平成30年８月２日
農業食料工学会
関東支部セミナー

機能安全による安全確保
～機能安全指針の概要と産業用ロボットへの適用～

厚生労働省安全衛生部安全課
安井省侍郎

本日の内容

１　はじめに

２　機能安全指針の概要

３　機能安全に関する主要な論点

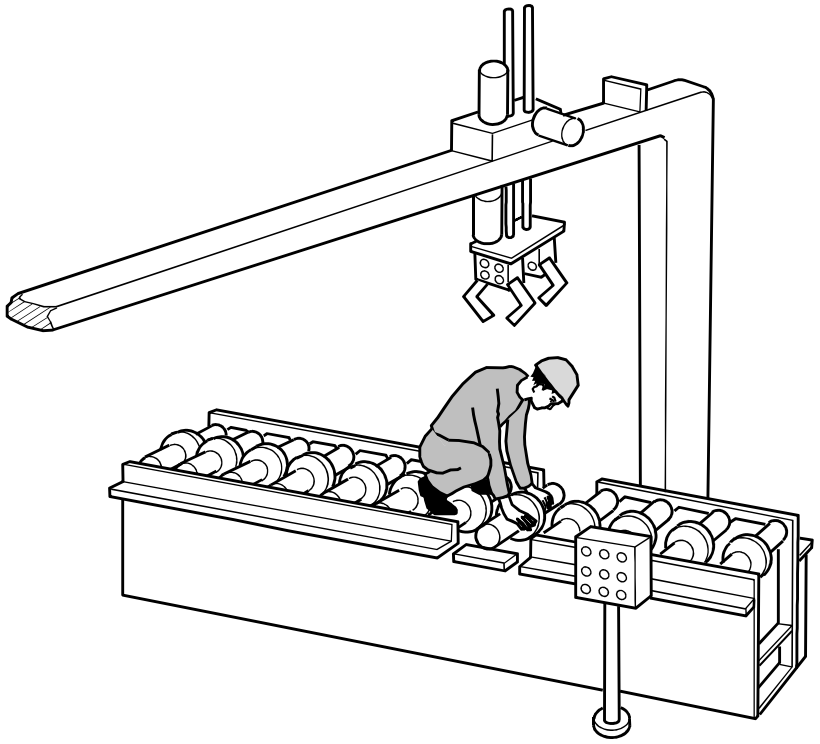
４　産業用ロボットへの機能安全の導入

５　考察及び結論

１　はじめに
(１)産業用ロボットに起因した死亡災害事例

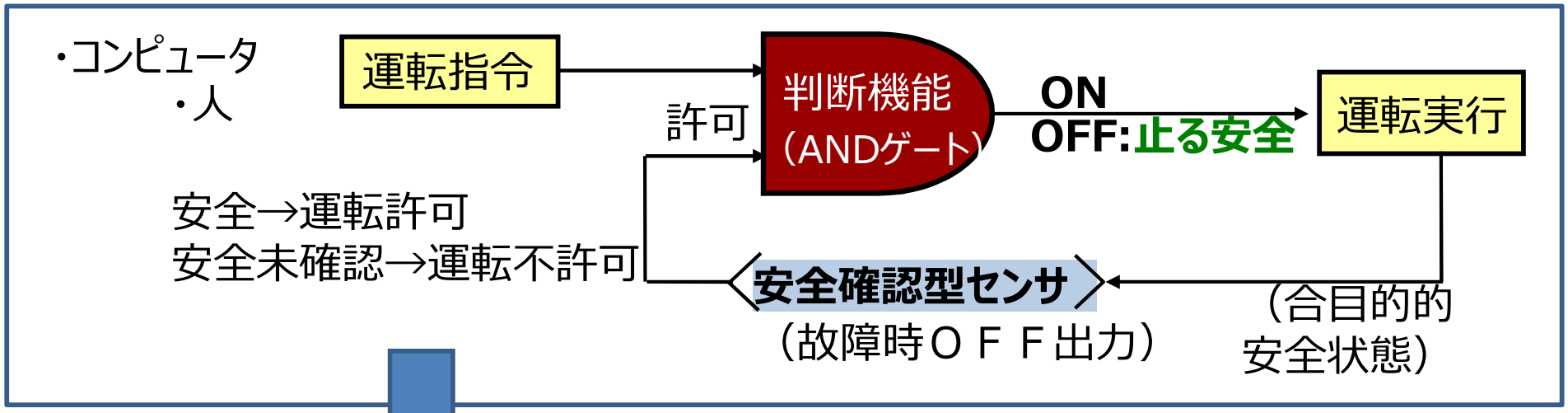
状況：車のシリンダーヘッド鋳造ラインの工程で、半製品を搬送する搬送用油圧ロボット(ローダー)の把持部に、被災者が挟まれて死亡した。

原因：ローダー異常時に、動力源を切らずに開口部のドアを開けて入った。ドアのインタロック機構が機能しなかった。

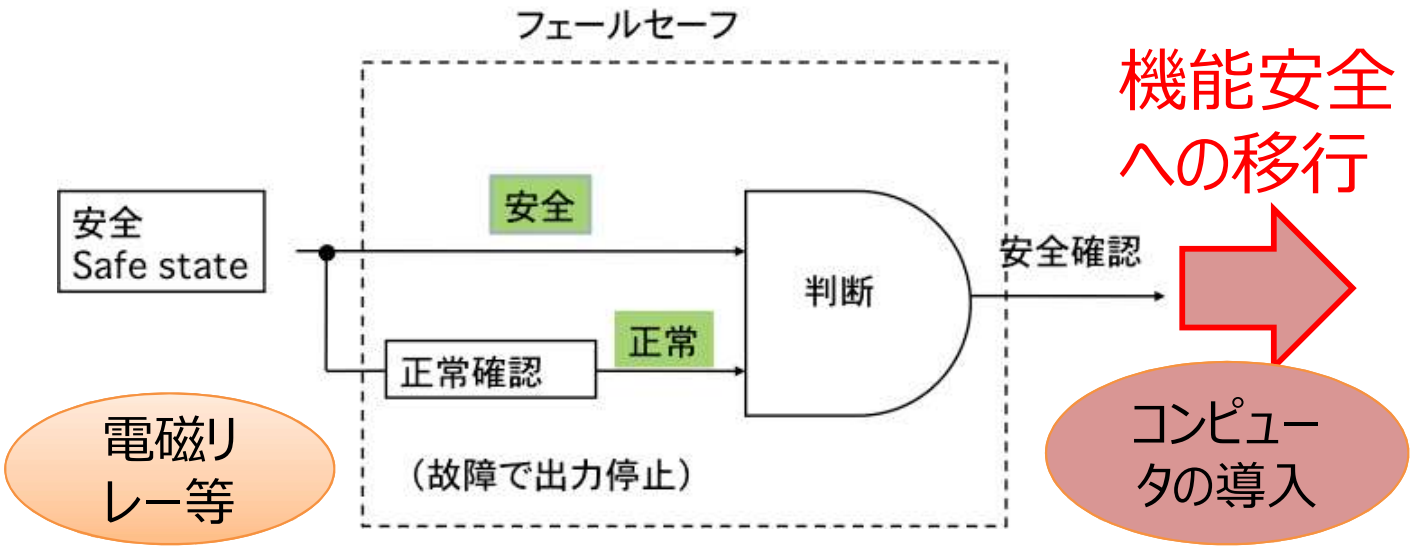


機械の異常等により人が近接したとき、機械が不意に起動して被災する

(２)安全関連システムの機能分離



安全確認センサに求められる特性（判断部も同様）



機能安全への移行

コンピュータの導入

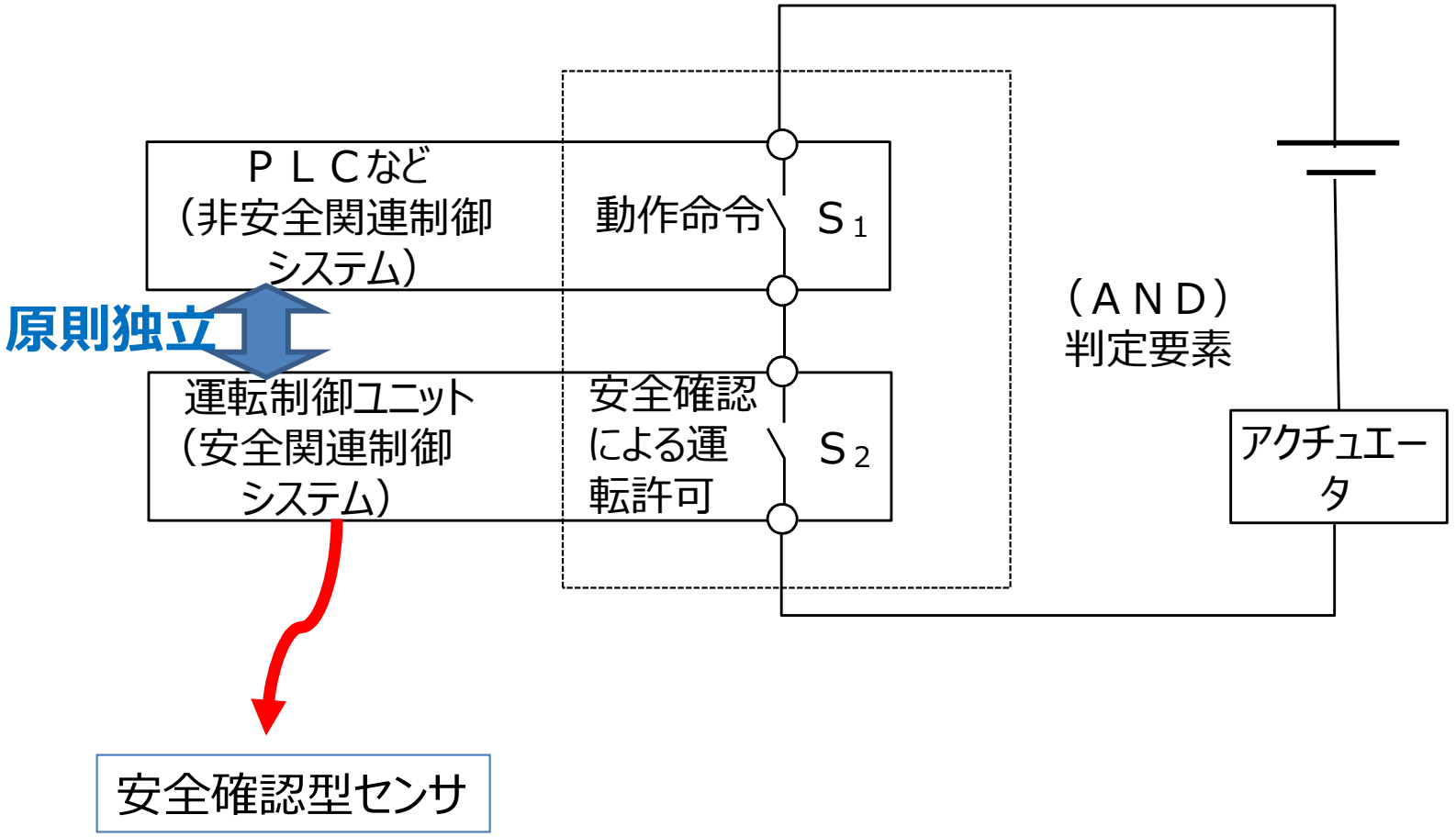
電気・電子・プログラマブル電子制御の付加により安全を確保する
→ 危険側の故障を診断、検出して、機械を安全状態へ遷移

(3)安全関連システムへの機能安全の導入

制御システム全体をフレキシブル化、高機能化

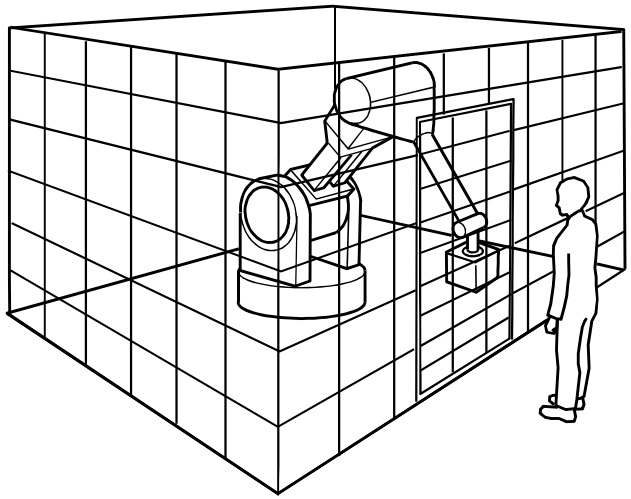
↓

混在する制御系であっても、非安全関連部の不具合等が安全関連部に影響を及ぼさない



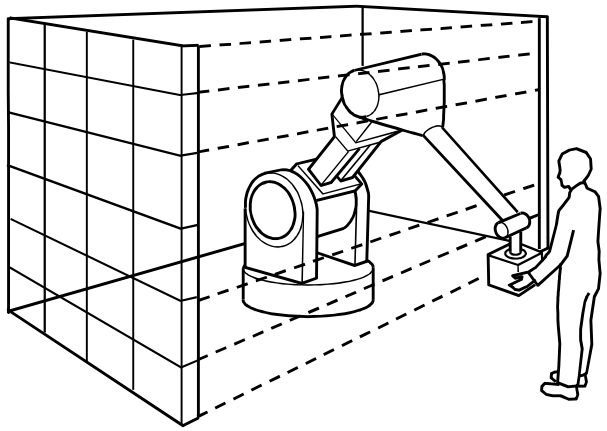
(4)産業用ロボットシステムへの機能安全の導入

ワーク授受の協働システムへの移行



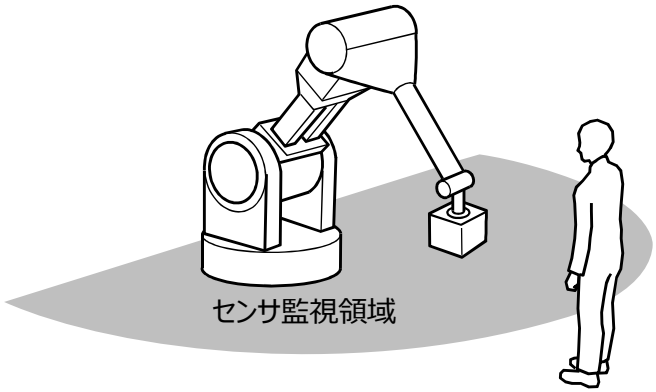
(a) 柵あり（可動ガード）

人とロボットとの「隔離」と接近時の「停止」の確保



(b) 開口部あり（光線センサ）

光線センサの一部を無効化
↓
ロボット動作に係わる制御(位置、速度、力等)が限定範囲で機能的な安全制御系



(c) 柵なし（センサ監視）

バーチャルフェンス機能
↓
ロボット可動部と人との距離（速度）を常時モニタ
↓
機能安全の導入

2　関係法令
(1)機能安全の法令への取り入れ

専門家検討会設置の目的

- 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) ロボットへの機能安全の適用

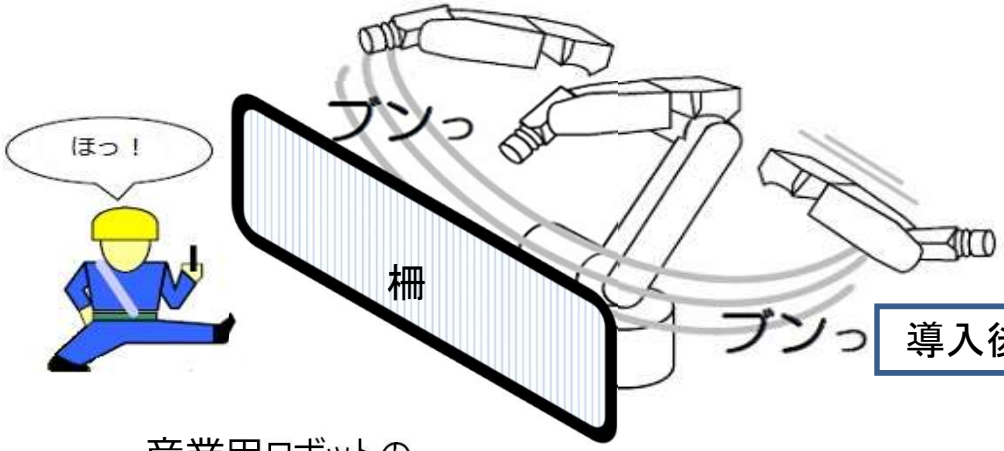
- 従来、安衛則第150条の４の規定により、さく又は囲いを設ける等、労働者の危険を防止するための措置が義務付け
- 通達（平成25年12月24日付け基発第1224第２号）
  - 「さく又は囲いを設ける等」の「等」には、ＩＳＯ10218シリーズにより設計、製造及び設置された産業用ロボット（技術ファイル及び適合宣言書を備えているもの）を、その使用条件に基づき使用することが含まれる
- 機能安全を含む適切な安全関連システムの適合宣言している産業用ロボットは、柵や囲いを設けることなく、労働者と協働作業が可能となった。

機能安全の導入による安全規制の高度化

従来の規制
（物理的防護・資格者による点検等）

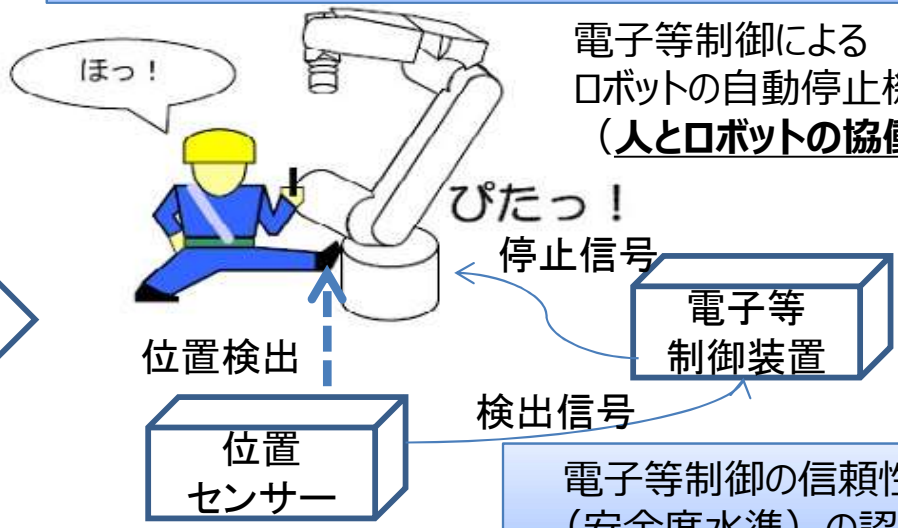
導入後

機能安全導入後の規制
（新たに制御の機能を付加することによる安全確保）
安全性を損なうことなく生産性の向上を実現



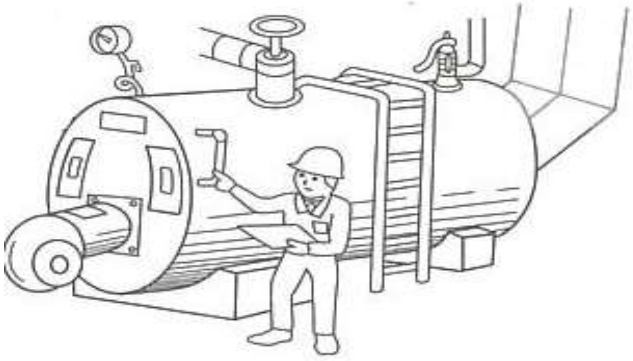
産業用ロボットの
周囲の柵等の設置
（**人とロボットは協働不可**）

導入後

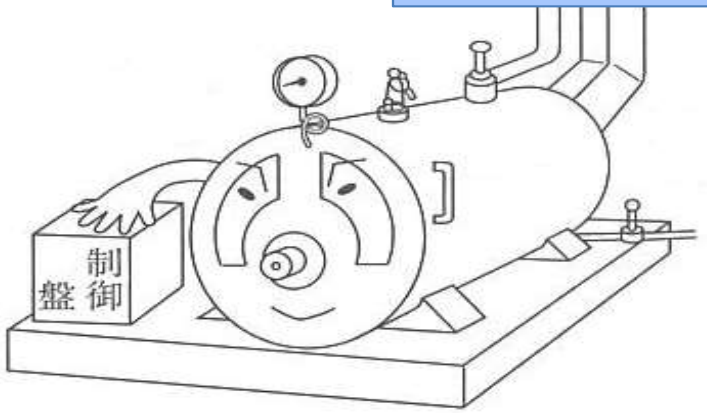


電子等制御による
ロボットの自動停止機能
（**人とロボットの協働可**）

電子等制御の信頼性の水準
（安全度水準）の認証が前提



導入後



信頼性の確認できない制御装置を装備したボイラーの資格者による点検（１日１回）

信頼性が認証された制御装置を装備したボイラーの点検頻度の延長（３日１回）による**自動運転期間の延長（３日間）**

２．機能安全指針の概要（１）

１　背景と基本的考え方

– 近年、**電気・電子技術やコンピュータ技術の進歩**に伴い、これら技術を活用することにより、機械等に対して**高度かつ信頼性の高い制御が可能**となってきている。

– 従来の機械式の安全装置等に加え、新たに**電子等制御の機能を付加**することにより、機械等による**リスクを低減するための措置及びその決定方法**（**機能安全**）のために必要な基準を示すことにより、**機械等の安全水準の向上**を図る。

2. 機能安全指針の概要（２）

２　機能安全に係る要求事項

①　要求安全機能の特定

- 製造者は、機械等による**危険性又は有害性（危険性等）を特定**した上で、**リスクを低減**するために要求される**電子等制御の機能（要求安全機能）**を特定する。

②　要求安全度水準の決定

- 製造者は、要求安全機能を実行する電子等制御のシステム（**安全関連システム**）に要求される**信頼性の水準（要求安全度水準）**※を決定する。

③　設計要求事項の決定とそれに基づく製造

- 製造者は、**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。

※要求安全度水準：危険事象を生ずる安全関連システムの故障の確率（**危険側故障確率**）で表される。

２．機能安全指針の概要（３）

３ 要求安全度水準の決定

① 製造者は、危険性等を特定し、その結果として**発生する事象（危険事象）**を特定。

② 危険事象毎に以下により、**要求安全度水準**を決定

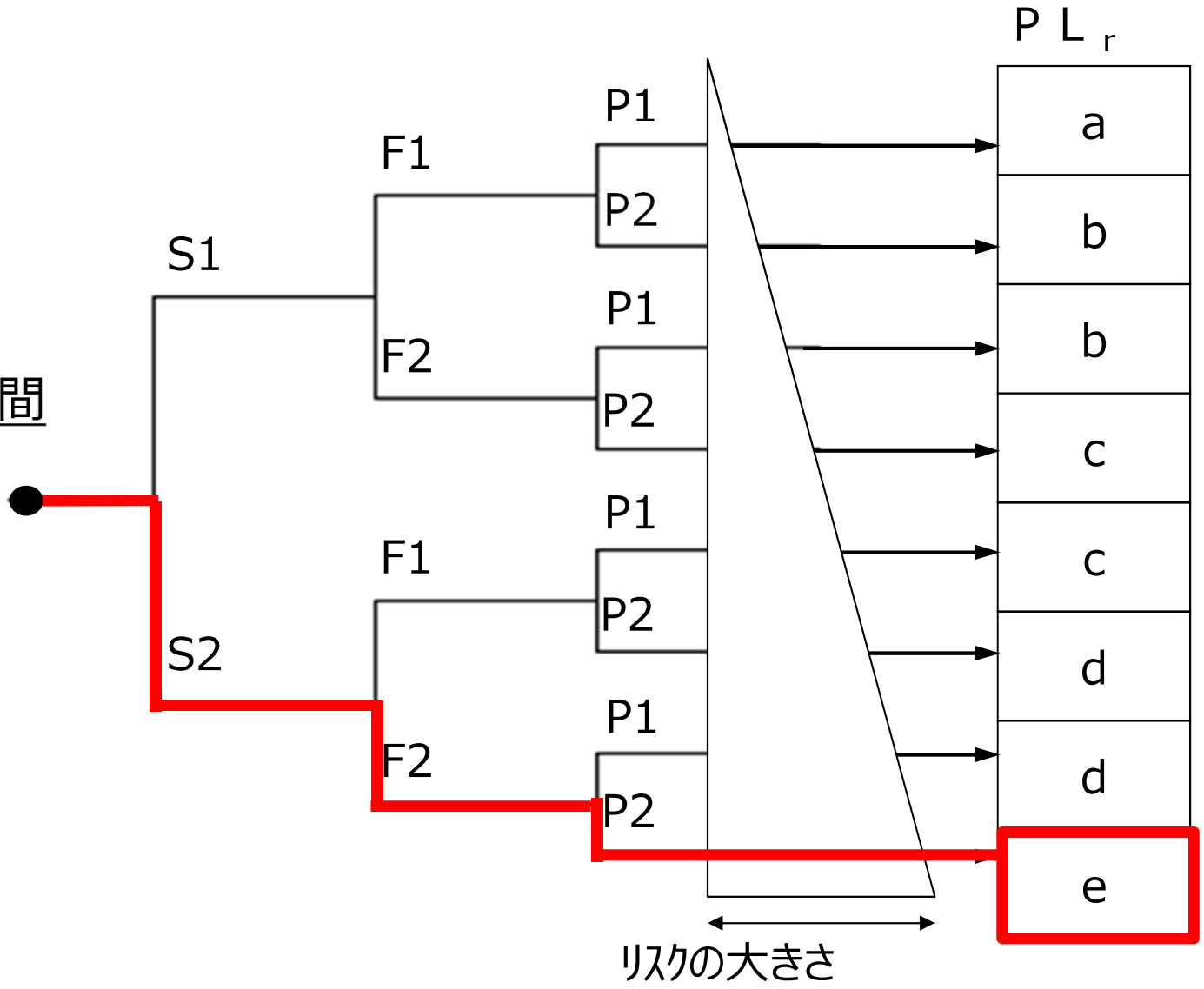
- 危険性等に**さらされる頻度**（時間）
- 生ずる負傷又は疾病の**重篤度**
- 危険事象からの**回避可能性**
- **危険事象の発生頻度**

要求パフォーマンスレベル（PLr）の決定例：ライトカーテン

S-傷害の大きさ
- S1：軽傷
- S2：死を含め重傷

F-危険源にさらされる頻度／時間
- F1：時間が短い
- F2：時間が長い

P-危険源回避の可能性
- P1：特定の状況下で可能
- P2：ほとんど不可能



PLとSILの関係

PLとSILの関係(表7-9)

SIL4に対応するPLは定義されていない。SIL4はガス爆発など多数が致命傷に至るリスクであるが、機械設備ではそのような事故はない。

PL	SIL 高／継続運転モード
a	-
b	1
c	1
d	2
e	3

要求安全度水準	高頻度の作業要求モード又は連続モードにおける基準値（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

２．機能安全指針の概要（４）

４　要求安全度水準を達成する方法

- **①　数値計算法（安全度水準（SIL））**
  - 平均**危険側故障確率**、**検査間隔**、平均**修理時間**、**共通原因故障**を計算式に代入し、数値的に計算する方法

- **②　要件の組合せ法（パフォーマンスレベル（PL））**
  - 構造要件（**カテゴリ**）、平均**危険側故障確率**、**診断範囲**、**共通原因故障**の組み合わせによって決定する方法。

要求パフォーマンスレベル（PL）を満たす設計方法

(1)カテゴリ

障害に対する抵抗性および障害発生後の安全関連システムの挙動に関する分類.
その構造的配置、障害検出および信頼性によって5段階（B、1～4）。
カテゴリの詳細は、「機能安全活用テキスト」を参照。

(2) MTTFd (Mean Time to Dangerous Failure)

安全関連システムが危険側故障を起こすまでの平均時間。

部品は、その使われ方によって故障率の考え方がふたつある。

・電気/電子部品のように連続的に使用することによる経年劣化による故障.
　連続稼働時間と各部品の危険側故障率からMTTFdが決まる。

・スイッチやリレー接点は、作動回数によって劣化。動作要求頻度によって
　MTTFdが決まる。

(3) 診断率（DC）

安全関連システムの危険側故障を回避

→構成部品の危険側故障を可能な限り診断する

DC：危険側故障率の診断率＝要素の全危険側故障率(分母)に対する診断可能な故障率(分子)

DCは要素に対して採用する診断手法に依存＝要素ごとにDCは異なる値となるため、安全関連システム全体を評価する場合は、平均値のDCavgを用いる。

DCavg＝Σ(DCi/MTTFdi)/Σ(1/MTTFdi)　　（式3）

DCは4つのレベルに分類される（表7-6）。

表7-6　DCavgの分類（JIS B 9705-1 表6）

DCavg	
None	DCavg<60%
Low	60%≦DCavg<90%
Medium	90%≦DCavg<99%
High	99%≦DCavg

(4) 共通原因故障（CCF）

共通原因故障(CCF):

安全関連システムの二重化チャンネルにおいて共通の原因となる危険側故障．例えば、温度や電気ノイズなどの環境条件、両チャンネルが同じソフトウェアを使っていた場合のバグなど。

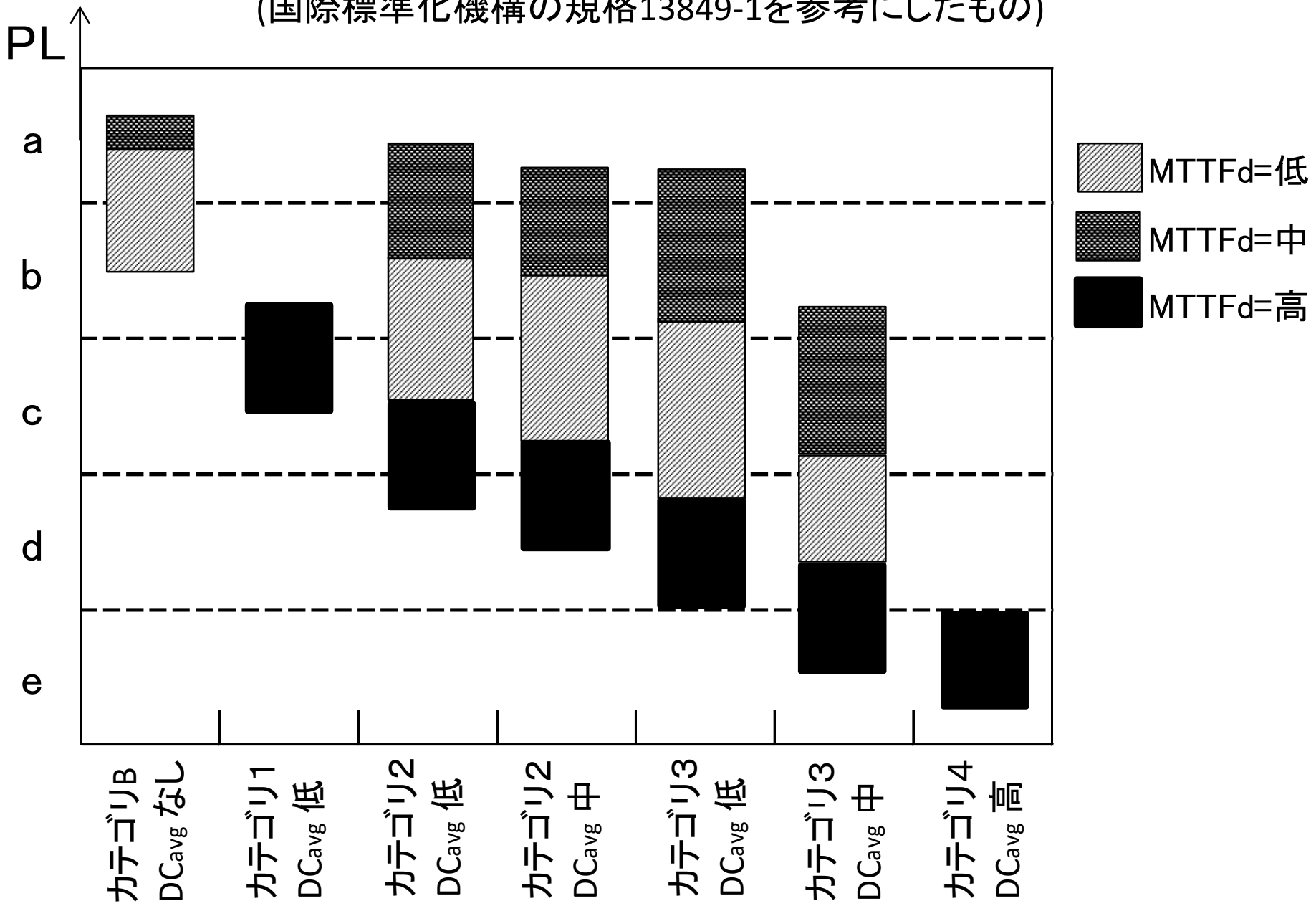
→二重化チャンネルが効果を発揮するためには、CCFをできる限り回避する。

JIS B 9705-1 (ISO 13849-1)は、CCFを回避するための手法を紹介。

各手法に点数(スコア)をつけ、採用した手法の合計スコアが65点以上になることを要求＝カテゴリ2以上の二重化チャンネルにおいて必須要求。

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)



3　機能安全に関する主要な論点
3.1.　機能安全の利点

1. 作業者と産業用ロボットが協働作業を行う場合や、介護作業用のロボットのように、**リスクに対する本質安全対策が困難な場合は**、電子等制御の機能によって安全を確保せざるを得ず、**機能安全が最後の手段**となる。
   - 複雑な電子制御システム（例：飛行機のように、**安全関連システムに故障があったときに機械等を単純に停止させるとかえって危険になるシステム**）においては、機能安全により、自動的に安全な順序で機械等を停止させることが特に必要となる。

2. 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、
   - 要求安全機能およ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。

3. 機能安全は、**通常の制御システムが故障**したときに、**独立した安全関連システムが介入して機械等を安全に停止**させるという考え方を取る。
   - このため、個別の規格により、**安全関連システムが制御システムから独立**していることを要求されることが通常である。
   - この考え方は、通常の制御の方法が、**プログラム制御、人間による操作、あるいは人工知能（AI）による制御のいずれであっても有効**である。

3.2. 機能安全の適用限界

1. 機能安全は、挟まれ・巻き込まれや爆発火災等の**機械等に起因する災害の防止**のための手法であることに留意する必要がある。
   - 不安全行動による災害など、**機械等の制御の機能によって防止できない危険事象には効果を期待できない**。
   - 機能安全は、**危険側故障確率を減少**させることで、危険事象の発生確率を下げることができるが、危険事象による**災害の重篤度を減少させることは困難**である。

2. 機能安全によるリスクの低減を図る場合、**本質安全対策など、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。
   - 例えば、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、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**
   - **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。

3. 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ることは認められない**。

3.3. 機能安全の認証と法令規制の関係

1. 機能安全の基準を満たす**適合性証明を受けた電子制御等によって制御される機械等**の取り扱いについては、特定の機械等ごとに検討の上、一定の**法令上の特例を規定**することになる。
   - ただし、国際規格においては、**危険事象により複数の死亡をもたらすおそれのある機械等（ボイラー、クレーン等）**については、電子等制御の安全機能に要求安全度水準を満たす場合であっても、**安全弁等の機械式の安全装置等を省略することは認められていない**。
   - その理由としては、**多重防護**の観点から、**異種の方式の安全装置**の設置が求められていること、**想定外の事象が発生した場合**には、**物理的な構造や機械式の安全装置で安全を担保**する必要があることがあげられる。

2. **事故の結果の重篤度が相対的に低い機械等（産業用ロボットなど）**については、**機械式の安全措置（ストッパー、柵等）を要求安全度水準の高い電子等制御の安全関連システム（監視・保護停止）により代替**することが国際規格で認められつつある。
   - 安衛法令においても、このような機械等について、一定の程度、**機械式の安全機能の代替を認める余地**がある。

3.4. 適合性証明の対象となる範囲と審査内容

1. 適合性証明は、**制御システム全体として、要求安全度水準の適合性を証明**する必要がある。
   - コントローラ等の機器（デバイス）単位で要求安全水準の適合証明を受けている場合であっても、**システムとして組み込んだ機械等の制限によってその安全度水準が達成できない場合がある**ため。
   - 認定の対象となる適合自動制御装置には、新たに設置される機械等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機械等を改修して新たに備え付けられるものも含まれる**。

2. 法令上の特例措置を受ける必要がない機械等については、**製造者自らが機能安全指針に適合することを宣言**することも認められる。

3. 適合性証明にあたっては、**ＲＡにより、要求安全機能が適切に特定**され、**要求安全度水準が適切に設定**されているかどうかが審査対象。
   - 同一型式による量産品に適合証明を行う場合、定期的に製造者に対するマネジメント監査も含まれる。

4. 登録適合性証明機関は、**ボイラー以外の電子等制御の機能安全の適合証明を行うことも可能**。

3.5. 要求安全度水準の決定のための使用条件の把握

1. **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、機械等の**使用者と製造者が連携**し、使用条件を決定する必要がある。

2. 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を決定することは困難**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**等を行う必要がある。

4　導入事例：ロボットの安全速度制限(SLS)

リスクアセスメントにより適切な安全対策が実施された場合、ロボットを囲む柵のない機械設備の運用が可能。

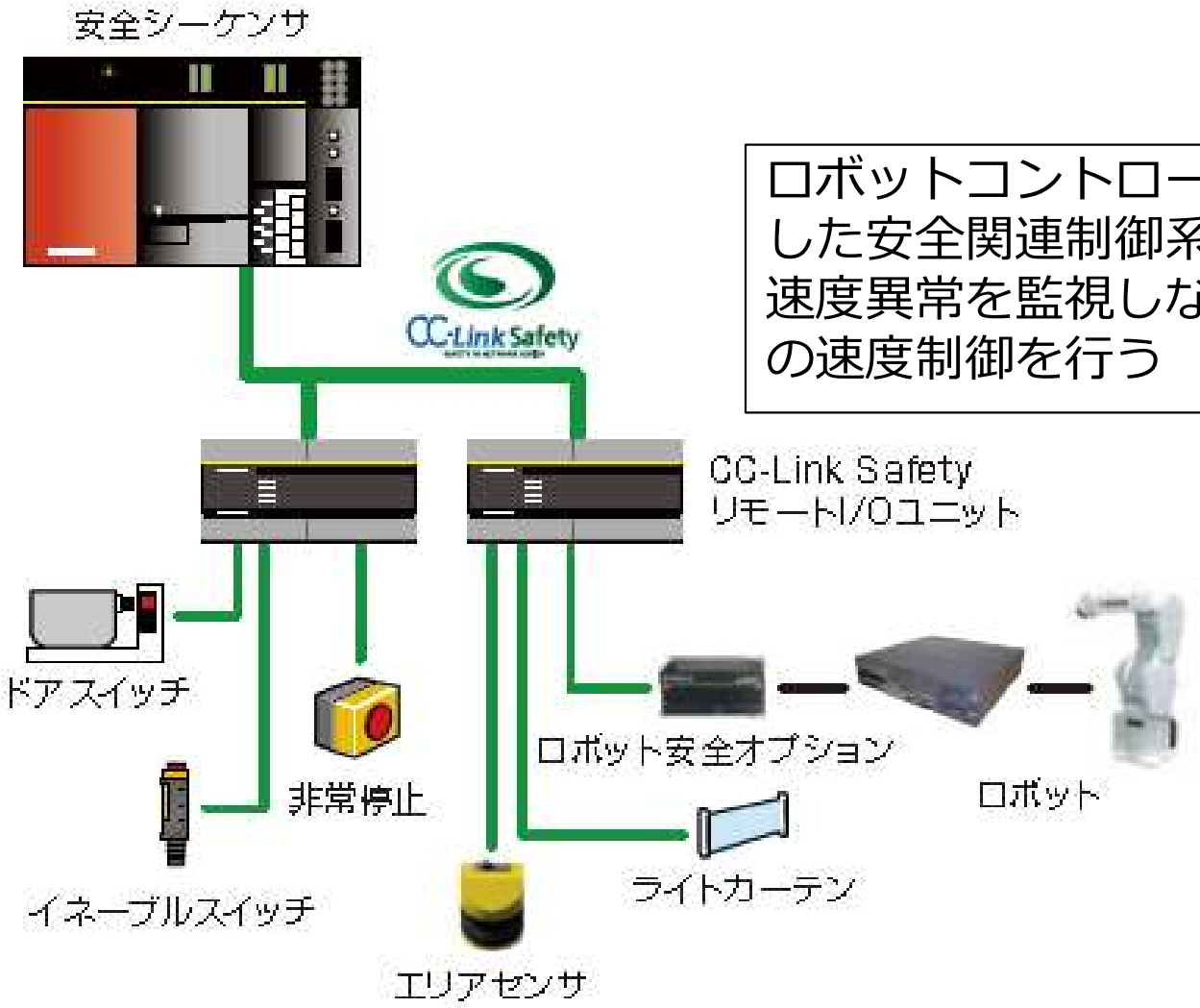
ここでは、安全適合監視速度機能の具体的事例として、ロボットの安全速度制限(SLS: Safety Limited Speed)を紹介。

SLSは、IEC 61800-5-2可変速ドライブの機能安全規格に定義された安全機能の一つである。

4.1. 機械・設備イメージ

制限エリアへの進入：ロボットを指定の安全速度以下で運転
停止エリアへの進入：ロボットを即時停止する。

4.1. システム構成

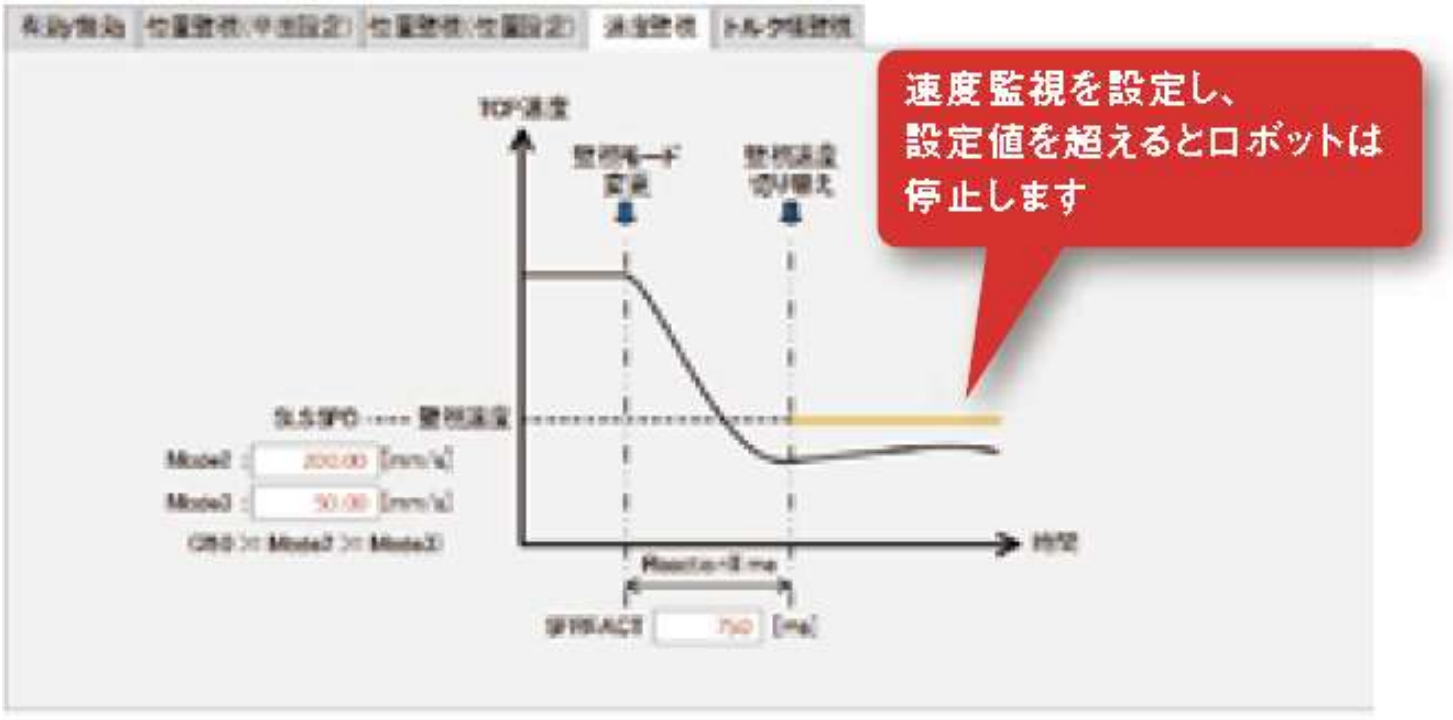


ロボットコントローラは規格適合した安全関連制御系を内蔵し，n速度異常を監視しながらロボットの速度制御を行う

4.2. 機能の設定（1）

SLSの設定＝ロボットコントローラの安全監視機能の設定

…ロボットコントローラの専用ツールを用いて行う

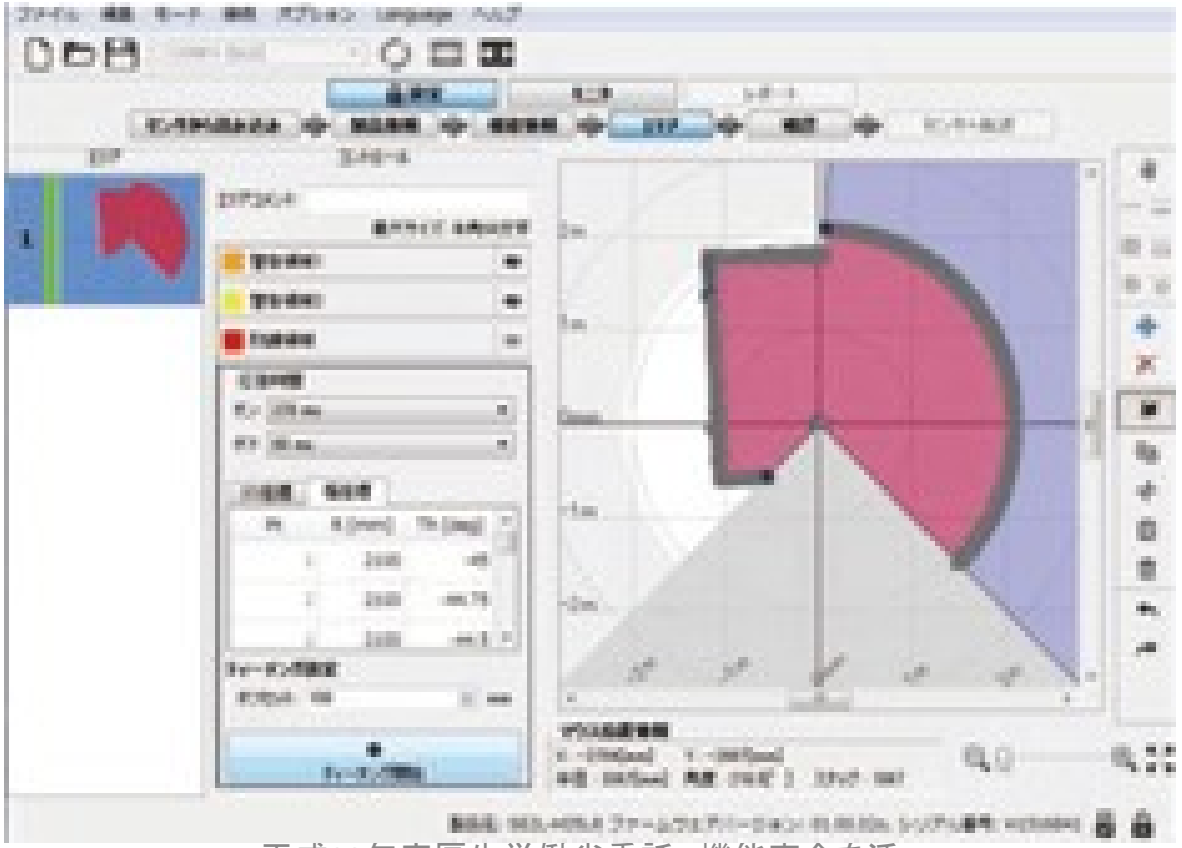


速度監視設定

4.2. 機能の設定（2）

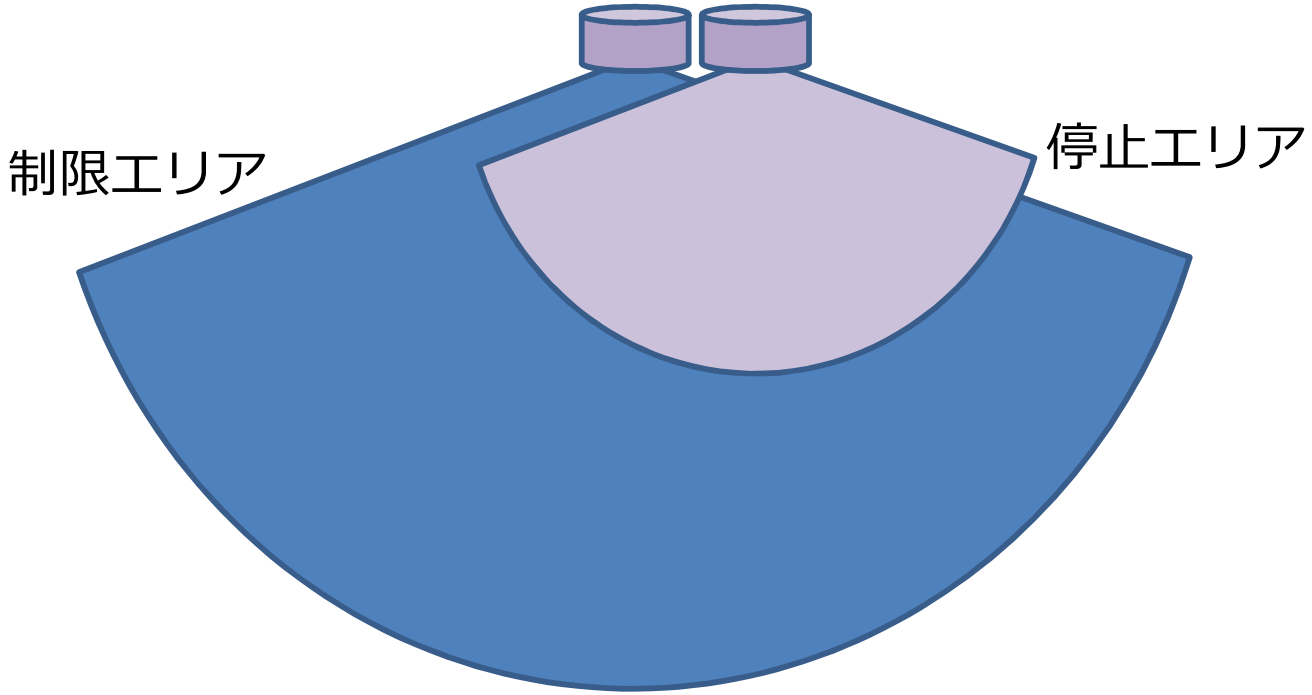
エリアセンサ：警告エリアと非常停止エリアを角度と距離で設定

…一般的に、専用ツールで扇形を描くようにして設定する



4.2. 機能の設定(3)

レーザースキャナ1:制限エリアの検出用
レーザースキャナ2:停止エリアの検出用
　いずれも安全関連機能なので，OSSD信号を信号入力として用いる.



4.3. 妥当性確認

協働作業ロボットはJIS B 8433-1 (ISO 10218-1)に適合し、かつSIL2/PLdの安全性能を達成すること。

- 安全センサや安全PLCなどもそれぞれの安全規格に適合し、MTTFdやDCavgなどの安全パラメータが製造業者から入手可能

SLSの速度やエリアセンサの設定などの妥当性確認

- 例えば、ロボットの通常速度と制限区域、停止区域の範囲、人体の接近速度など当初の安全要求を満足したかどうか妥当性を確認する。
- 据え付け状態でのリスクアセスメントも必要である。

５．考察及び結論（１）

- 産業用ロボットについては、安衛則150条の４の解釈の変更により、ISO10218への自己適合宣言ロボットを技術ファイルどおりに使用すれば、柵等の設置が免除される。
- しかし、具体的な作業内容を特定した上でリスクアセスメントを実施する必要があるため、システムインテグレータが機能安全指針への適合の妥当性を評価できる必要。
- 厚労省では、システムインテグレータ向けの機能安全活用テキストとマニュアルを作成し、普及を図っている。

5. 考察及び結論（2）

- 自動走行ロボットについては、現時点で明確な国際規格はない。
- 無人搬送車（AGV）については、ISO規格が改定作業中であり、機能安全の考え方が取り入れられる予定。
- 厚労省としては、ISO規格の動向を踏まえ、AGVへの機能安全の適用に取り組んで行く。

参考文献

機能安全による機械等の安全確保について

- 厚労省ＨＰ内の機能安全ポータルサイト（以下の文献は全て掲載）
- http://www.mhlw.go.jp/stf/seisakunitsuite/bunya/0000140176.html

機能安全指針

- 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）

関係法令

- 機能安全に係るボイラー則及び登録省令の改正の概要
- ボイラー及び圧力容器安全規則等の一部を改正する省令（新旧対照表）抜粋（平成28年厚生労働省令第149号）

関係通達

- ボイラーの遠隔制御基準等について（平成15年３月31日付け基発0331001号。平成28年９月30日付け基発0930第35号により一部改正。）

テキスト･マニュアル等

- 機能安全活用テキスト（講義用スライドあり）
- 機能安全活用実践マニュアル　ボイラー編（講義用スライドあり）
- 機能安全活用実践マニュアル　ロボットシステム編（講義用スライドあり）
- 機能安全実践マニュアル　演習用教材
- ボイラー自動制御装置の機能安全指針への適合証明申請の手引き

本日の内容

１　はじめに

２　機能安全指針の概要

３　機能安全に関する主要な論点

４　産業用ロボットへの機能安全の導入

５　考察及び結論