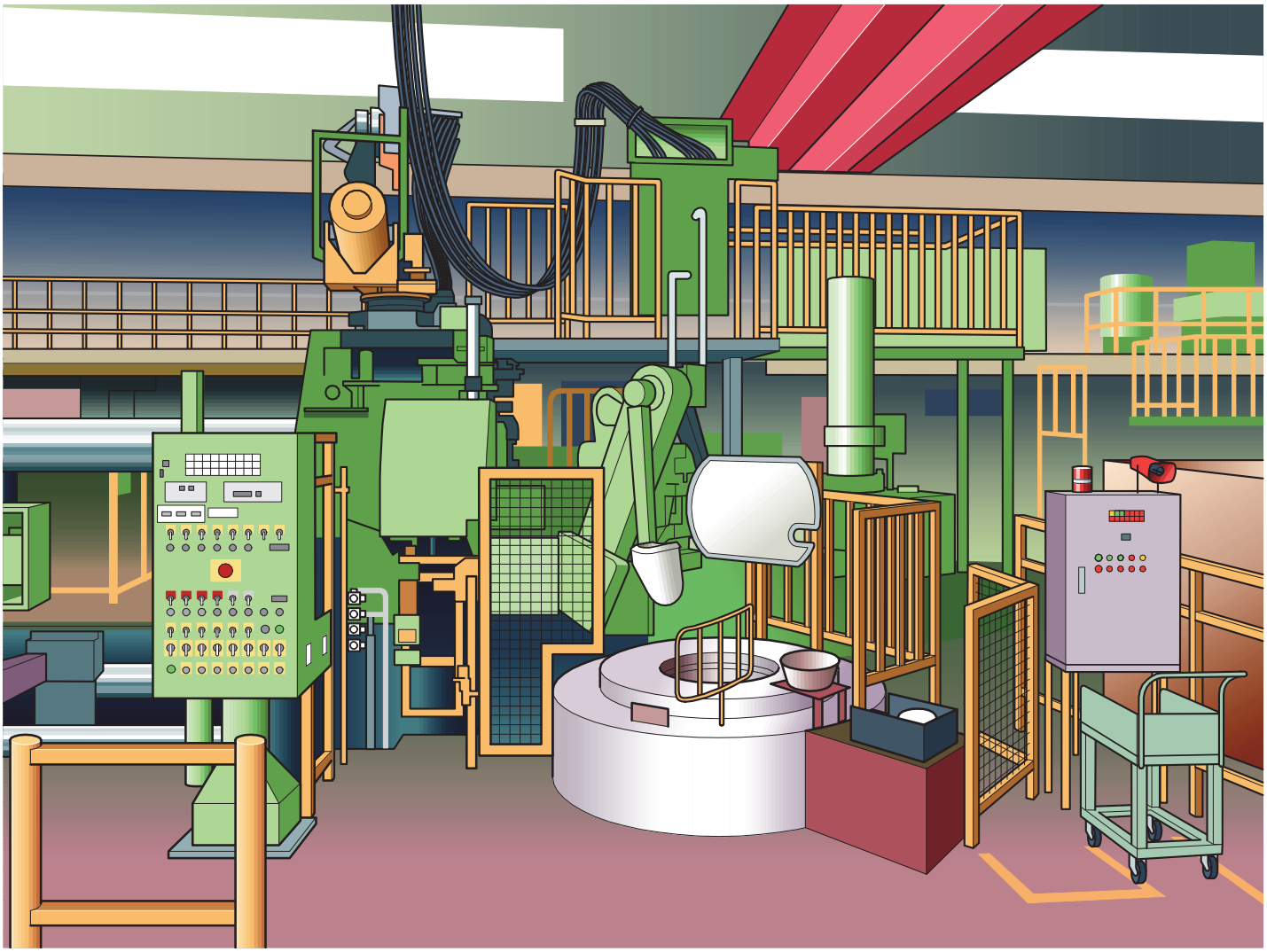
機能安全を
ご存じですか!?

機能安全が可能にする機械の安全確保

（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」）



「機能安全」（Functional Safety）という言葉をご存じですか。
最近いろいろな分野での「安全」のための方策を考えるときに
盛んに使われるようになっています。
機能安全とは何か、それによってどんな安全がもたらされるか探ってみましょう。

平成28年3月
中央労働災害防止協会

機能安全とは

「機能安全」という言葉は、日本規格協会のパンフレットでは、「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」と説明されています。具体的には、以下の３点によって実現されます。(IEC61508-1、IEC61508-4)

① 機械等を製造する者（以下「製造者」という。）は、リスク解析を用いて、被制御機器（EUC）の潜在危険、危険状態及び危険事象を全ての運転モードで明確化し、危険事象に関して安全な状態を達成又は保持するために要求される安全機能（要求安全機能）を特定する。

↓

② 製造者は、要求安全機能を実行する電気・電子・プログラマブル電子（E/E/PE）制御によるシステム（安全関連システム）に要求される安全度の水準（要求安全度水準等。パフォーマンスレベル（PL）又は安全度水準（SIL）。）を決定する。

↓

③ 製造者は、要求安全機能ごとに、要求安全度水準等を満たすように、安全関連システムの要求事項を決定する。

厳密な定義は、国際規格 IEC61508「電気・電子・プログラマブル電子安全関連系の機能安全」のなかで、「被制御機器（EUC）と被制御機器（EUC）制御系の全体に関する安全のうち、電気・電子・プログラマブル電子（E/E/PE）安全関連系、他リスク軽減措置の正常な機能に依存する部分」とされています。

被制御機器（EUC）は、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、プラントなどがそれに当たります。被制御機器（EUC）制御系は、プロセス及び / 又は運転員からの入力信号に応答して、被制御機器（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を言います。

そこで、ここでは、**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」**と呼ぶことにします。

具体的には、人を検知して機械を止めるライトカーテン、圧力検知マットスイッチや、非常停止装置などを思い浮かべればよいでしょう。

安全関連部

機能安全の役割を担う制御システムの部分を、IEC61508 の傘下の機械安全関連規格である IEC62061「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」では**「安全関連システム」**と呼び、ISO12100 の下で、制御システムで機能的安全を扱うときに参照するための規格 ISO13849-1「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」では**「制御システムの安全関連部」**と称しています。IEC61508 では、「安全関連系」として図 1 のように位置付けています。これらは全て同じものといえます。

ここでは、これらをまとめて**「安全関連部」**と呼ぶこととします。

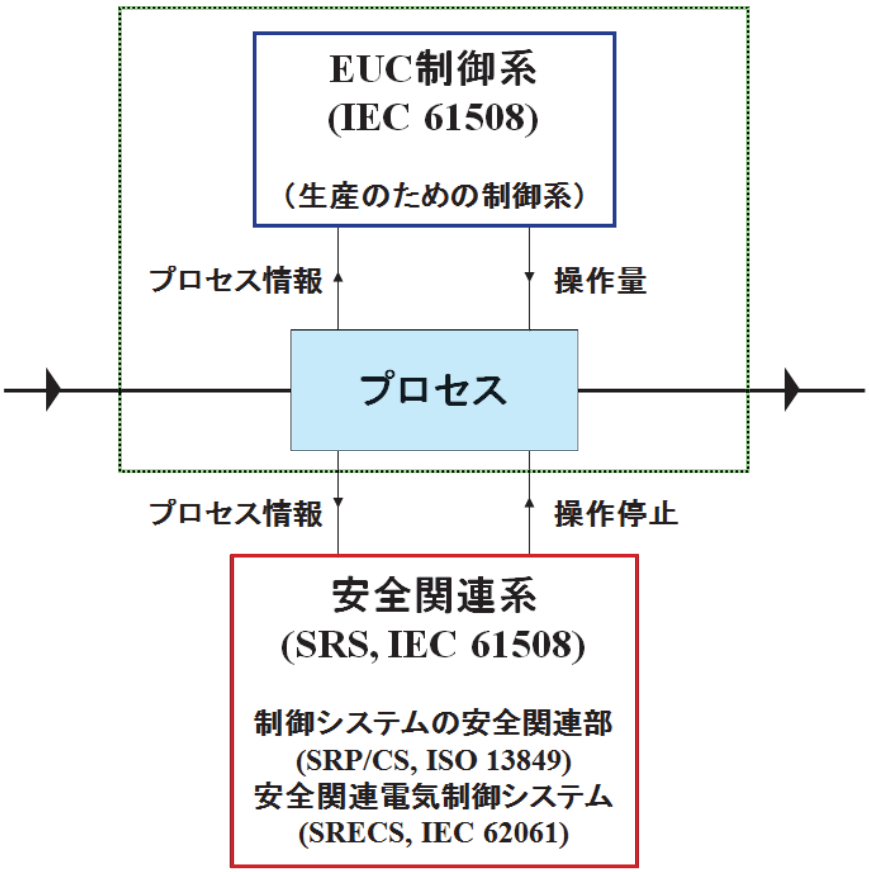


図 1　IEC61508 示される安全関連部

安全関連部の性能:
要求パフォーマンスレベル (PL) と要求安全度水準 (SIL) の決定

安全関連部により、機能安全が達成されることになるのですが、その達成度合いについても国際規格の中で決められています。

その一つが、ISO13849-1 の中で出てくるパフォーマンスレベル (PL) で、もう一つが IEC62061 と IEC61508 で出てくる安全度水準 (SIL) です。PL や SIL のレベルは安全の機能で防護しようとする危険事象のリスクの大きさによって、どのくらいのレベルが必要になるかが決まります。

安全関連部に要求される安全機能の性能レベルの求め方は 2 種類あります。1 つは、個別安全規格すなわち個別の機械などの規格に規定された PL 又は SIL のレベルがあるとき、当該機械に適用可能か確認のうえ、それに従うやり方です。例えば工作機械 (旋盤) では ISO23125:2015 の中で、パートごとに安全関連部の要求カテゴリーと要求パフォーマンスレベルが示されています。

もう一つの求め方は、規格の中で示された方法によりリスクを見積り、それに見合った PL 又は SIL を決めるやり方です。

1 ISO13849-1 に示されるリスクグラフ法

ISO13849-1 では、付属書 A において安全関連部に要求される PL である PLr の求め方を、リスクグラフ法で示しています。図 2 の 1 を基点として、対象となる危険源が顕在化した場合に想定される危害のひどさ (S) 、危険源のばく露の頻度及び時間 (F) 、危険源からの回避又は危害の制限の可能性 (P) を選びながら右に進み、最後に要求パフォーマンスレベル (PLr) が求められるというものです。

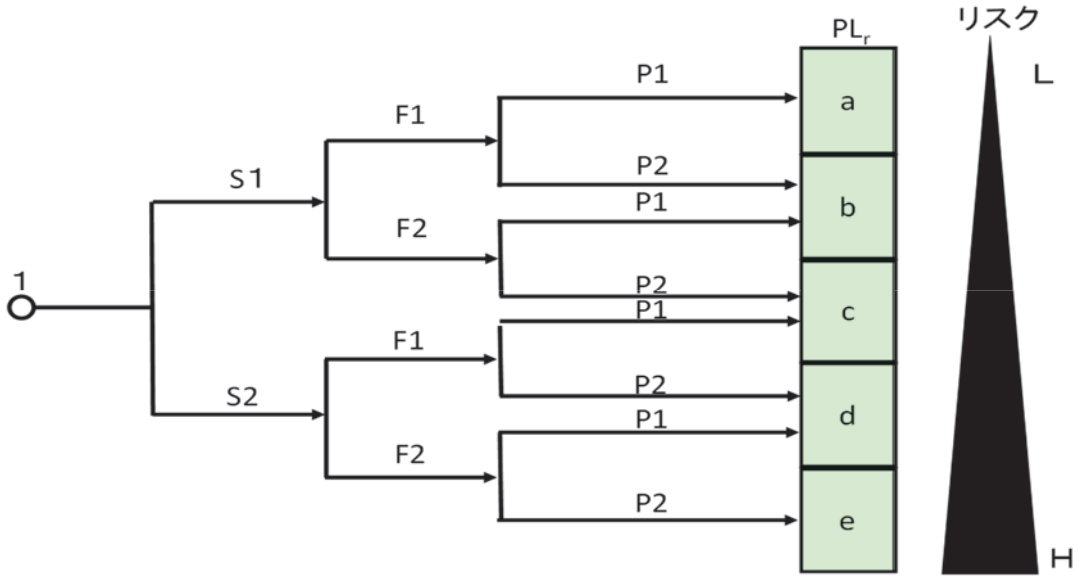


図 2　リスクグラフ法による PLr の決め方

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

2 IEC62061 に示されるハイブリッド法による要求 SIL の求め方

一方、要求安全度水準（要求 SIL）については、IEC62061 に示されるマトリックス法と加算法を合わせたハイブリット法が用いられます。表 1 に示すように危害のひどさのレベル（*Se*）に対し、ばく露レベル（*Fr*）、発生確率（*Pr*）、危険回避／限定可能性（*Av*）の 3 つの要素のレベルを足し合わせた数値で構成されるマトリクスで、要求安全度水準（要求 SIL）を求めます。

なお、この表自体は、もともと ISO／TR14121-2 に示されたもので、「IEC62061 付属書 A の SIL の割付に使われる」とされているものです。

表 1　ハイブリット法による要求 SIL の求め方

危害のひどさ	*Se*	**クラス** Cl=*Fr*+*Pr*+*Av*					**ばく露レベル** *Fr*	**発生確率** *Pr*	**回避／限定**可能性 *Av*
		4	5-7	8-10	11-13	14-15			
回復不可能 死亡、目・腕の喪失	4	SIL2	SIL2	SIL2	SIL3	SIL3	1 時間以内 Fr=5	とても高い Pr=5	
回復不可能 手足骨折・指喪失	3		(OM)	SIL1	SIL2	SIL3	1 時間～1 日 Fr=5	起こりやすい Pr=4	
回復可能 医師の治療が必要	2			(OM)	SIL1	SIL2	1 日～2 週 Fr=4	時々起こる Pr=3	不可能 Av=5
回復可能 応急手当	1				(OM)	SIL1	2 週～1 年 Fr=3	まれに起こる Pr=2	まれには可能 Av=3
							1 年超え Fr=2	無視できる Pr=1	かなり可能 Av=1

ここで、（OM）は、安全関連システム以外の安全方策を推奨していることを示します。

パフォーマンスレベル (PL) と安全度水準 (SIL) の尺度

安全関連部の PL 又は SIL は、当該安全関連部の安全機能の危険側故障確率 (PFHd (1/h)) で定義されています。表 2 と表 3 を参照すると、PLb と PLc が SIL1 に相当するのが分かります。

表 2　パフォーマンスレベル (PL)

パフォーマンスレベル (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	$3 \times 10^{-6} \leqq PFH_d < 10^{-5}$
c	$10^{-6} \leqq PFH_d < 3 \times 10^{-6}$
d	$10^{-7} \leqq PFH_d < 10^{-6}$
e	$10^{-8} \leqq PFH_d < 10^{-7}$

表 3　安全度水準 (SIL)（高頻度モード）

安全度水準 (SIL)	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	$10^{-8} \leqq PFH_D < 10^{-7}$

なお、パフォーマンスレベル (PL) については、カテゴリー、診断範囲 (DC) 、共通原因故障 (CCF) への配慮が、また SIL については、安全側故障比率、冗長性 (ハードウエア・フォールト・トレランス HFT) の評価・制約があります。

機能安全に関連する国際規格

機能安全に関連する国際規格のうち、機械安全に関するものは以下のとおりです。(図 3 参照)

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、これをもとに 1999 年に ISO13849-1 が制定され、制御システムの安全関連部を設計するための基準となりました。

2000 年に、電子・電気機器製造、設計者のための基本規格として IEC61508 が発行され、2005 年に、機械安全に特化した規格として IEC62061 が発行されました。2006 年の改正により、ISO13849-1 は、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パフォーマンスレベル (PL) を導入しました。

さらに、2010 年に制御システムの設計を行うためのガイドラインとして、ISO/TR23849、IEC/TR62061-1 が発行されました。

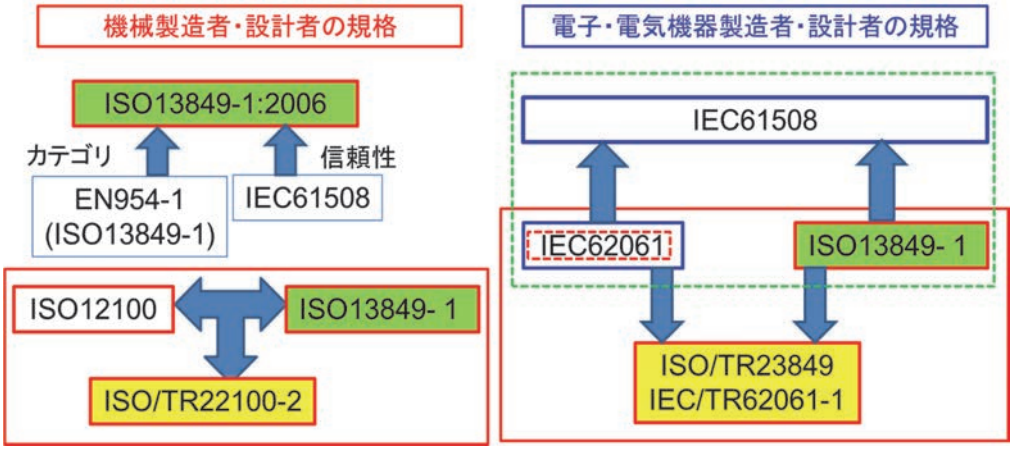


図 3　機能安全の主要な規格

事 例：産業用ロボットの機能安全 ～協働作業を中心にして～

産業用ロボットの安全に関する規格は ISO10218-1 (JISB8433-1) と ISO10218-2 (JISB 8433-2) があります。この規格のなかで、安全関連部に要求される性能レベルが示されています。

ロボットおよびロボットシステムの安全関連部の制御性能の要求レベル

制御システムの安全関連部は、以下のいずれかに適合する必要があります。

① カテゴリー 3 のアーキテクチャでのパフォーマンスレベル (PL) が d

② プルーフテスト間隔 20 年以上で、冗長性 (ハードウェア・フォールト・トレランス HFT) が 1 での安全度水準 (SIL) が 2

これに加え、最近話題になっている人とロボットで協力して作業を行う「協働」を可能にするには、さらに追加の要求事項があります。

協働運転要求事項

① 安全適合の監視停止

② ハンドガイド

③ 速度及び間隔の監視

④ 本質的設計又は制御による動力及び力の監視

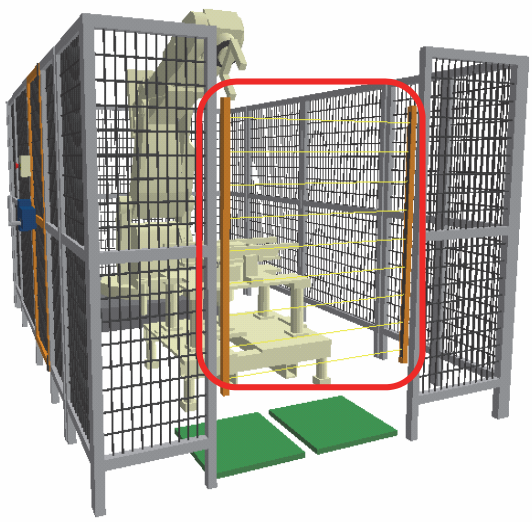
協働運転は人とロボットが共通の作業空間を共有する特別な運転

1 あらかじめ決めたタスクにだけ使うこと

2 全ての必要な保護法策が作動中のときだけ協働可能なこと

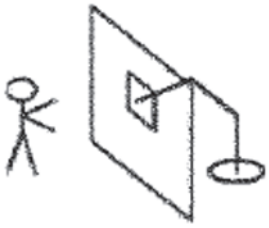
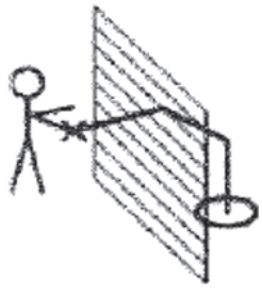
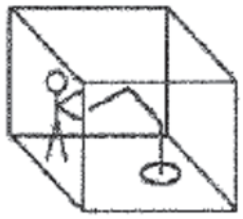
3 JISB8433-1 に適合する協働運転のために特別に設計された特性を持つロボットであること

を全て満足する場合だけ可能となる



ロボットとの協働のイメージは、ISO10128-2 付属書に次のように示されています。

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