用が考えられる。以下の装置は，動力プレス機械構造規格，プレス機械又はシャーの安全装置構造規格，安全装置管理指針等に装置の性能，設置，運用について規定されている。しかしながらグローバルな視点で考えると日本国家規格（JIS），機械安全の国際規格（ISO/IEC）の適用が求められる。ここでは以下に示した保護装置について JIS，IEC/ISO を適用した場合の日本国内における規制緩和の可能性について検討する。

ア　光線式安全装置

イ　両手操作式安全装置（両手操作制御装置）

ウ　インタロックガード式安全装置

(2)　光線式安全装置適用についての規制緩和

光線式安全装置は，日本国内で動力プレス機械に適用する場合，「プレス機械又はシャーの安全装置構造規格」による型式検定が義務付けられている。本構造規格を JIS 規格（ISO/IEC 規格）で対応する場合，光線式装置自体の構造要件に関連する規

格，設置に関する規格がある。以下に装置に関連する規格，設置に関連する規格がある以下にその規格を動力プレス機械に適用した場合について示す。

ア　JISB9704-1（IEC61496-1）「電気的検知保護設備－第 1 部：一般要求事項及び試験」：動力プレス機械の場合，本規格内に示されているタイプ４が適用される。

イ　JISB9704-2（IEC61496-2）「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」

ウ　JIS-B9715（ISO13855）「人体部位の接近速度に基づく保護設備の位置決め」：この規格には前面から人が危険源に近づく場合の人の移動速度に基づく安全を確保するめの光線式安全装置の設置に関する危険源からの最小距離（離して設置するための最低限の距離：最小距離）を算出する基準，及び光線式安全装置の設置高さに対して光線式安全装置の上から危険源に接近する場合の最小距離に対する追加距離の基準が示されている。

以上，構造規格など現状の日本の法令で示されている基準と比較すると JIS 基準は，現状の法令で示されている基準と同等以上と判断できる。従って規制緩和の可能性については以下が提案できる。

ア　JISB9704-1（IEC61496-1），JISB9704-2（IEC61496-2）準拠したタイプ４の光線式安全装置については，「プレス機械又はシャーの安全装置構造規格」の構造要件は満足しているものとして型式検定の構造に関する検査対象からはずすことができると考えられる。

イ　アで示した光線式安全装置を使用して，JIS-B9715（ISO13855）の設置基準及び動力プレス機械の制御システムにおいて保護蔵置としての機能安全説明が出来ている場合は，「動力プレス機械の構造規格」の光線式の危険防止機構を満足しているとして光線式の危険防止機構を有する安全プレスの制御システムに関する検査対象から外すことができると考えられる。

(3)　両手操作式安全装置適用についての規制緩和

両手操作式安全装置についても，日本国内で動力プレス機械に適用する場合，「プレス機械又はシャーの安全装置構造規格」による型式検定が義務付けられている。本構造規格を JIS 規格（ISO/IEC 規格）で対応する場合，両手操作式装置自体の構造要件に関連する規格，設置に関する規格がある。以下に装置に関連する規格，設置に関連する規格について動力プレス機械に適用した場合を示す。

ア　JIS-B9712 (ISO13851)_両手操作制御装置―機能的側面及び設計原則：動力プレス機械の場合，本規格内に示されているタイプⅢC が両手操作式安全装置として適用される。タイプⅢC は両手操作式安全装置の中でも最高レベルの装置で制御システムの機能安全においてカテゴリ４に相当する。また，両手操作の同時性だ

けでなく 0.5 秒以内の両手操作の同期生が要求事項として求められている。表４に JIS-B9712 (ISO13851)で示されている両手操作制御装置の要求事項を示す。

表４．各両手操作制御装置の要求事項

要求事項	適用箇条	タイプ				
		Ⅰ	Ⅱ	Ⅲ		
				A	B	C
両手の使用(同時操作)	5. 1	○	○	○	○	○
入力信号と出力信号間の関係	5. 2	○	○	○	○	○
出力信号の停止	5. 3	○	○	○	○	○
偶発的操作の防止(箇条8. 9で規定)	5. 4	○	○	○	○	○
機能不良の防止(箇条8. 9で規定)	5. 5	○	○	○	○	○
出力信号の再開始	5. 6	○	○	○	○	○
同期操作(0.5秒以下の同期性)	5. 7	注)		○	○	○
カテゴリ1の使用(タイプⅠ・ⅢA)	6. 2	○		○		
カテゴリ3の使用(タイプⅡ・ⅢB)	6. 3		○		○	
カテゴリ4の使用(タイプⅢC)	6. 4					○
○:適用される要求事項 注)リスクアセスメントで同期性・再開始特性が無視できるか決定要.(箇条8. 6を確認)						

イ　JIS-B9715 (ISO13855)「人体部位の接近速度に基づく保護設備の位置決め」: この規格は，光線式安全装置でも示したが，人が危険源に近づく場合の人の移動速度に基づく安全を確保するめの危険源からの最小距離（離して設置するための最低限の距離：最小距離）を算出基準として両手操作式安全装置でも使用する。

以上，構造規格など現状の日本の法令で示されている基準と比較すると JIS 基準は，現状の法令で示されている基準と同等以上と判断できる。従って規制緩和の可能性については以下が提案できる。

ア　JIS-B9712 (ISO13851)で示されているタイプⅢC であれば両手操作式安全装置については,「プレス機械又はシャーの安全装置構造規格」の構造要件は満足しているものとして型式検定の構造に関する検査対象からはずすことができると考えられる。

イ　アで示した両手操作式安全装置を使用して，JIS-B9715 (ISO13855) の設置基準及び動力プレス機械の制御システムにおいて保護蔵置としての機能安全説明が出来ている場合は,「動力プレス機械の構造規格」の両手操作式の危険防止機構を満足しているとして両手操作式の危険防止機構を有する安全プレスの制御システムに関する検査対象から外すことができると考えられる。

(4)　インタロックガード式安全装置適用についての規制緩和

インタロックガード式安全装置も日本国内で動力プレス機械に適用する場合,「プ

レス機械又はシャーの安全装置構造規格」による型式検定が義務付けられている。本構造規格をJIS規格（ISO/IEC規格）で対応する場合，インタロックガード式安全装置自体の構造要件に関連する規格，設置に関する規格がある。以下に装置に関連する規格，設置に関連する規格がある以下にその規格を動力プレス機械に適用した場合について示す。

ア　JISB9716（ISO14120）「ガード―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」

イ　JISB9710（ISO14119）「ガードと共同するインタロック装置―設計及び選択のための原則」

ア，イの規格は，ガードの構造とインタロックに関連する規格で，これらの規格で示されている要求事項と機能安全を組み合わせることでインタロックガード式安全装置が構造的に「プレス機械又はシャーの安全装置構造規格」を満足したものと同等となる。

ウ　JIS-B9715（ISO13855）「人体部位の接近速度に基づく保護設備の位置決め」:この規格は，ガードがいつでも開くことができるインタロックガード式安全装置において前面から人が危険源に近づく場合の人の移動速度に基づく安全を確保するためのインタロックガード式安全装置の設置に関する危険源からのの最小距離（離して設置するための最低限の距離：最小距離）を算出する基準が示されている。

以上，構造規格など現状の日本の法令で示されている基準と比較するとJIS基準は，現状の法令で示されている基準と同等以上と判断できる。従って規制緩和の可能性については以下が提案できる。

ア　JISB9716（ISO14120），JISB9710（ISO14119）と機能安全が適用されたインタロックガード式安全装置は，「プレス機械又はシャーの安全装置構造規格」の構造要件は満足しているものとして型式検定の構造に関する検査対象からはずすことができると考えられる。

イ　アで示した光線式安全装置を使用して，JIS-B9715（ISO13855）の設置基準及び動力プレス機械の制御システムにおいて保護蔵置としての機能安全説明が出来ている場合は，「動力プレス機械の構造規格」のインタロックガード式の危険防止機構を満足しているとしてインタロックガード式の危険防止機構を有する安全プレスの制御システムに関する検査対象から外すことができると考えられる。

以上，ここで示した各危険防止機構，安全プレスにおいては，グローバルな視点で考えると日本国家規格（JIS），機械安全の国際規格（ISO/IEC）に従った構造に機能安全を組み込むことで「動力プレス機械構造規格」，「プレス機械又はシャーの安全装置構造規格」に適合が求められている型式検定において将来的に規制緩和の可能性が考えられる。

V　機械の安全関連システム/制御装置の安全関連部の性能/レベルに関する認証機関に関する現状と今後について

本編では、認証機関とはどのような枠組みの中で活動しているかを簡単に紹介したうえで、日本の認証機関に関する現状と今後について述べる。

1.　認証機関、試験機関と認定機関

認証機関[1]が適切に認証を行うことを担保するために、特定分野の認証機関を除き、国際的にはISO/IEC 17065 (JISQ 17065; 適合性評価 － 製品、プロセス及びサービスの認証を行う機関に対する要求事項)が制定されている。

一方、認証機関とは別に試験を行い、その結果を評価する機関には ISO/IEC 17025 (JISQ 17025; 試験所及び校正機関の能力に関する一般要求事項) の適用が要求される。

さらに、認証機関と試験機関を認定する機関にはISO/IEC 17011 (JISQ 17011; 適合性評価−適合性評価機関の認定を行う機関に対する一般要求事項)の適用が要求され、権威のある機関から公認される (図 1)。

例えば、英国であれば、国の財政的支援で運営されている非営利団体の認定機関、UKAS (United Kingdom Accreditation Service) が存在し、UKAS が認定した認証機関(例　Sira (現 CSA UK))、また、日本では、国際的な機関 IAF(International Accreditation Forum, Inc.)　傘下の JAB が認定した認証機関(例　公益社団法人産業安全技術協会)などがある。

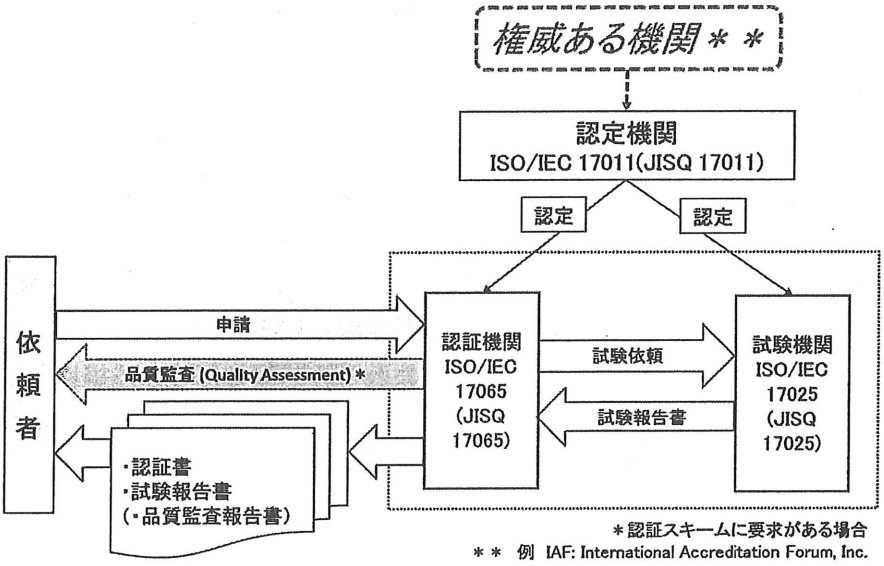


図 1　認証機関、試験機関、認定機関の関係

[1] 本編では、「認証機関」(Certification Body) は JISQ 17065 の定義に従って使用している。

2. 日本の現状

(1) 法律に基づく検定、検査機関

日本の検定／検査機関[2]は多くの場合、法律に基づき登録されている（図 2)。

労働安全衛生法（以下、「法」）のもとでは、例えば、以下のような登録検定／検査機関が存在する。

（一社）日本ボイラ協会、（公社）ボイラ・クレーン安全協会、
（公社）産業安全技術協会、(一社)日本クレーン協会

法により検定合格が要求される強制品目であれば、その技術基準は明確なので登録検定／検査機関が発行する合格証は、国内は必須要求として、海外にも受け入れられる可能性はある。

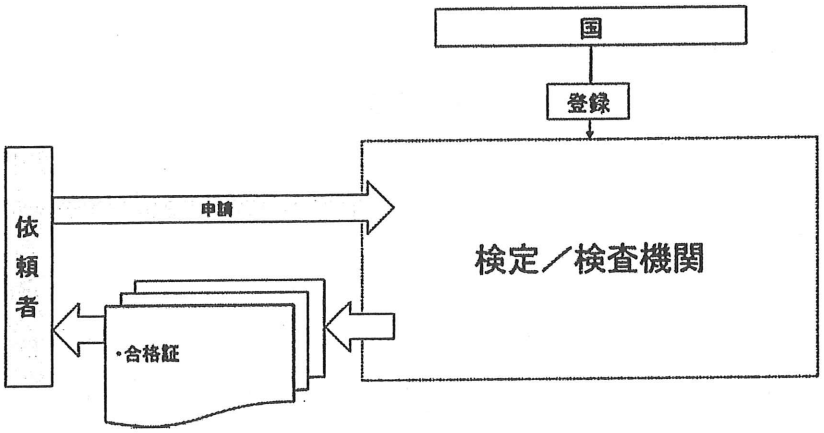


図 2　法律に基づく検定／検査機関

(2) 日本の現状

登録検定機関や登録検査機関は法の規定に基づき登録されており、法に基づく技術基準を適用して評価した結果については、海外でも受け入れられる可能性が高い。しかしながら、強制品目であっても技術基準にない要求事項（例えば、最新の ISO/IEC 規格で追加された、あるいは、欧州指令の整合規格による要求事項）の評価には、多くの場合、ISO/IEC 17065 や 17025 の下での評価結果が要求される。

例えば、防爆分野では機能安全の要求が含まれるガス検知器の性能規格[3]、EN 60079-29-1（Gas detectors - Performance requirements of detectors for flammable gases)、

---

[2] 労働安全衛生法より引用。ちなみに、法務省からの外部リンク "Japanese Law Translation　(http://www.japaneselawtranslation.go.jp/?re=01)" では、検定機関は "Examination Agency"、検査機関は "Inspection Agency" という単語を使用し、ISO/IEC 17065 で使用されている Certification Body とは区別されている。

[3] EN 60079-29-1 の機能安全要求は IEC 61508 が引用されている。

はATEX指令の整合規格[4]である。しかし、日本の検定に適用される工場電気設備防爆指針にはEN 60079-29-1がカバーされていないため、欧州の事業者は第三者認証の証明書、特に機能安全評価の第三者認証の証明書の提出を製造者に要求することが多い。製造者がこの要求に応えようとしても日本では、この受け皿、すなわちISO/IEC 17065や17025で認定されたIEC 61508に基づく証明書を発行できる機関が存在しない。

日本における認定上の問題点がもう一つ存在する。防爆電気機器の検定に使用される技術基準は原則最新のIEC 60079（爆発性雰囲気）シリーズに整合しているが、日本のISO/IEC 17025の認定では、それら規格の試験項目ごとに認定証が発行される。一方、UKASにより発行される認定では、規格ごとに認定証が発行されている。

試験機関に試験結果報告書を要求する製造者は、規格ごとに発行される証明書を要求するのは当然なので、現状の日本の認定制度はマーケットの要求にマッチしていないと感じるところである。

3. 今後（日本で第三者認証機関を育てるシステム作り）

EMCのIEC 61000シリーズ、環境試験 IEC 60068シリーズ、または、保護等級IEC 60529などの規格が、あらゆる分野別規格に取り込まれているように、今後、機能安全規格 IEC 61508は多くの分野別規格に入ってくることは間違いない。ちなみに**表1**に例を示すように分野別規格に既に取り込まれている。

EMC試験や環境試験の分野では、多くの試験機関がISO/IEC 17025による認定を受けており、これら機関を上手に使って、製造者自身が自己宣言できるシステムができていると思われる。

同様に基本規格のIEC 61508をカバーする認証機関を作ることで、EMC試験や環境試験と同様に容易に外部委託できる体制を作ることで、日本の製造者が国際競争の土俵に立ちやすくなると考えられる。

そのために英国UKASと同様に行政のバックアップで早くIEC 61508をカバーする認定機関を作る必要があると考える。また、規格に規定される試験項目ごとに認定証が発行されるシステムではなく、規格ごとに認定証が発行されることを希望するところである。

以上

---

[4] ATEX指令の整合規格であるが、これらの規格に対しては自己宣言によって適合性を表明すればよい。

表　IEC 61508 による評価を要求している分野別規格例

分野	ISO/IEC 規格	対応 JIS	規格名称
産業用機械	IEC 62061	JISB 9961	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
医療機器	IEC 62304	JIST 2304	医療機器ソフトウェア　―　ソフトウェアライフサイクルプロセス
自動車	ISO 26262s	－	Road vehicles -- Functional safety
鉄道	IEC 62278	－	Railway applications - Specification and demonstration of reliability, availability, maintainability and safety (RAMS)
原子力	IEC 61513	－	Nuclear power plants - Instrumentation and control important to safety - General requirements for systems
ロボット	ISO 10218-1	JISB 8433-1	ロボット及びロボティックデバイス－産業用ロボットのための安全要求事項－第１部：ロボット
可変速電力駆動システム	IEC 61800	－	Adjustable speed electrical power drive systems
プロセス産業	IEC 61511-1	JISC 0511-1	機能安全－プロセス産業分野の安全計装システム－第１部：フレームワーク，定義及びシステム・ハードウェア・ソフトウェアの要求事項
防爆	IEC 60079-29-1/-3	－	Gas detectors - Performance requirements of detectors for flammable gases / Explosive atmospheres - Part 29-3: Gas detectors - Guidance on functional safety of fixed gas detection systems
	IEC 60079-33	－	Explosive atmospheres - Part 33: Equipment protection by special protection 's'
フィールドバス	IEC 61784s	－	Industrial communication networks - Profiles

試験所

認定証

認定番号 RTL01930

機　関　名　称：公益社団法人 産業安全技術協会

所　在　地：埼玉県狭山市広瀬台二丁目16番26号

貴機関は本協会の下記の基準に適合していることが認められましたので、ここに試験所として認定します。

適　用　基　準：JIS Q 17025:2005 (ISO/IEC 17025:2005)

認　定　範　囲：産業安全機械器具試験（附属書による。）

事　業　所：附属書による。

有　効　期　限：2018年4月30日

この認定は貴機関が認定範囲においてISO/IEC 17025:2005の技術的能力要求事項およびマネジメントシステム要求事項を満たしていることを証明するものです。ISO/IEC 17025:2005のマネジメントシステム要求事項はISO 9001:2008の原則を満たし、その関連する要求事項に沿ったものです。

第8回改定日　2015年9月11日
第2回更新日　2014年4月15日
初回認定日　2006年4月28日

公益財団法人 日本適合性認定協会

理事長　久米 均　　試験所認定委員会 委員長　小田 哲治

管理番号：RTL01930-20150911

認定番号	RTL01930

認定証 附属書

試験所・校正機関の別	試験所
機関名称	公益社団法人 産業安全技術協会
機関所在地	埼玉県狭山市広瀬台二丁目１６番２６号

1) 試験を実施する事業所

事業所名称	公益社団法人 産業安全技術協会	
同 所在地	〒	350-1328
	住所	埼玉県狭山市広瀬台二丁目１６番２６号
恒久的施設で行う試験か、現地試験かの別	☑ 恒久的施設で行う試験 □ 現地試験	

認定範囲

分類コード	クラス	試験規格及び詳細	サンプリング
M31.1.1	防爆構造電気機械器具	IEC 60079-0　26.4.2、26.5.1 IEC 60079-1　15.2、15.3 IEC 60079-11　10.1、10.3	×
M31.2.1	安全靴	JIS T 8101　9.1、9.2、9.6	×
M31.2.5	防護服	JIS T 8124-1　4.3.2 JIS T 8124-2	×

公益財団法人 日本適合性認定協会

管理番号：RTL01930-20150911

UKAS PRODUCT CERTIFICATION 0011 Accredited to EN 45011:1998 (ISO/IEC Guide 65:1996) to provide product conformity certification	**Schedule of Accreditation** issued by **United Kingdom Accreditation Service** 21 - 47 High Street, Feltham, Middlesex, TW13 4UN, UK **Sira Certification Service** **Issue No:** 062 **Issue date:** 04 November 2014

DETAIL OF ACCREDITATION

Product	Standard
At the last review of Form 3002 the following standards were included within the scope of accreditation, other standards may have since been added using the flexible scope arrangement Electrical apparatus for potentially explosive atmospheres using the following protection concepts: General requirements	Flexible scope enabling new versions, or technically equivalent versions, of existing accredited standard test methods to be introduced in accordance with Sira's documented in house procedure IEC 60079-0:2011 IEC 60079-0:2007 IEC 60079-0:2006 IEC 60079-0:2004 (withdrawn) IEC 60079-0:2000 (withdrawn) IEC 60079-0:1998 (withdrawn) EN 50014:1997 (withdrawn) EN 50014:1992 (withdrawn) EN 50014:1977 (withdrawn)
Flameproof enclosures 'd'	IEC 60079-1:2007 IEC 60079-1:2003 IEC 60079-1:1983 (withdrawn) IEC 60079-1:1971 (withdrawn) EN 50018:2000 (withdrawn) EN 50018:1994 (withdrawn) EN 55018:1977 (withdrawn)
Pressurised apparatus 'p'	IEC 60079-2:2007 IEC 60079-2:2001 (withdrawn) IEC 60079-2:1983 (withdrawn) EN 50016:2002 (withdrawn) EN 50016:1995 (withdrawn) EN 50016:1977 (withdrawn) EN 50016:1977 (withdrawn)
Powder filling 'q'	IEC 60079-5:2007 IEC 60079-5:1997 (withdrawn) EN 50017:1998 EN 50017:1994 (obsolescent) EN 50017:1977 (withdrawn)

機能安全を活用した機械設備の安全確保

平成 27 年度　厚生労働省委託
国内外における機械安全規格の調査事業

平成 28 年 3 月
中央労働災害防止協会　　技術支援部
〒108-0014　東京都港区芝 5－35－1
TEL 03-3452-6375 FAX 03-5445-1774
E メール　sidouka@jisha.or.jp

中央労働災害防止協会　技術支援部　2016.3