2013-7-29 SA協議会、名古屋にて

連続する機械・設備の安全について

向殿政男

（明治大学　名誉教授）

連続する機械・設備とは？

～統合生産システム（IMS)～

連続する機械類とは？

- 単体機械から連続する(連携する、協調する)機械・設備へ（統合生産システムへ）

- 部品の構成から単体機械へ
- 単体機械の連結から総合生産システムへ
- 単純な部品の組み合わせというよりも、むしろ全体で新規でかつ異なる機械であると考えるべきである

連続する機械の安全設計とは

- 単体でも連続でも、共通部分がある
- 連続することにより、新しいリスクが生じる
- 単体の結合ではない、総体的に見よ：単純な機械の組み合わせというよりも、むしろ全体で新規でかつ異なる機械システムであると考えるべきである
- 一部への頻繁な手動介入、例えば検査、保守、設定の要求事項が存在する場合、全体を停止させることは実用的でない

連続する機械の安全設計とは

- 各機械は、既に、安全設計されているとする
- 安全設計の考え方は、同じである
- 機械類の基本設計ISO12100＋（IMS：ISO11161, 2007年）

- 安全設計思想の基本から考えよ

連続するとどんな問題が発生するのか？

～現実的課題～

誰がインテグレートするのか？

- 設計者？
- インテグレーター？
- ユーザー？
- 設計者は、ユーザの使い方が分かっているのか？
- インテグレータは、実力と経験があるのか？
- ユーザは、要望を正しく伝えているのか？
- 安全確保の責任分担は？

連続する(複合)機械設備システムでの困りごと1(機械ユーザより)

「インテグレーターが組織の中に仕組みとして確立していない企業が多い」

- 結果として、製造者側やユーザー側とのリスクコミュニケーションがうまく機能しない場面が多く見られ、例えば機械システムのインターフェース不備による許容できない残留リスクを見逃して設備を使用しているケース。
- この場合重大災害が発生して、初めて前述の問題が気付くケースとなる。
- 背景として企業TOPも(インテグレーターの)重要性を充分理解(認知)していないことが、企業内の仕組みの中に取り入れらない要因のひとつと考えられる。

連続する(複合)機械設備システムでの困りごと2(機械ユーザより)

「単体の設備として、個々の製造者(A社、B社、C社･･･)で製造された設備が、連続する生産システムとして構築された時、全体システムとしての安全評価に漏れが生じる」

- (トータル的にシステムを安全評価できるインテグレーターの不在)
- 要因として、特に製造者側が国際規格を導入(理解)している企業と導入(理解)していない企業の落差が大きく、全体システムとしてのリスク評価を実施する責任も不明確になるケースがみられる。
- 機械設備システムが自動化、複合化されている日本の現状を考慮すると、既に体系化されている企業も一部あるが、日本としても早く連続する機械設備に対するリスクアセスメント等を含め、早期にIS011161の体系化が必要と思われる。

連続する(複合)機械設備システムでの困りごと3(機械ユーザより)

「国際規格に適合していない(以下旧規格と称す)設備と国際を適合した(以下新規格と称す)設備が混在する連続する生産システムでは、リスクの低減が予想以上に困難になっている」

- 特に制御システムについては、リスク低減するために改造等が必要になってくるが、例えば10年前の旧規格ロボットは「安全カテゴリ2」がほとんどで、製造者側でも技術的に新規格対応の改造は困難になっている。 ‥‥でも現状は、まだ旧規格ロボットを活用している企業は多く存在する。

連続する(複合)機械設備システムでの困りごと4(機械ユーザより)

「連続する生産設備システムでの制御(インタフェース)での困りごと」

- 複雑化した生産設備システムは、自動、手動以外にもメンテナンスモードなど各種モードも存在していて、いくつかの条件が重なる複雑なインタロックにより、逆に重大なリスクが顕在化できず、重大事故を引き起こす可能性のある許容できない残留リスクが潜在化しているケースがある。
- これは1項と同じで、製造者側が、ユーザー側の使用条件を充分にトスされなかったため(リスクコミュニケーション不足)危険源の同定に漏れが生じ、重大な災害を起こす要因にもなっている。

実際に発生した災害事例１(機械ユーザより)

・メンテナンスで面取工程で作業中に切削工程での搬送装置で詰まりが発生した為、開口部からつまりを取り除こうとした。

・手を伸ばしたところにロボットのアームが移動してきて、ハンドで挟まれてしまった。

➡ 開口部はライトカーテンで侵入を検出しておりますので、これは起こらないと思いますが、ライトカーテン、制御装置が故障していた場合。

実際に発生した災害事例2 (機械ユーザより)

- メンテナンスの為、切削工程で作業中に扉を閉めて作業しており、作業者に気が付かずに再起動をかけてしまい。作業者が怪我をする。

➡ モード変更後、鍵を持って、柵内にはプラグを持ち込む形としているので、実際は起動することはないのですが・・・

実際に発生した災害事例3 (機械ユーザより)

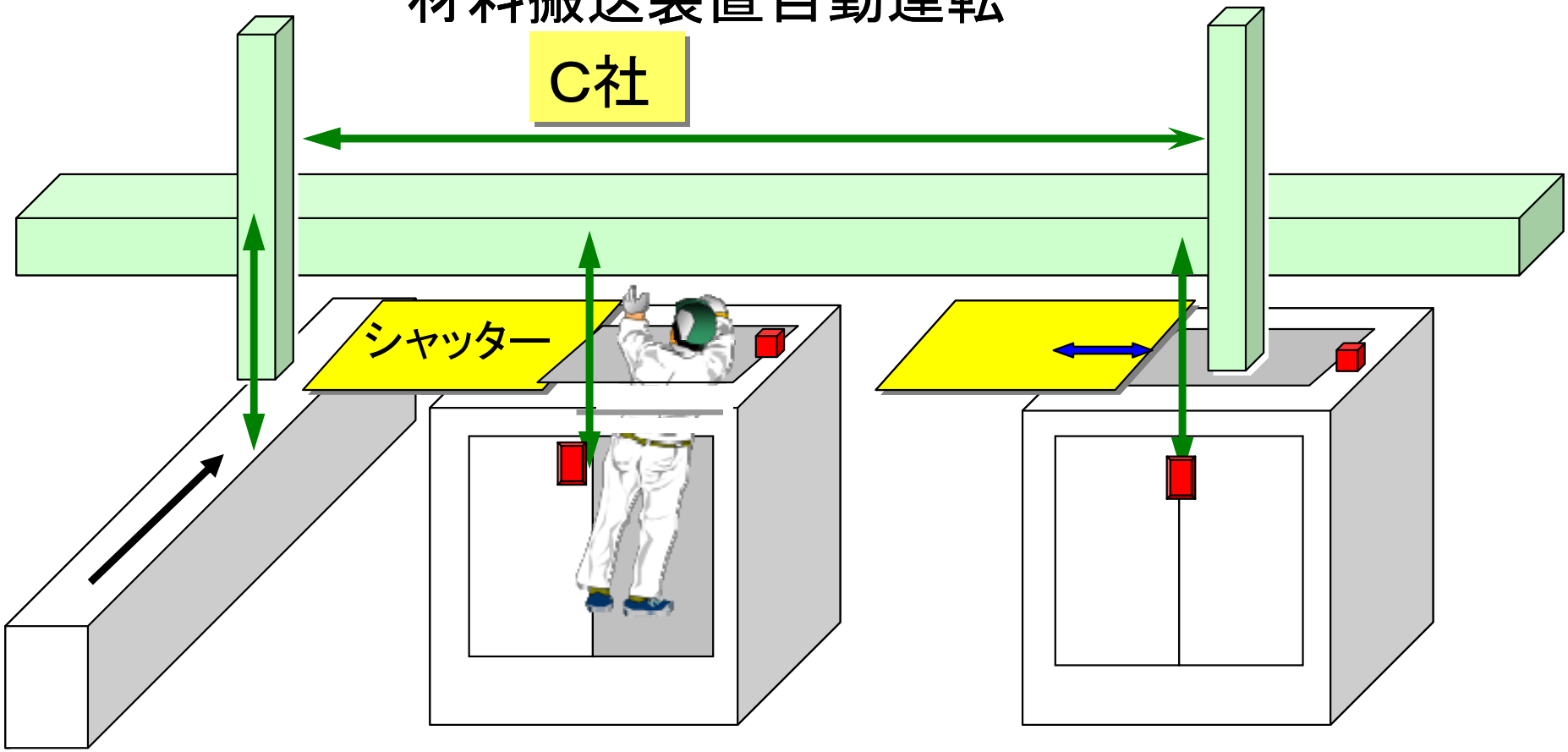
- メンテナンス作業中にコンベアの確認を行っている時、背後のロボットが急に動作を開始し、受傷。

→ メンテナンス中は動力供給を限定しているので、起こらないと思いますが。

実際に発生した災害事例4(機械ユーザより)

- 連続する機械設備で、1台の設備（A設備）が故障してバイパスモードにして、保全マンが修理作業を実施。
- A設備の上部シャッターの開いた状態であったため、保全マンが設備内で立ち上がった時に走行してきたローダーに頭部をぶつけた。
- この時、バイパスモードにしていたため、A設備関連のインタロックが無効になっていた。
- A設備と搬送設備は、別々の製造メーカーであった。
- リスクアセスメントは、個々の設備のリスク評価は実施されていたが、この状況でのリスクは洗い出しできていなかった。

材料搬送装置自動運転



世界の流れは
どうなっているのか？
～ ISO11161統合生産システム～

統合生産システム(IMS)の定義

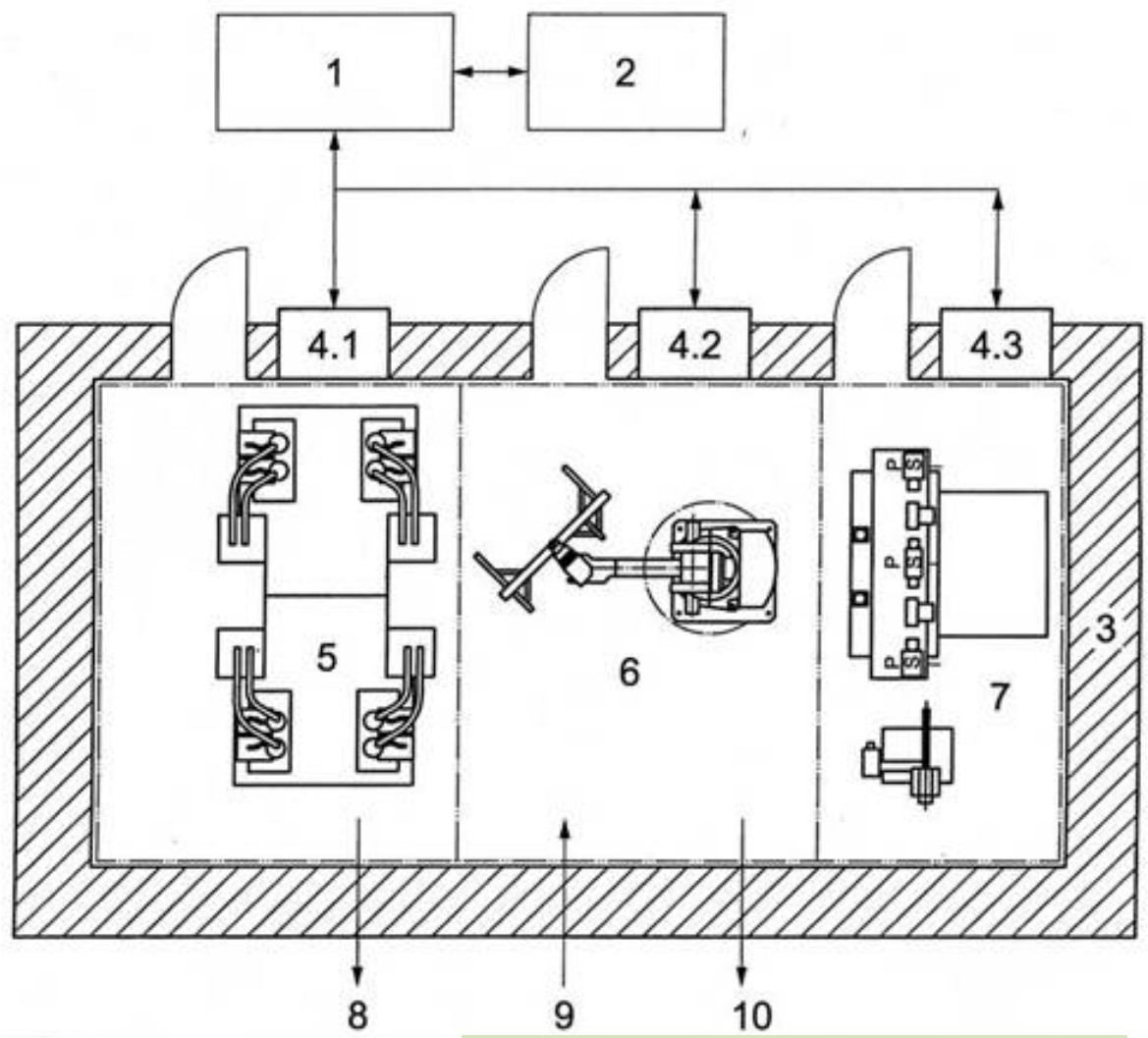
- 個別部品又は組立品を製造、処理、移動、包装する目的で、制御によって連結され、材料ハンドリングシステムにより結合して、協働作業を行う機械グループ。

インテグレータの定義

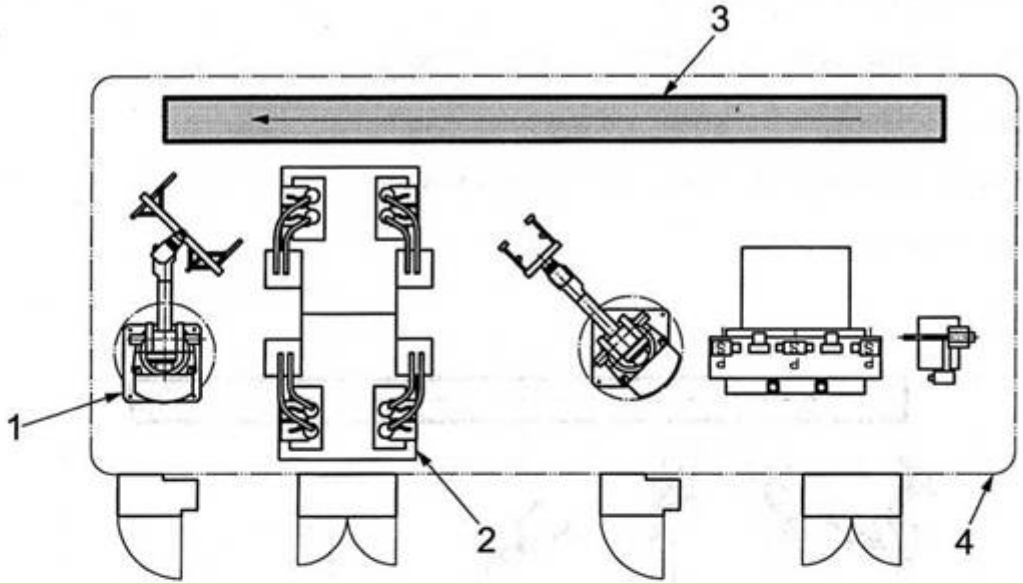
- 統合生産システムを設計、供給、製造又は組み立て、かつ、防護（保護）方策、制御インターフェース、及び制御システムの内部接続を含めて、安全戦略を監督するもの。
- 注記：インテグレータは、製造業者、組み立てる人、技術系業者又は使用者となる場合がある。

統合生産システムの一般的構成例

1 制御
2 オペレータペンダント
3 安全防護空間
4 局部制御装置
5 危険区域A
6 危険区域B
7 危険区域C
8 スクラップ及び
消耗品の流れ
9 原材料の流れ
10 最終品

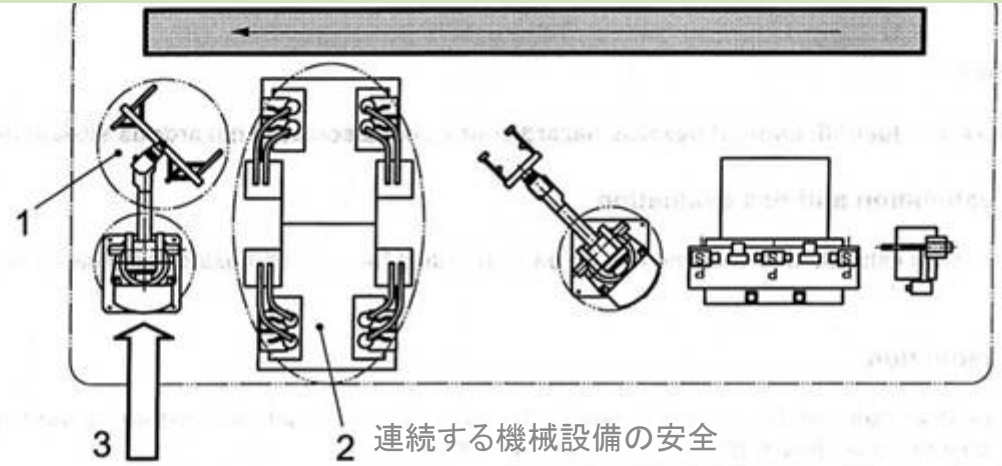


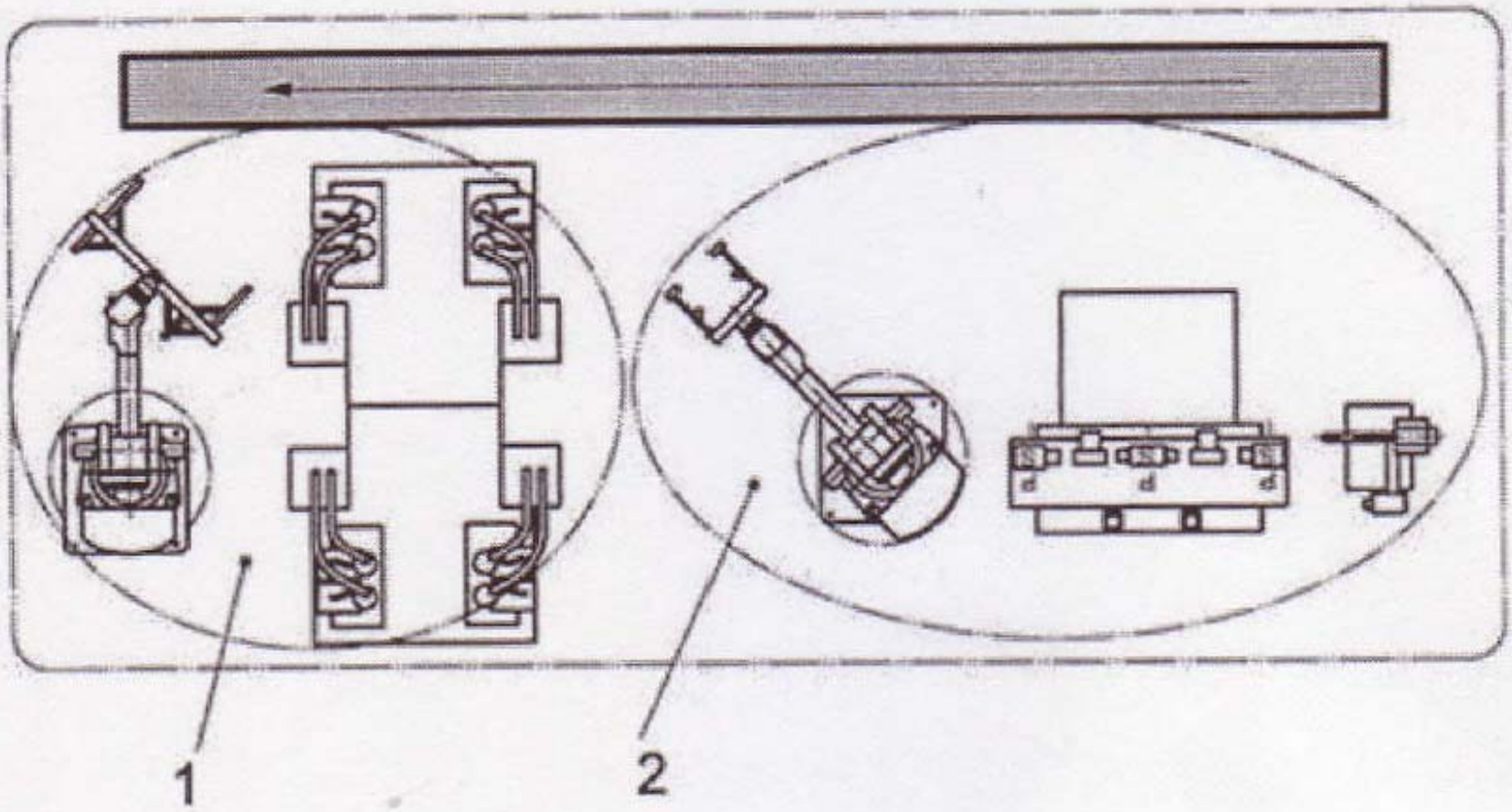
ISO11161統合生産システムより



IMSの制限(上図）
1 機械A-ロボット
2 機械B-工作機械
3 機械C-コンベア
4 IMS

任務の決定(下図)
1 任務1-工具交換
2 任務2-清掃
3 任務への接近



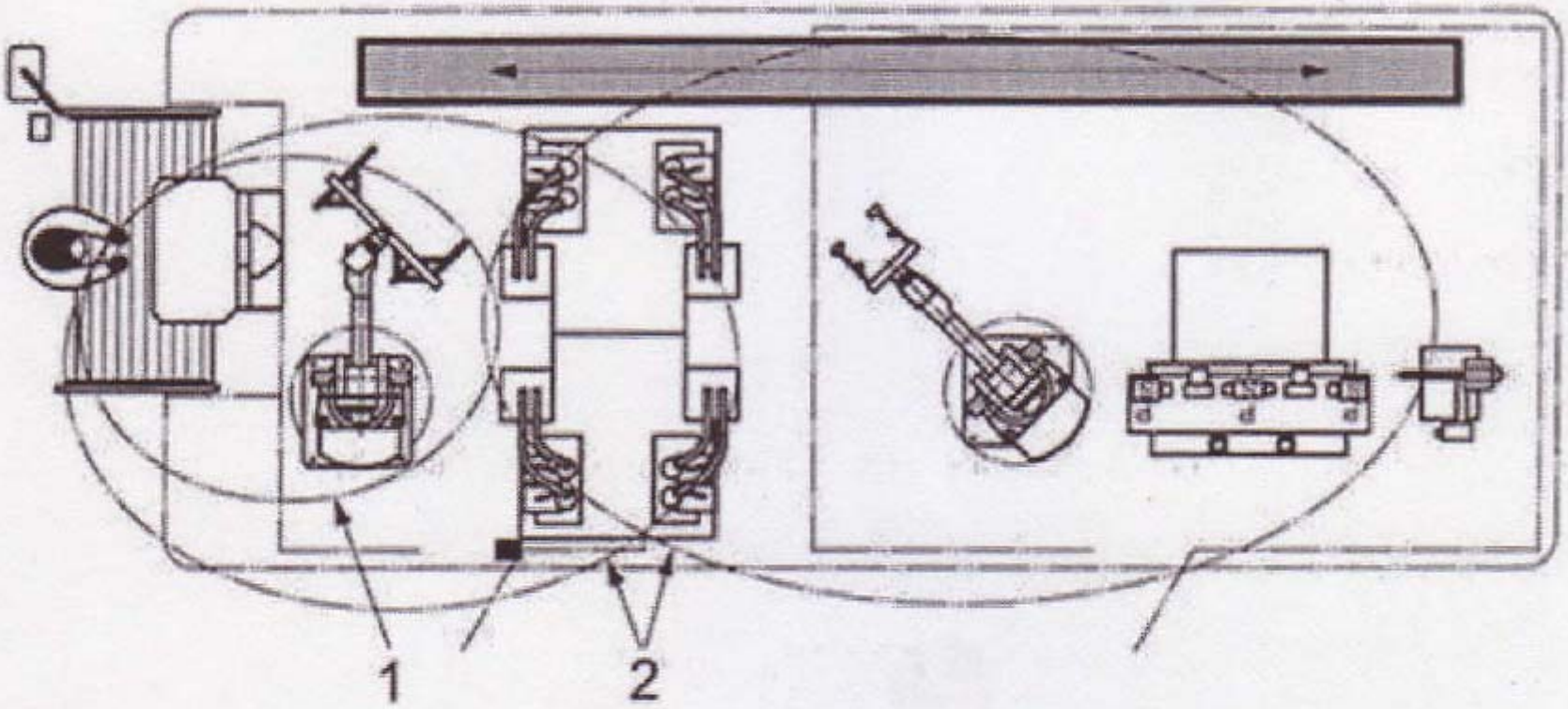


（キーワード）

1　タスクゾーンA

2　タスクゾーンB

図5　タスクゾーンの決定



（キーワード）

1　光線式制御による制御区間

2　インターロック装置による制御区間

図 6　制御区間を含む安全防護の決定

タスクゾーンのインターフェース

- 危険源がタスクゾーン間で生じる場合、適切な安全防護が用意されなければならない。タスクゾーン間のインターフェースは、以下に関連する。
- （a） ータスクゾーンから近接するタスクゾーンまでの材料の流れ、及び
- （b） ータスクゾーンから近接するタスクゾーンまでの接近の経路

制御区分

- タスクゾーンに関連する種々の制御及び保護装置の制御区分は、リスクアセスメント及び関連するタイプC規格により、以下を考慮して決定しなければならない。
- （a） 統合生産システムの物理的レイアウト
- （b） 生産プロセス自体
- （c） 任務の達成で要請される接近性

タスクゾーンと局部制御の定義

タスクゾーン

- オペレータが作業を遂行するIMS内及び／又は周辺の予め決定された空間

局部制御

- タスクゾーンの制御がそのタスクゾーンでのみ実施可能な状態

どうあるべきなのか？
～解決策の模索～

インテグレータの役割の明確化

- システムインテグレータの仕事と役割を分離し、その内容と責任を明確にせよ。
- インテグレータのコンピテンシー(基本的能力)を明らかにして、人材の養成を行え
- ・・・・・
- ・・・・・

階層的構造化

- すべての組合せのインターフェースで安全を考えるのは不可能
- サブシステムの分離、階層化
- 各サブシステムで安全の確保を行い、異常状態に関しては統一的出力を決める
- 連携するサブシステムの異常出力に対しては、分離する、フェールソフト、フェールセーフ等の概念の適用：ユネート性の重要性

残留リスク情報の流れ

- 残留リスクの情報を上から下へ（メーカ→インテグレータ→ユーザ）、かつ、下から上へ（ユーザ→インテグレータ→メーカ）流して還流させよ
- PDCAを回して常に改善の努力を
- 安全は全員で作って行く時代
- 基本は一般安全原則（安全設計思想）にあり、共通である（ISO12100はA規格、ISO1161は、12100の下のB規格）

安全設計思想

～すべてに共通する～

安全の常識

- 機械設備は劣化等でいつかは壊れるものである
- 人間はいつかは間違えるものである（時には、認知症の人、意識を失う人、悪意の人もいる）
- 組織やルールに完全なものはあり得ない
- 絶対安全は存在しない（リスクゼロはあり得ない）

安全確保のステージ

- **未然防止**方策
  ↓(予防安全：設計安全、寿命予測)
- 事故を起こさない
  ↓(運用安全：保守・点検・修理)
- 危害のひどさを下げる
  ↓（衝突安全：拡大防止、再稼働）
- **再発防止**対策（事後安全）

(事故調査：原因究明)

→正常な終焉（死に方設計）**廃棄**

・過去の歴史に学べ

・事故データを収集せよ

・緊急時を考えておけ

・全ステージを総合的に考えておけ

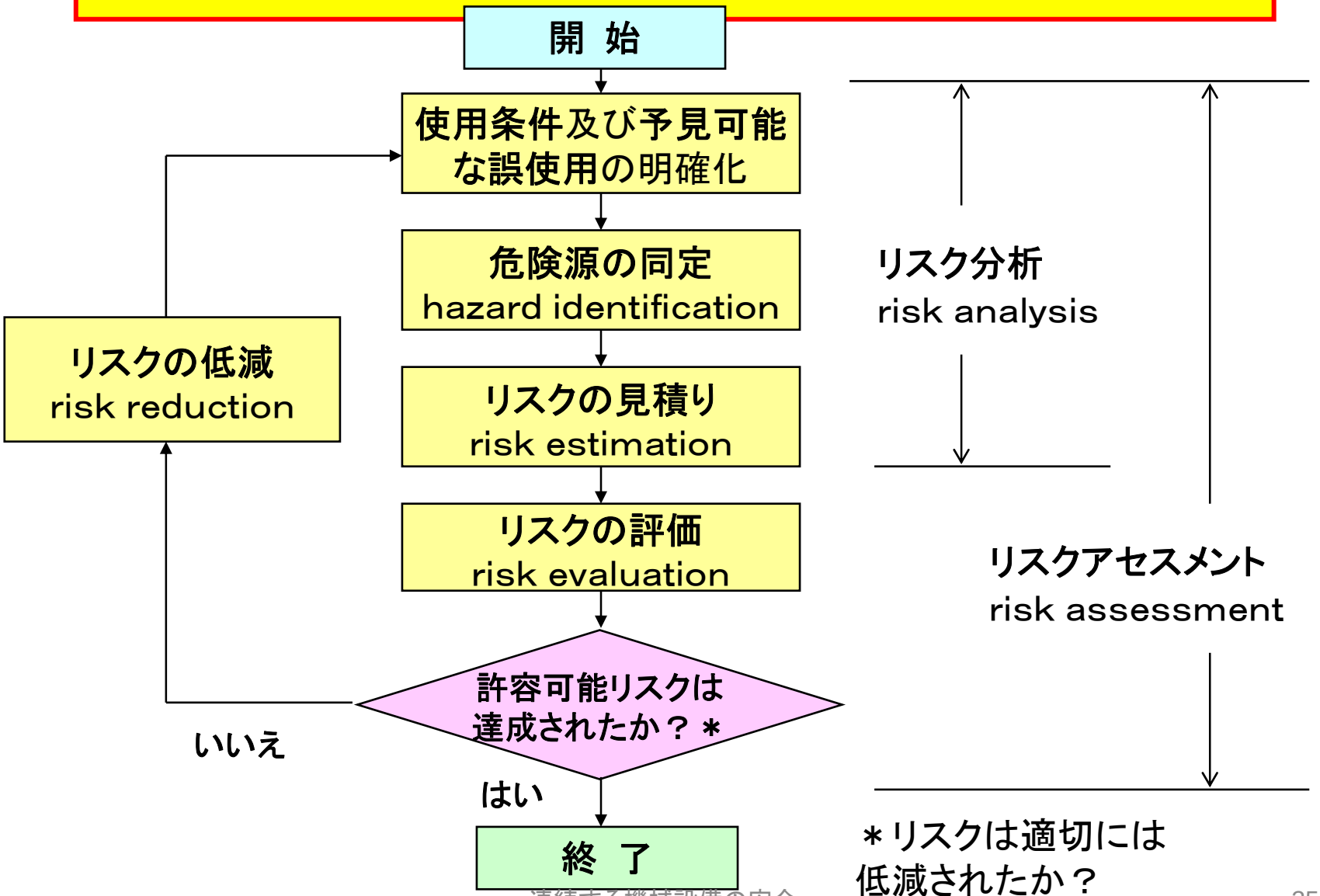
安全設計おける常識
～安全設計思想～

- **事後より事前に**（再発防止より未然防止）
- **下流より上流で**（安全装置より安全設計）
- **被害を受ける側より被害を与える側が**（人間の注意の前に施設・設備の安全化）
- **力からの小さいものより力の大きなものが**（消費者より企業が、現場よりトップが）
- ・・・

優先して方策を施すのが原則

リスクアセスメントの手順

（ISO/IECガイド51より）



スリーステップメソッド

～リスク低減には順番がある～

（1）本質的安全設計によるリスクの低減
（2）安全防護対策(安全装置等)による
　　リスクの低減
（3）使用上の情報の提供による
　　リスクの低減
↑設計製造側の役割

↓作業者の役割

＊使用上の情報に基づき、教育、訓練、
組織・体制・管理、個人防具による
リスクの低減

本質的安全設計

（1）はじめから危険源が無いように設計せよ

（2）危険源のエネルギー等を下げて事故が起きても危害の酷さを小さくするように設計せよ

（3）危険源に人間が近づかなくて済むように設計せよ

（4）修理等の非定常作業をしなくて済むように信頼度高く設計せよ

安全設計の考え方の例

- 信頼性と安全性の概念
- 本質的安全設計
- 構造安全と確率安全
- フェールセーフ
- フォルトトレランス
- フールプルーフ
- フェイルソフト
- フォルトアボイダンス

- インターロック
- フォルトレジスタンス
- タンパレジスター
- 冗長性，多重性
- 多様冗長、独立性
- 機能安全
- ・・・・

安全設計における視点

- 機能を如何に維持させるか・・・信頼性の問題
- 安全性を如何に確保させるか・・・安全性の問題
- 科学的根拠（物理的、化学的、数理的根拠）に基づく客観性を重視すること
- 科学と価値（安全と安心）の関係を考慮すること
- 未然防止を第一義とすること
- 安全学からの視点：技術的、組織的、人間的側面から総合的に対応すること
- 安全学からの視点：ライフサイクル全体のわたり体系的に対応すること

安全設計の考え方

構造安全

- 機械設備が故障しても安全側になる･･･フェールセーフの構造
- 人間が間違えても大事には至らない･･･
  フールプルーフの構造

（コンフリクトはあり得る）

確率安全

- 信頼性を上げることで安全性を実現する･･･
  多重系、フォールトトレランス、多重防護の構造、数量化、機能安全

両者の融合が必須

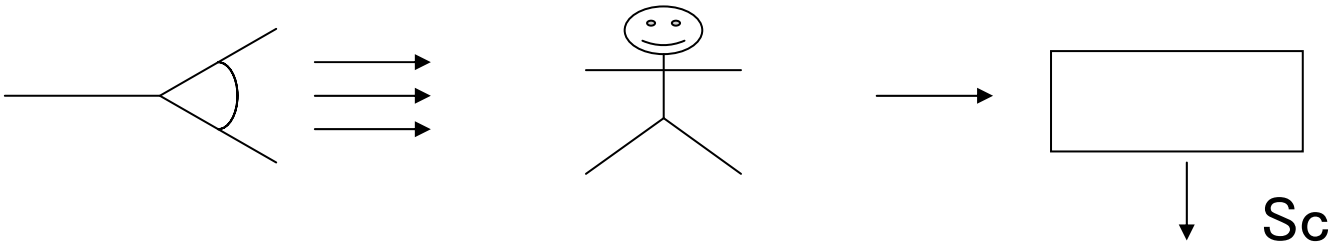
例：危険検出型と安全確認型

＊安全なシステムの作り方

1．危険検出型－－危険であることを検出して、この危険情報により作業を止める／回避する(ない時は続行)

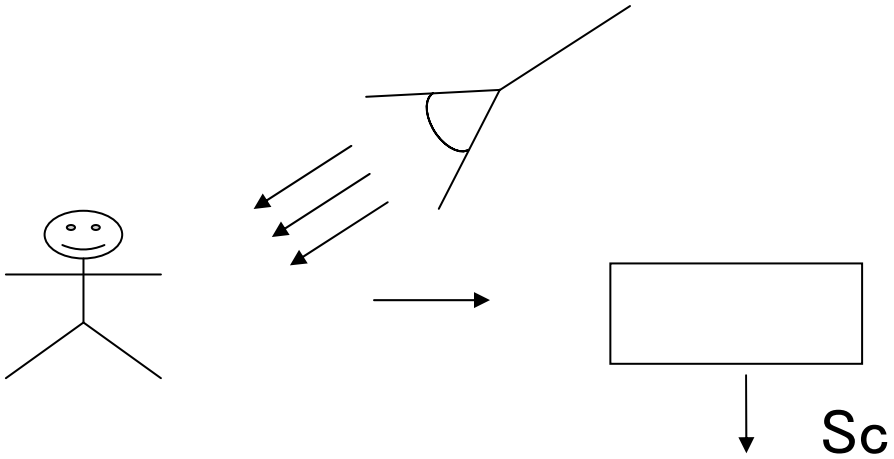
2．安全確認型－－安全でることを確認して、安全情報を受けているときだけ作業を続行する(ない時は実行しない)

Two types of light beam sensors



Safety : Absence of human

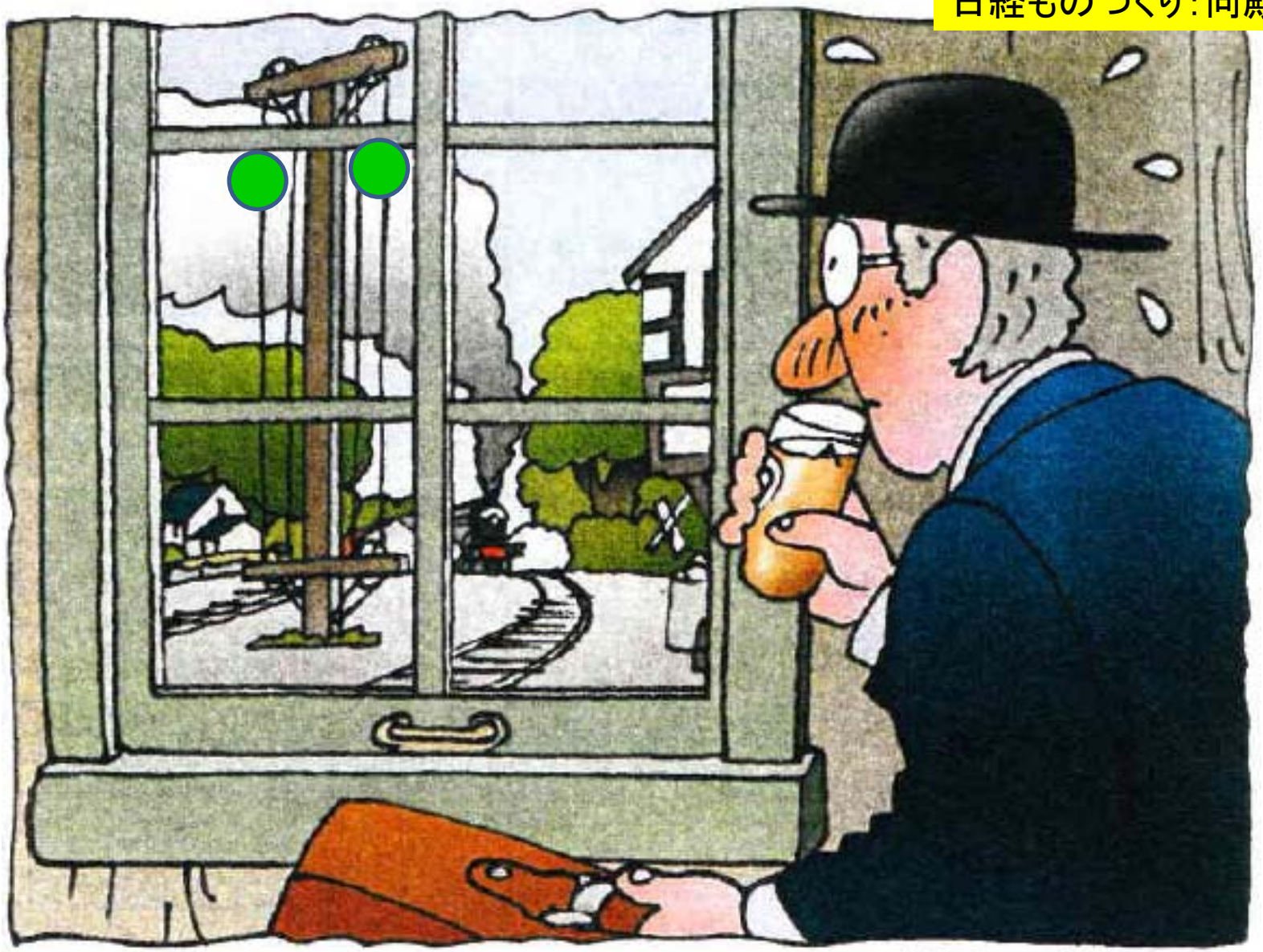
(a) **Transmission type**



Safety : Presence of human

(b) **Rader type**

ハイボールの原理
日経ものづくり：向殿

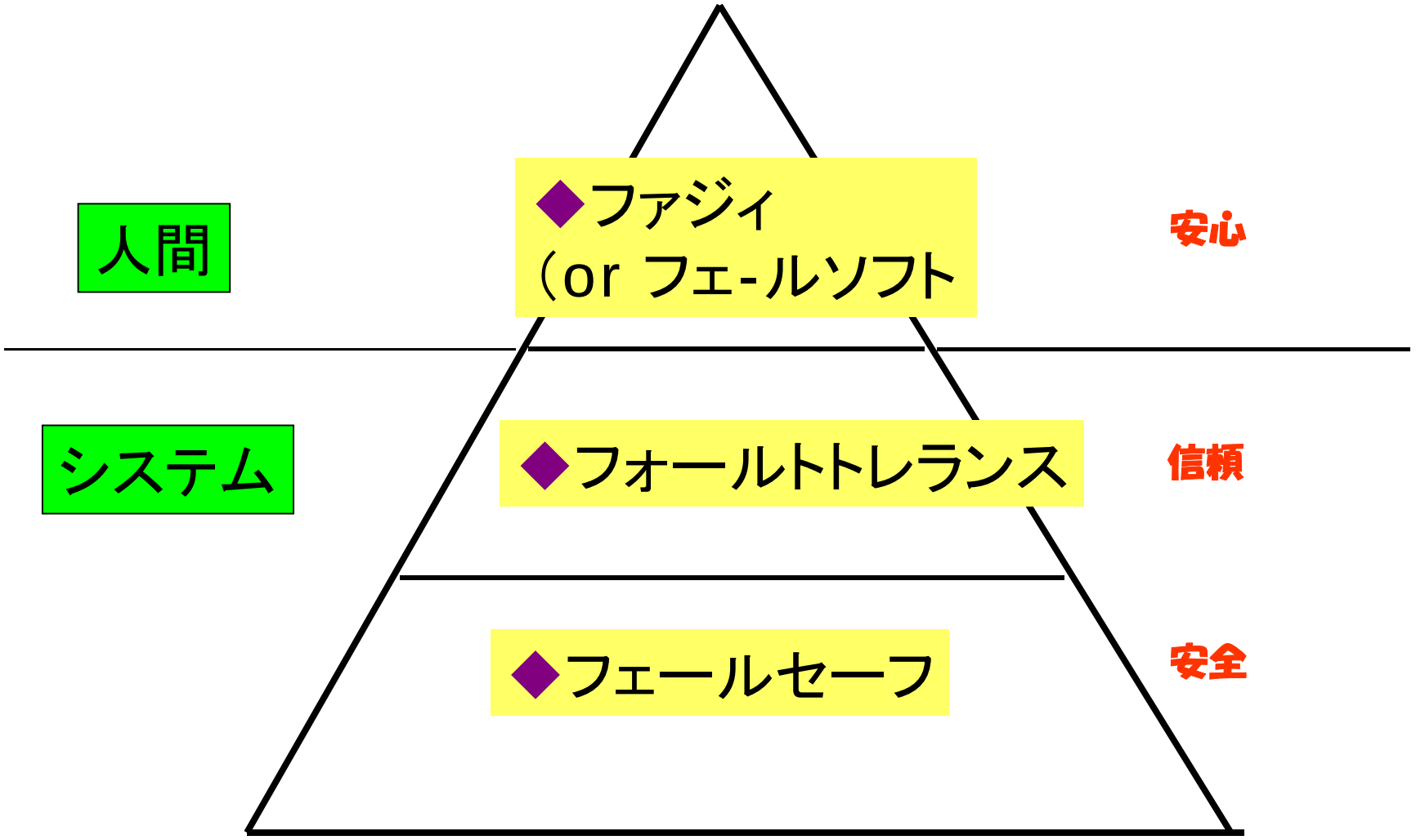


イラスト：つだかつみ

多重系における独立性

- 多重系は信頼度を上げることが目的
- 独立性の概念が重要
- common mode failure（共通原因故障）がないように、機構的にも、配置的にも、材料的にも、エネルギー的にも、コンピュータのソフトウエア的にも多様性をもった独立性が要請される
- このことは、監視やチェック等における組織や人間における独立性についても同様
- いくら高信頼であるとい言ってもすべてが駄目になる可能性はゼロではない。

◆F^{3}システムの提案



新しい安全の文化創造へ

～より高度な安全の実現に向けて～

- 安全思想の体系化
- 安全学の確立
- 技術者倫理の確立
- 企業トップの安全意識の向上・安全の価値を重視した経営
- 消費者力の向上
- 報道力の向上
- 安全を支援する社会制度の確立（税制・保険・認証・投資等の活用）
- 大学における安全教育・安全/保全技術者の育成と待遇改善
- 安全文化の向上
- 日本は、安全・安心を基本とした国づくりへ(Japan is back)

参考資料

- 日機連:機械工業の安全・安心のシステム構築に関する調査研究報告書（1）,2013-3
- ISO11161統合生産システム,2007
- 向殿監修、日機連編：機械・設備のリスク低減技術、pp.75~104, 2013-7