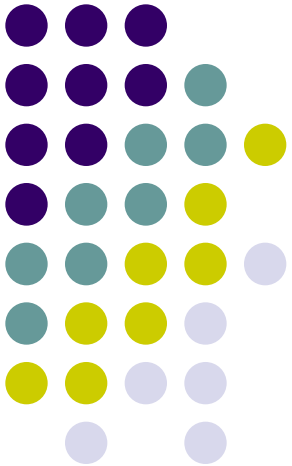
IMSの事故事例に見るセイフティシステムインテグレーションの課題

ーシステムインテグレーターとユーザーの安全責任の課題ー



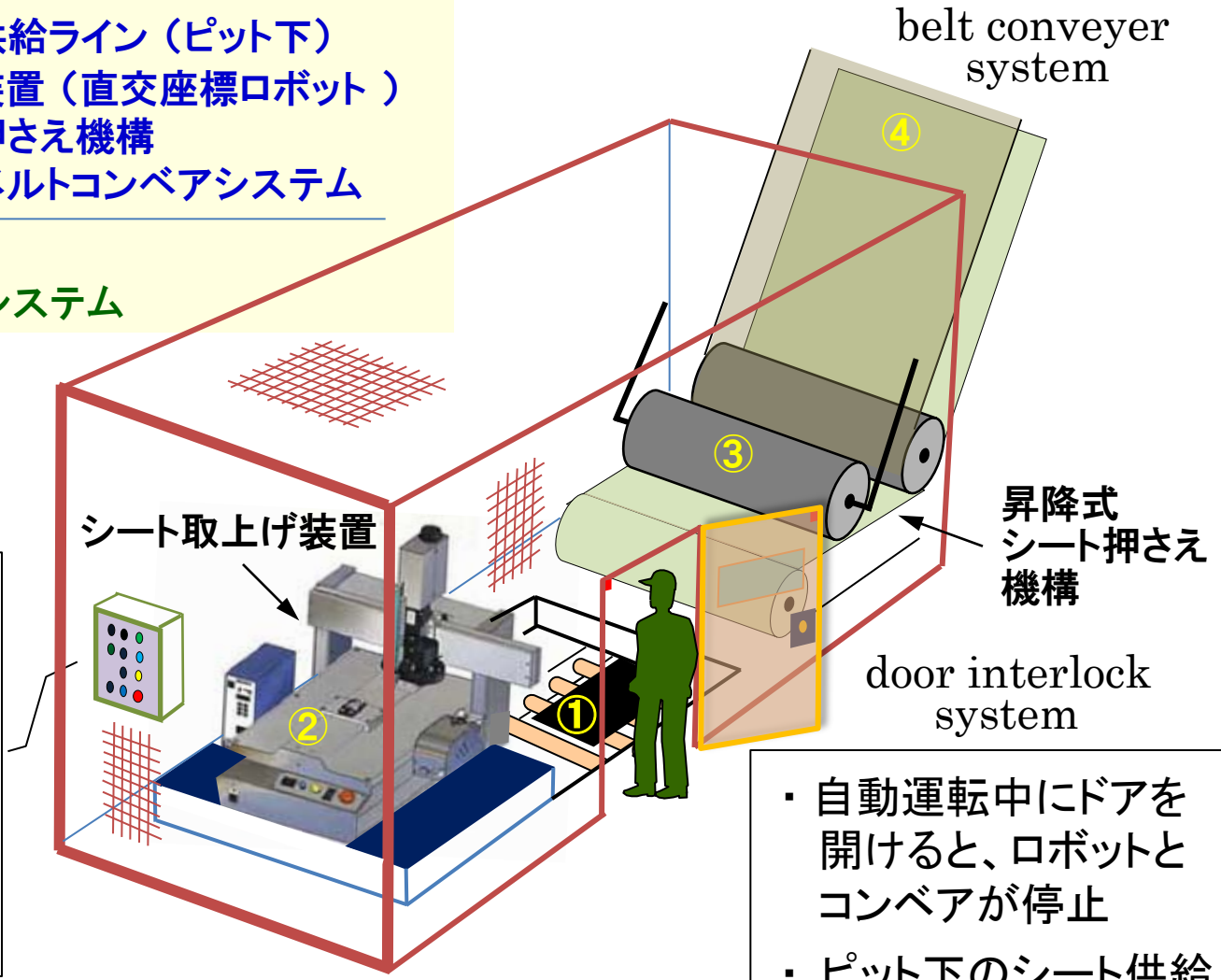
Safety Craft 代表　水 野　恒 夫

IMS におけるひとつの死亡事故例 （単一ゾーン内）

機械システムの構成要素

- ① 加工済シート供給ライン（ピット下）
- ② シート取上げ装置（直交座標ロボット ）
- ③ 昇降式シート押さえ機構
- ④ シート搬送用ベルトコンベアシステム

☆ 囲い式ガード
☆ ドアインタロックシステム



操作盤

- 手動モードを選択すると、ドアインタロックは「解除」
- 手動モードではコンベアの「連続運転」が可能

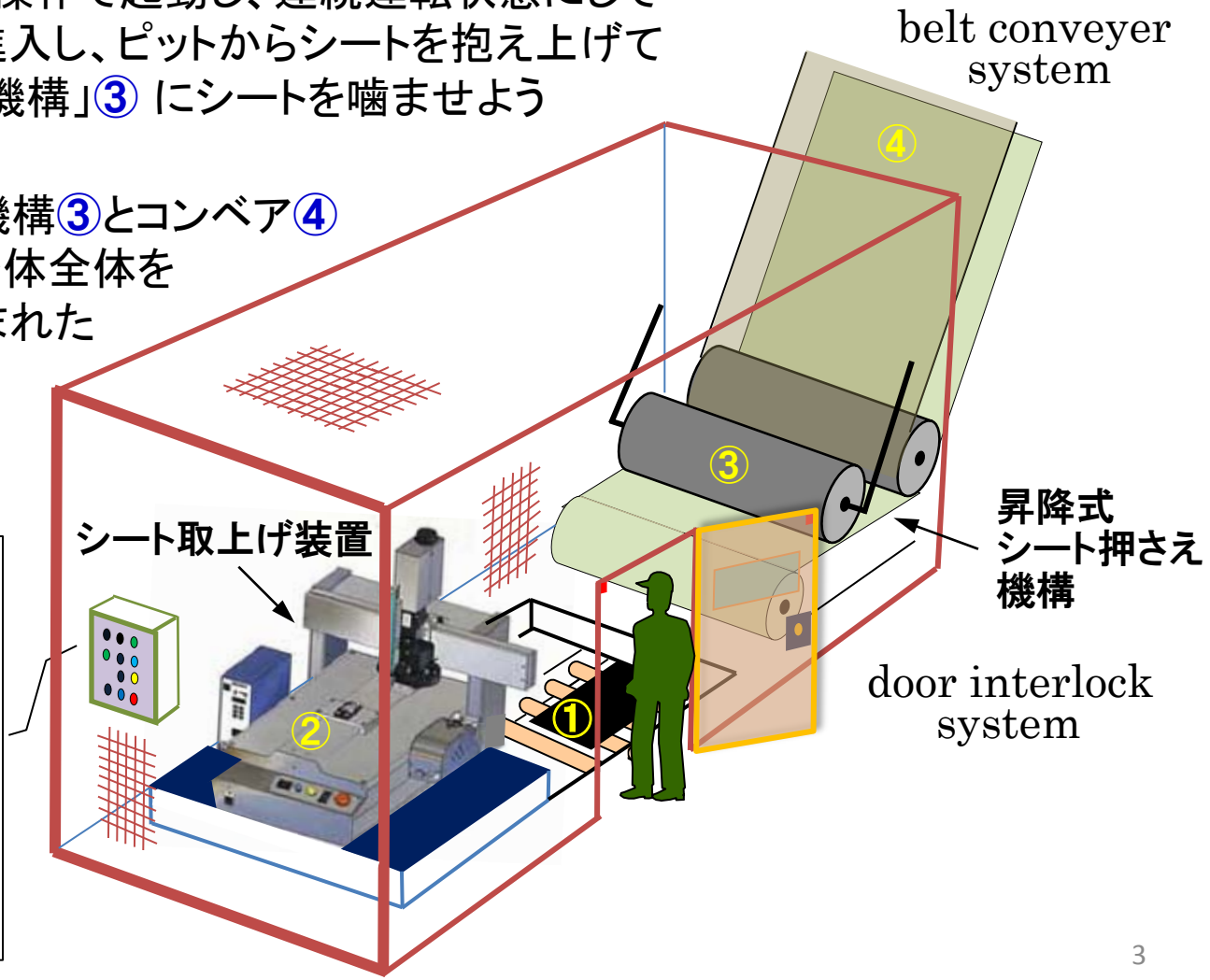
- 自動運転中にドアを開けると、ロボットとコンベアが停止
- ピット下のシート供給ラインは待機停止

事故の発生経過

1. シート取上げ装置（直交座標ロボット）② のシート掴み不良が発生し、機械停止
2. オペレータが操作盤を「手動モード」に切り替え、ロボットを待機位置へ
3. 「コンベア」④ を手動操作で起動し、連続運転状態にしてインタロックドアから進入し、ピットからシートを抱え上げて「昇降式シート押さえ機構」③ にシートを噛ませようとしたところ
4. 昇降式シート押さえ機構③とコンベア④の間に腕をとられ、身体全体をコンベア内に引き込まれた

操作盤

- 手動モードを選択すると、ドアインタロックは解除
- 手動モードではコンベアの連続運転が可能



事故時の制御条件から見た問題点 （赤字 が安全防護方策の選定の誤り）

システム要素	停止カテゴリー	運転モード/状態	備　考
シート搬送用ベルトコンベアシステム	—	手動モード 連続運転状態	ホールドトゥランを適用せず　IEC60204-1
昇降式シート押さえ機構	—	手動モード 作動圧入りの状態	エアシリンダーによる昇降動作
加工済シート供給ライン（ピット下）	停止カテゴリー2	待機停止	別の制御区分（Span of control）に属する
シート取り上げ装置（直交座標ロボット）	停止カテゴリー2 IEC60204-1	手動モード 制御停止状態	ロボット作動領域への立入りを許容
ドア・インタロックシステム	—	手動モードでは無条件でミュート ISO13849　ISO11161	自動モードでのみゾーン内の機械をインタロック停止

※ ユーザー（生産部門）は、シート取上げ装置（直交座標ロボット）のシート掴みの信頼性に不安があったため、従来通りの人手による取上げ作業が可能なように
手動モード選択時は　・ドアインタロックが無条件でミュートされ、ゾーン内へ任意に立入り
・コンベアはホールドトゥランではなく、連続運転の選択
を可能とするよう、システムインテグレータに要求していた

事故時の制御条件から見た問題点 （赤字 が安全防護方策の選定の誤り）

システム要素	停止カテゴリー	運転モード/状態	備　考
シート搬送用ベルトコンベアシステム	—	手動モード **連続運転状態**	**ホールドトゥランを適用せず　IEC60204-1**
昇降式シート押さえ機構	—	手動モード **作動圧入り**	ダーによる
加工済シート供給ライン（ピット下）	停止カテゴリー2	待機停止	（Span of する
シート取り上げ装置（直交座標ロボット）	**停止カテゴリー2** **IEC60204-1**	手動モード **制御停止状態**	**作動領域への立入りを許容**
ドア・インタロックシステム	—	**手動モードでは無条件でミュート** **ISO13849　ISO11161**	自動モードでのみゾーン内の機械をインタロック停止

システムインテグレータが異常処置のタスクのリスク評価を放棄？
ISO11161

※ ユーザー（生産部門）は、シート取上げ装置（直交座標ロボット）のシート掴みの信頼性に不安があったため、従来通りの人手による取上げ作業が可能なように
手動モード選択時は　・ドアインタロックが無条件でミュートされ、ゾーン内へ任意に立入り
・コンベアはホールドトゥランではなく、連続運転の選択
を可能とするよう、システムインテグレータに要求していた

Safety System Integration の観点から見た事故教訓（1）

■ システムインテグレーションの課題 「本質的安全設計」

・この事故の本質は、シート取上げ装置（直交座標ロボット）のシート掴みの信頼性の不足にある

・事故の未然防止策として、正しい安全防護方策が適用されていたとしても、安全な領域からのオペレーターの手動操作は難度が高く、オペレータの負荷の適切な軽減にはつながらない

― システムの信頼性の低さは、正しい安全防護をもってしても補うことはできない

■ セイフティシステムインテグレーションの課題 「安全防護方策」

◇ 制限なしのドアインタロックのミュート

・オペレータによる無効化を実質的に許容

・停止カテゴリー2 のロボットの作動範囲内への自由な立入り

◇ 手動モードでの制御原則の逸脱

・危険領域外からの手動操作によらず、危険領域内で適切な安全防護なしで、人手による異常処置

・ホールドトゥランによらず、手動モードで「連続運転」

― システムの信頼性に不安を抱くユーザーの要求に対して、システムインテグレータが、安全設計原則の妥協を拒むのは難しい局面も

Safety System Integration の観点から見た事故教訓（2）

■ 「システム承認」の責任の構造について再考が必要

この事故の責任所在は、システムインテグレータか、手動モードの誤った仕様を要求したユーザーのいずれにあるか？

双方の「システム承認者」に責任があるが、双方に責任がある場合は、日本では誰も責任を取らない（責任を感じない）

最終的な責任はユーザー側の「システム承認者」にあるが、名目的な承認者にとどまり、技術的な判断能力が欠如しているため、事故防止の責任所在は曖昧なまま

- **技術的なシステム評価能力を持つ者の助言により、システム承認者が承認の裏付けを担保する仕組みが必要**

■ システムインテグレーション（セイフティシステムインテグレーションを含む）の妥当性検証の主体/プロセスの分離独立

- **ユーザー要求へのシステムインテグレータの無原則な妥協、セイフティシステムインテグレーションの逸脱をチェックして、是正する牽制機能（人、組織または機関）の独立が必要**
- **システムインテグレーション機能がユーザー側に属する場合でも、インテグレータ、安全性の検証者いずれにも相応の「技術者倫理」が求められる**

Safety System Integration の観点から見た事故教訓（2）

■ **「システム承認」の責任の構造について再考が必要**

この事故の責任所在は、システムインテグレータか、手動モードの誤った仕様を要求したユーザーのいずれにあるか？

双方の「システム承認者」に責任があるが、双方に責任がある場合は、日本では誰も責任を取らない（責任を感じない）

最終的な責任はユーザー側の「システム承認者」にあるが、名目的な承認者にとどまり、技術的な判断能力が欠如しているため、事故防止の責任所在は曖昧なまま

- **技術的なシステム評価能力を持つ者の助言により、システム承認者が承認の裏付けを担保する仕組みが必要**

■ **システムインテグレーション（セイフティシステム含む）の妥当性検証の主体/プロセスの分離独立**

安全専門技術者が果たす役割

- **ユーザー要求へのシステムインテグレータの無原則な妥協、セイフティシステムインテグレーションの逸脱をチェックして、是正する牽制機能（人、組織または機関）の独立が必要**
- **システムインテグレーション機能がユーザー側に属する場合でも、インテグレータ、安全性の検証者いずれにも相応の「技術者倫理」が求められる**