STAMP/STPAの実用事例から得た教訓
～クレーンの遠隔制御の安全分析への応用～

2025年11月19日

会津大学　名誉教授　兼本茂
(株)タダノ　林洋幸

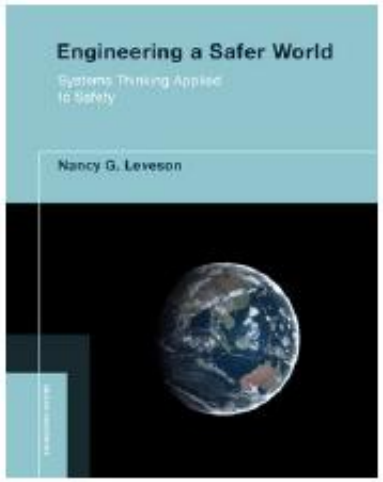
一般社団法人 組込みシステム技術協会
Japan Embedded Systems Technology Association

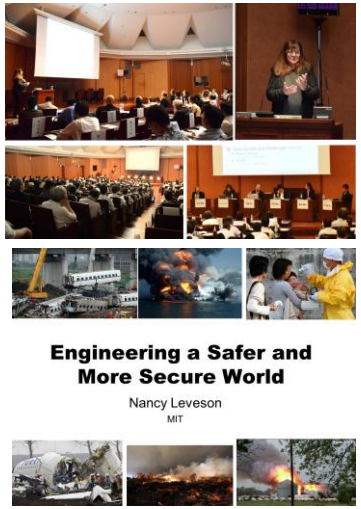
目次

- STAMP/STPA/CASTの概要
- クレーン遠隔操作システムの安全分析への適用
- 実システムへの適用から得た教訓

STAMP（Systems-Theoretic Accident Model and Processes）とは

2011年原著 ⇒ 2015年IPAセミナ ⇒ 2024年翻訳本 ⇒ 2025年　JASA STAMP広場開設





「JASA STAMP広場」で検索

「なるほどSTAMP（カラム記事）

なるほどSTAMP（Tips、コラム）

- コントロールストラクチャー（CS図）は物理モデルではない (2025-07-22, 1.0 MB)
- STAMP/STPAでの損失（Loss,Accident）の峻別とは（2025-07-22, 1.2 MB）
- STAMP/STPAにおけるハザードの定義は必須か？～「ハザードが定義できないアクシデント」を巡る考察～ (2025-07-22, 930 KB)
- STAMPのコントロールストラクチャーを考える（2025-10-23,925KB）
- STAMPはSTPAだけではない（2025-10-23,309KB）
- STAMPのキーワード 複雑システムと創発とは（2025-10-23,411KB）
- STPA分析での「状況（Context）」 の 考え方と取り扱い方法（2025 - 10-30.426KB）
- STPA分析でのHCF（ハザード因果要因）からLS(損失シナリオ）への変遷の理由（2025 - 10-30.440KB）

一般社団法人 組込みシステム技術協会 Japan Embedded Systems Technology Association

STAMPとは

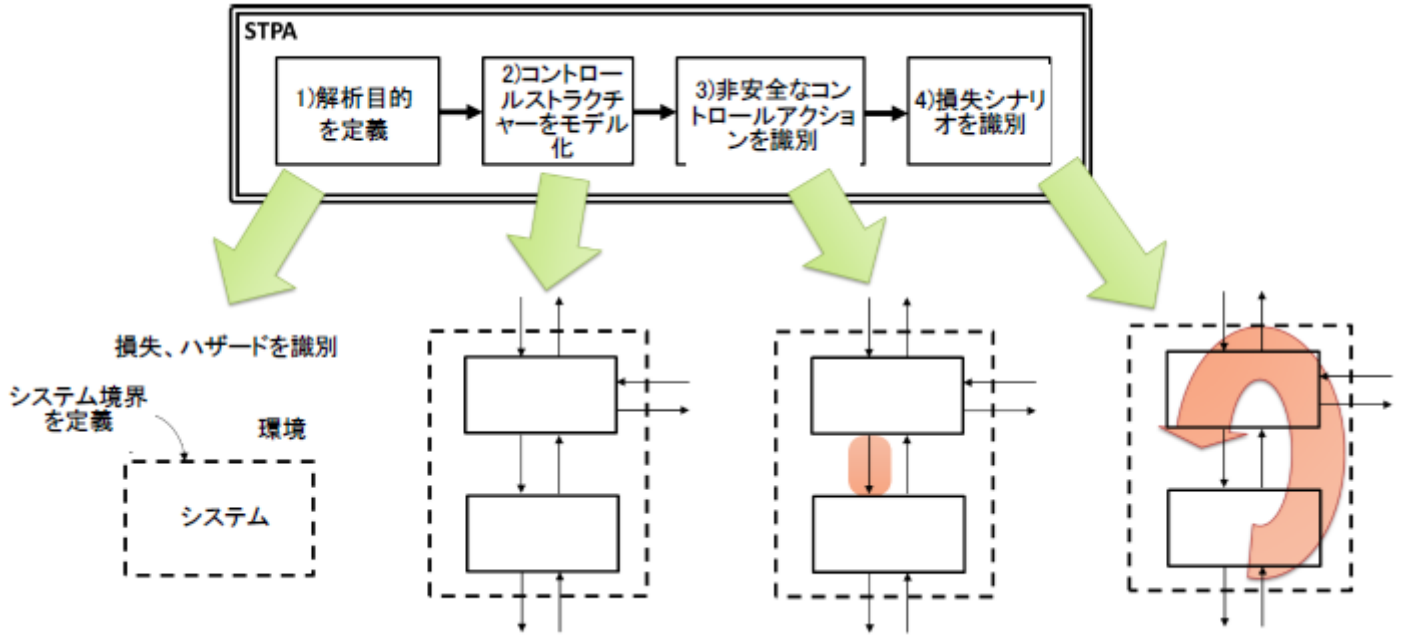
◎システム理論に基づいたSystemic（包括的）な安全分析の考え方と方法論（STPA/CAST)の提供
◎抽象化と階層化により作成した（機能・安全）制御構造モデルを通して包括的な安全分析を行う

◎従来の安全分析法で扱いにくい新たな因果要因として、ソフトウェアの欠陥も含む設計エラー、コンポーネントの相互作用による事故、認知的に複雑な人間の意思決定エラー、事故に影響する社会的・組織的・管理的要因などを含める
◎単一の因果要因から複合的な因果要因による事故の説明と対策

◎「信頼性の確保」から「安全の制御」へのパラダイムシフト

STPA_Handbook_JPv02/ CAST_HandbookJPN

STAMP:　Systems-Theoretic Accident Model and Processes
STPA:　Systems-Theoretic Process Analysis　（設計時の安全分析）
CAST:　Causal Analysis based on STAMP　（事故後の要因分析）



今回追加

［ ✚ ステップ⑤
シナリオに対する安全対策→システム安全方針としての整理 ］

STAMPと従来法の比較

	リスクアセスメント	従来法（FTA,FMEAなど）	STAMP（STPA、CASTなど）
基本的考え方	システムの危険源をベースに被害の厳しさ、発生頻度から、リスクのレベル（Safety Integrity Levelなど）を決め、そのレベルに応じて規格に沿った安全設計を行う。	コンポーネントの故障（ヒューマンエラー含む）が事故を引き起こす。各コンポーネントの信頼性を向上することで事故を防止する。	コンポーネントの故障だけでなく、コンポーネント間のコミュニケーションの不適切さなどの複合要因が事故を引き起こす。システム全体を網羅的に見て複合的な事故防止対策（安全のコントロール/制御）を考える。
基本知識	対象分野の専門知識、リスク評価手法	対象分野の専門知識、信頼性工学	複数分野の統合知識、システム理論
アプローチ	危険源、事故の被害の厳しさと発生頻度を定性的に評価し、リスクマトリックスに応じてリスクのレベルを決める。	各コンポーネントの故障の因果関係を、結果から原因（FTA)または原因から結果（FMEA)を辿って事故のシナリオを明示化する。	システム全体の構造を制御構造図で表し、各コンポーネントの制御指示とフィードバックループの振舞いの分析から、安全を制御する方策を考える。
適用対象	作業や設備一般、比較的単純なシステム。人的・組織的要因の考慮は限定的。	機械的要素と人の行動が中心で、因果関係が比較的単純なシステム。	自動車、航空機、原子力、医療機器、建設機械など、組織・人・ソフトウェア・機械が複雑に関わるシステム
適用範囲	現場安全の確保が主	主に設計段階で詳細設計が決まった後	設計（特に概念設計時）、運用、事故分析
導入難易度	低い（ただし、作業や設備に潜む経験的危険源の知識が必要）	低い（ただし、機械や部品の信頼性工学的知識が必要）	高い（分析手法やシステムモデリングに関するスキルが必要）

実システムへのSTAMP安全分析から得た教訓

CRANET

クラネット＝遠隔地操作システム

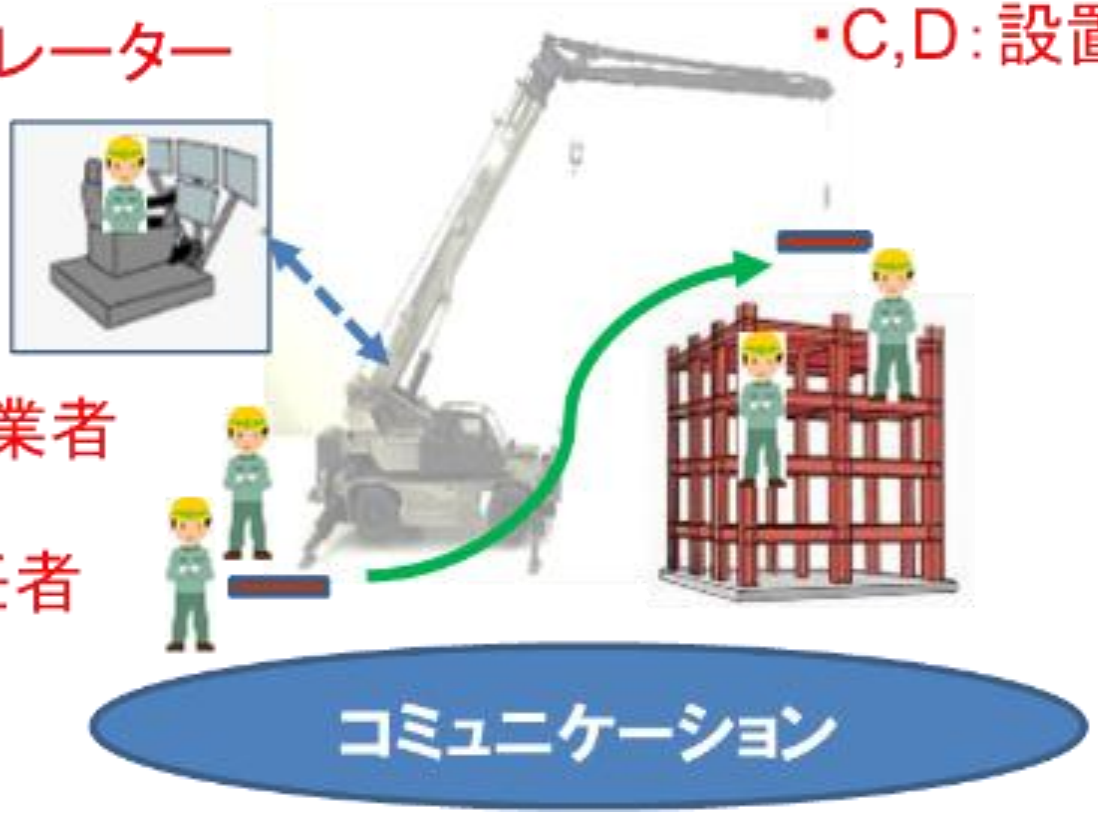
通信

課題
- 人と機械の協調作業時の安全分析
- 遠隔地操作での安全分析

クレーン遠隔操作作業での登場人物

・B：遠隔オペレーター

・C,D：設置作業者



・A'：玉掛作業者

・A：作業責任者

登場人物：5人

STPAでのアクシデントとハザードの定義（Step-1）

分析後の見直し（最終定義）

アクシデントID	アクシデント	ハザードID	ハザード	安全制約ID	安全制約
A1	ブームや吊荷との衝突により人や構造物、吊荷が損傷する	H1	ブームや吊荷と人や構造物との安全距離が保てない	SC1	ブームや吊荷と人や構造物との安全距離を保たなければならない
		H2	クレーンが不安定になり吊荷移動も不安定になる	SC2	クレーン本体のバランスを安定させなければならない
		H3	吊荷が不安定（巻上げや移動操作で吊荷が揺れたり落下したりする）	SC3	吊荷を安定させなければならない
		H4	吊荷に外力が加わり吊荷が揺れたり落下したりする	SC4	吊荷に外力をかけない
		H5	経年劣化でフックの取り付け治具、ワイヤなどの強度が低下する	SC5	定期検査などで経年劣化の対策を行う
A2	クレーン転倒で、人・構造物が大きく損傷する	H6	クレーンが不安定になり転倒しやすくなる	SC2	クレーン本体のバランスを安定させなければならない

分析当初の定義

アクシデントID	アクシデント	ハザードID	ハザード	安全制約ID	安全制約
A1	ブームや吊荷との衝突により人や構造物が損傷する	H1	ブームや吊荷と人や構造物との安全距離が保てない	SC1	ブームや吊荷と人や構造物との安全距離を保たなければならない
A2	クレーン本体の転倒により人や構造物が損傷する	H2	クレーン本体のバランスが不安定	SC2	クレーン本体のバランスを安定させなければならない
A3	吊荷の落下により人、構造物、吊荷が損傷する	H3	吊荷が不安定	SC3	吊荷を安定させなければならない
A4	吊荷が損傷する	H4	吊荷に外力が加わる	SC4	吊荷に外力をかけない

STPAでのアクシデントとハザードの定義（Step-1）

分析後の見直し（最終定義）

アクシデントID	アクシデント	ハザードID	ハザード	安全制約ID	安全制約
A1	ブームや吊荷との衝突により人や構造物、吊荷が損傷する	H1	ブームや吊荷と人や構造物との安全距離が		ブームや吊荷と人や構造物との安全距離
		H2			安定させなけ
		H3			ない
		H4	たりする		
		H5	経年劣化でフックの取り付け治具、ワイヤ	SC5	定期検査などで経年劣化の対策を行う
A2	クレーン転倒で、人・構造物が大きく損傷する	H6			を安定させなけ

アクシデントの整理
A1:ブームや吊荷との衝突で、人・構造材・吊荷が損傷
A2:クレーン転倒により、人・構造材の損傷
の二つに集約

A3:吊荷の落下により人・構造物・吊荷が損傷する
はA1に包含できる。
A4:吊荷の損傷も同様

分析当初の定義

アクシデントID	アクシデント	ハザードID	ハザード	安全制約ID	安全制約
A1	ブームや吊荷との衝突により人や構造物が損傷する	H1	ブームや吊荷と人や構造物との安全距離が保てない	SC1	ブームや吊荷と人や構造物との安全距離を保たなければならない
A2	クレーン本体の転倒により人や構造物が損傷する	H2	クレーン本体のバランスが不安定	SC2	クレーン本体のバランスを安定させなければならない
A3	吊荷の落下により人、構造物、吊荷が損傷する	H3	吊荷が不安定	SC3	吊荷を安定させなければならない
A4	吊荷が損傷する	H4	吊荷に外力が加わる	SC4	吊荷に外力をかけない

STPAでのアクシデントとハザードの定義（Step-1）

分析後の見直し（最終定義）

当初のハザード
H1:ブームや吊荷と、人・構造物との安全距離が保てない

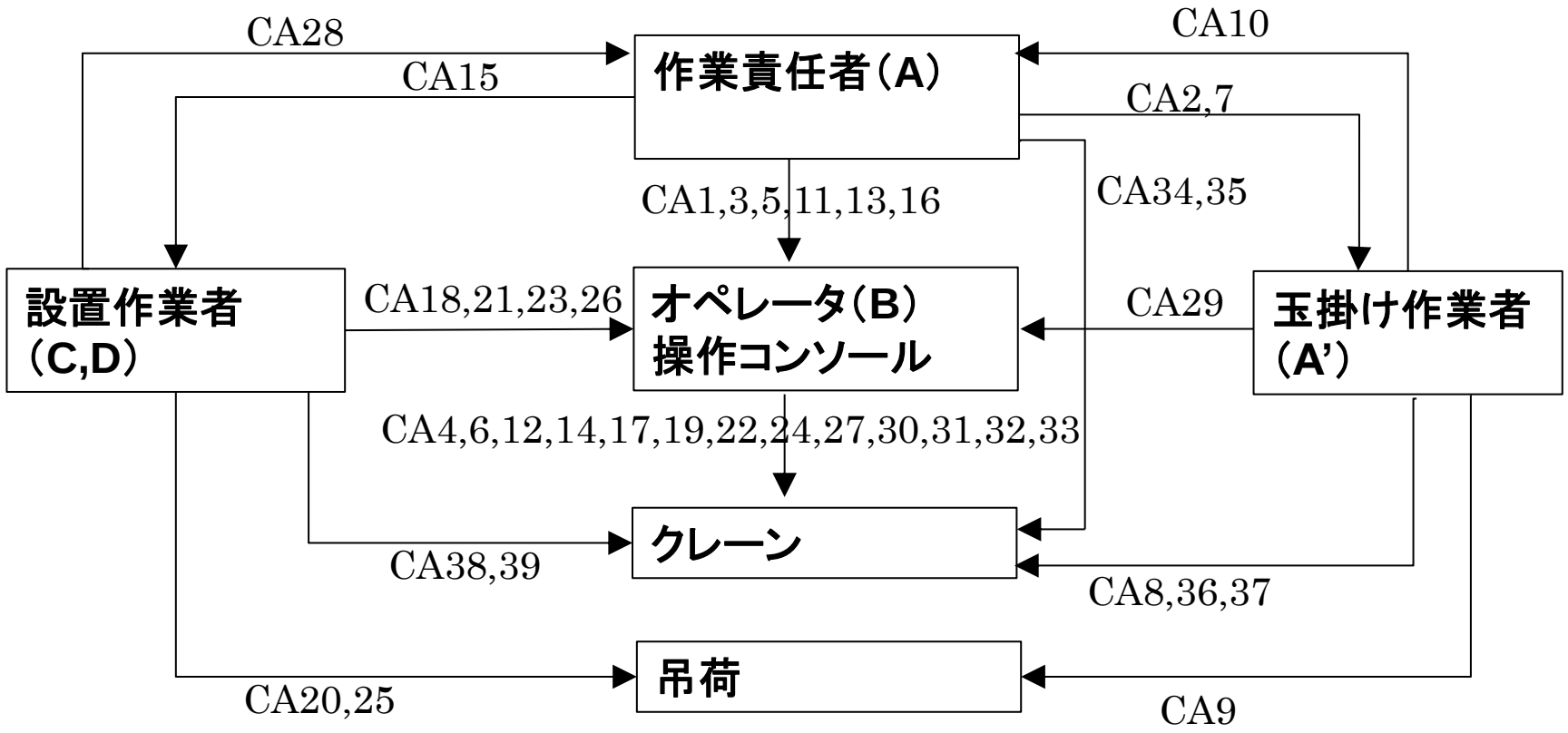
ハザードの見直し
H4:吊荷に外力が加わり、吊荷が揺れたり落下したりする

ハザードの見直し
H5:経年劣化でフックや取り付け治具、ワイアなどの強度が低下する

		ハザードID	ハザード	安全制約ID	安全制約
		H1	ブームや吊荷と人や構造物との安全距離が保てない	SC1	ブームや吊荷と人や構造物との安全距離を保たなければならない
		H2	クレーンが不安定になり吊荷移動も不安定になる	SC2	クレーン本体のバランスを安定させなければならない
A1	ブームや吊荷との衝突により人や構造物、吊荷が	H3	吊荷が不安定（巻上げや移動操作で吊荷が揺れたり落下したりする）	SC3	吊荷を安定させなければならない
		H4	吊荷に外力が加わり吊荷が揺れたり落下したりする	SC4	吊荷に外力をかけない
		H5	経年劣化でフックの取り付け治具、ワイヤなどの強度が低下する	SC5	定期検査などで経年劣化の対策を行う
A2	クレーン転倒で、人・構造物が	H6	クレーンが不安定になり転倒しやすくなる	SC2	クレーン本体のバランスを安定させなければならない

		ハザードID	ハザード	安全制約ID	安全制約
		H1	ブームや吊荷と人や構造物との安全距離が保てない	SC1	ブームや吊荷と人や構造物との安全距離を保たなければならない
		H2	クレーン本体のバランスが不安定	SC2	クレーン本体のバランスを安定させなければならない
A3	吊荷の落下により人、構造物、吊荷が損傷する	H3	吊荷が不安定	SC3	吊荷を安定させなければならない
A4	吊荷が損傷する	H4	吊荷に外力が加わる	SC4	吊荷に外力をかけない

制御構造図(Step-2) CAのみ表示

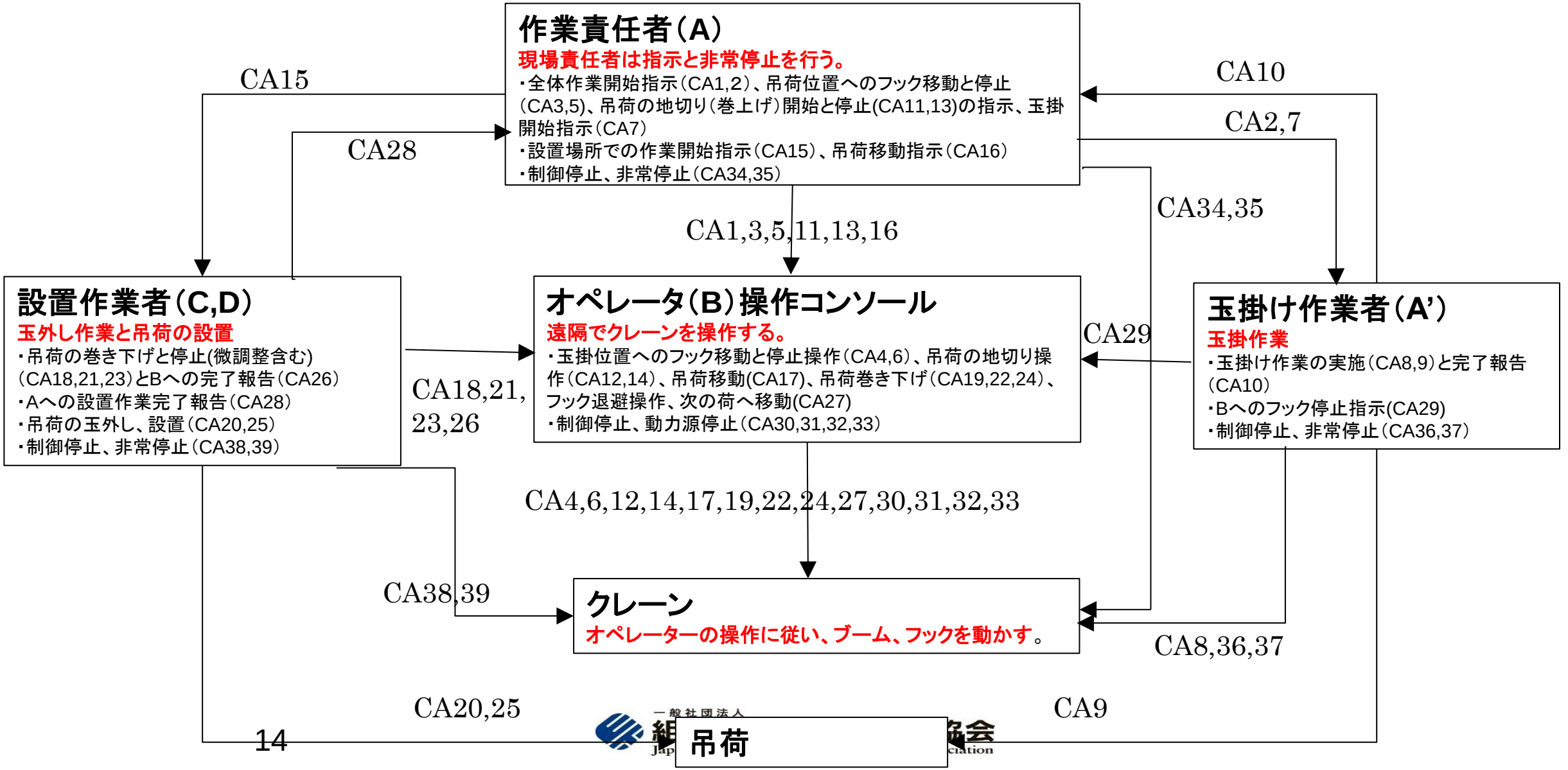


39のコントロールアクション(CA)

CA1 作業開始指示
CA2　作業開始指示
CA3 玉掛位置へフック移動指示
CA4 玉掛け位置へフック移動
CA5 フック停止指示
CA6 フック停止操作
CA7 玉掛け開始指示
CA8 玉掛作業：フック
CA9　玉掛作業：吊荷
CA10　玉掛完了報告
CA11　吊荷の地切り指示：巻上
CA12　地切り操作：巻上
CA13　地切り停止指示：巻上停止
CA14　地切り停止操作：巻上停止
CA15　作業開始指示：設置場所指示
CA16　吊荷移動指示：設置位置へ
CA17　吊荷移動：設置位置へ
CA18　吊荷停止指示、微調整含む：設置位置
CA19　吊荷停止操作、微調整含む
CA20　吊荷の設置、固定

CA21　玉外しのため巻下指示
CA22　巻下操作：玉外しのため
CA23　巻下停止指示
CA24　巻下停止操作
CA25　玉外し作業：吊荷側
CA26　玉外し完了報告
CA27　フック退避操作、次の荷へ移動
CA28　設置完了報告
CA29　フック停止指示
CA30　制御停止、操作信号通信遮断
CA31　制御停止解除
CA32　動力源停止
CA33　動力源始動
CA34　制御停止　無線スイッチで操作緩停止
CA35　非常停止、動力源停止　クレーン本体のスイッチ
CA36　制御停止　無線スイッチで操作緩停止
CA37　非常停止、動力源停止　クレーン本体のスイッチ
CA38　制御停止　無線スイッチで操作緩停止
CA39　非常停止、動力源0停止　クレーン本体のスイッチ

制御構造図（Step-2） 機能と安全制約、CAの関係を表示



UCA分析（Step-3）

UCA表0 / UCA表

No	CA	From	To	CA提供条件	Not Providing	Providing causes hazard	Too early / Too late	Stop too soon / Applying too long
1	CA1 作業開始指示（B応答）	現場責任者（鳶A)＊指示のみ	遠隔オペレーター(B)	・声掛け				
2	CA2　作業開始指示（A'状況、応答）	現場責任者（鳶A)＊指示のみ	鳶A'　＊作業を担当	・声掛け				
3	CA3 玉掛位置へフック移動指示(B応答、A',フック,クレーン,吊荷周辺の状況)	現場責任者（鳶A)＊指示のみ	遠隔オペレーター(B)	・Aは現場状況を確認	(UCA3-N-1) A⇒B Aからの移動指示はないが、フック、クレーンが動いて近くの人にぶつかる。 [SC1]	(UCA3-P-1) A⇒B フックの近くに人がいるのに、AがBにフック移動指示を出し、クレーンが動いて人や物にぶつかる。 [SC1]	(UCA3-T-1) A⇒B フック近くに人がいて、退避が終わる前に先にAからBに移動指示が出て、クレーンが動いて人にぶつかる。 [SC1]	
4	CA4 玉掛け位置へフック移動（A,A',フック,クレーン,吊荷周辺の状況）	遠隔オペレーター(B)	クレーン	・Aからのフック移動指示を受けてBがクレーンを操作	(UCA4-N-1) B⇒クレーン Bはフック移動操作をしていないが、クレーンが動いてフック	(UCA4-P-1) B⇒クレーン 人や物がフックの近くにいる状況で、Bがクレーンを動かしフ	(UCA4-T-1) B⇒クレーン フック近くの人の退避が終わる前、先にBがクレーンを動かし	

この１つ１つがUCAで番号[3]はCAと一致させる

CA12：地切り操作：巻き上げの損失シナリオの例(1)

整理後に分類を実施（ヒューマンエラーの例）

CA	UCA	ロスシナリオ番号 UCAごとに通し番号をつける。	ロスシナリオ:LS	分類	対策
CA12：B⇒クレーン 地切り操作：巻上(A,A'の指示、フック、クレーン、吊荷、周辺の状況)	(UCA12-P-1) B⇒クレーン 地切りの巻上操作が急操作なため、玉掛具や吊荷が破損する。吊荷がバランスを崩し落下する。 [SC3][SC4]	LS1	・通信や映像の遅れにより、オペレータBはクレーンが動いていないと思い、巻上操作が急操作になってしまい、玉掛具や吊荷の破損、吊荷が落下する。	ヒューマンエラー (作業対象者＋部外者)	C7 遅延の理解：移動開始、停止の遅れ C10 通信遅延対策、表示
		LS2	・Aは吊荷の状態が見えないにも関わらず、急に操作指示を出し、かつオペレータBも自分で安全確認をせずにフックを動かして吊荷が落下する。		C1 A,A',C,Dまたは Bへの死角を補う機能 C6 クレーン動作の最終判断はオペレータB
		LS3	・オペレータBだけの判断で地切り操作をしたところ、吊り荷がバランスを崩し落下する。		C2 複数人での安全確認（遠隔と現場で）
		LS4	・AまたはBはまだ玉掛け中にも関わらず（見落とし、確認不足）操作指示を出し、そのままオペレータBがクレーンを動かして吊荷が破損や落下する。		C1 A,A',C,Dまたは Bへの死角を補う機能 C2 複数人での安全確認（遠隔と現場で） C6 クレーン動作の最終判断はオペレータB
		LS5	・操作レバーが断線し、操作信号が急に中立になった場合、操作が急停止し、玉掛具や吊荷の破損、吊荷が落下する。	遠隔地操作システムの故障、通信の不具合	C17 作業前点検、動作不良の確認 C12 自己診断：クレーン側、操作側

CA12：地切り操作：巻き上げの損失シナリオの例(1)

整理後に分類を実施（ヒューマンエラーの例）

CA	UCA	ロスシナリオ番号 UCAごとに通し番号をつける。	ロスシナリオ:LS	分類	対策
CA12：B⇒クレーン 地切り操作：巻上(A,A'の指示、フック、クレーン、吊荷、周辺の状況)	(UCA12-P-1) B⇒クレーン 地切りの巻上操作が急操作なため、玉掛具や吊荷が破損する。吊荷がバランスを崩し落下する。 [SC3][SC4]	LS1	・通信や映像の遅れにより、オペレータBはクレーンが動いていないと思い、巻上操作が急操作になってしまい、玉掛具や吊荷の破損、吊荷が落下する。	ヒューマンエラー（作業対象者＋部外者）	C2 複数人での安全確認（遠隔と現場で） C6 クレーン動作の最終判断はオペレータB
		LS2	・Aは吊荷の状態が見えないにも関わらず、急に操作指示を出し、かつオペレータBも自分で安全確認をせずにフックを動かして吊荷が落下する。		
			・オペレータBだけの判断で地切り操作をしたところ、吊り荷がバランスを崩し落下する。		
			・AまたはBはまだ玉掛け中にも関わらず（見落とし、確認不足）操作指示を出し、そのままオペレータBがクレーンを動かして吊荷が破損や落下する。		
			・操作レバーが断線し、操作信号が急に中立になった場合、操作が急停止し、玉掛具や吊荷の破損、吊荷が落下する。	遠隔地操作システムの故障、通信の不具合	C17 作業前点検、動作不良の確認 C12 自己診断：クレーン側、操作側

（分類）ヒューマンエラー（作業対象者＋部外者）

◇通信や映像の遅れにより、オペレータBはクレーンが動いていないと思い、巻上操作が急操作になってしまい、玉掛具や吊荷の破損、吊荷が落下する。

◇オペレータBだけの判断で地切り操作をしたところ、吊り荷がバランスを崩し落下する。

CA12：B⇒クレーン
地切り操作：巻上（A,A'の指示、フック、クレーン、吊荷、周辺の状況）

UCA12-P-1：B⇒クレーン
地切りの巻上操作が急操作なため、玉掛具や吊荷が破損する。吊荷がバランスを崩し落下する。
[SC3] [SC4]

CA12：地切り操作：巻き上げの損失シナリオの例(2)

遠隔地操作システムの故障、通信の不具合

LS5	・操作レバーが断線し、操作信号が急に中立になった場合、操作が急停止し、玉掛具や吊荷の破損、吊荷が落下する。	遠隔地操作システムの故障、通信の不具合	C17 作業前点検、動作不良の確認
LS6	・オペレータBが操作していないのに、操作装置（レバー）が故障して操作出力が出たままになり、クレーンが動いて吊荷が落下する。		C12 自己診断：クレーン側、操作側 C17 作業前点検、動作不良の確認
LS7	・オペレータBは操作していないが、クレーン側のコントローラの暴走などにより、クレーンが勝手に動き吊荷が落下する。	クレーン本体故障（含む設定不良）	C12 自己診断：クレーン側、操作側 C5 動力源停止機能（オペレータB） C3 制御停止：緩停止（現場作業者A,A',C,D） C4 非常停止：動力源停止（クレーン近くのA,A）

（分類）遠隔地操作システムの故障、通信の不具合
◇操作レバーが断線し、操作信号が急に中立になった場合、操作が急停止し、玉掛具や吊荷の破損、吊荷が落下する。

CA12：地切り操作：巻き上げの損失シナリオの例(3)

クレーン本体故障、外部要因（風、地震、低温など）

LS7	・オペレータBは操作していないが、クレーン側のコントローラの暴走などにより、クレーンが勝手に動き吊荷が落下する。	クレーン本体故障(含む設定不良)	C12 自己診断：クレーン側、操作側 オペに機能、クレーン状態を通知：旋回フリー、緩停止、傾斜情報 C17 作業前点検、動作不良の確認
LS8	・旋回フリー機能がONになっており、旋回操作を停止していたつもりがフックが流れて（動いて）吊荷が破損、落下する。		C15 オペに機能、クレーン状態を通知：旋回フリー、緩停止、傾斜情報
LS9	・急操作などにより玉掛け具やワイヤが破断し、吊り荷が落下する。	外部要因(風、地震、低温など)	C17 作業前点検、動作不良の確認
LS10	・オペレータBは操作を行ったが、低温によりクレーンの油圧系の動作が遅れて急操作となり吊荷が破損、落下する。停止動作も同様。		
LS11	・玉掛作業中に突風が吹き、フックまたは玉掛具がA'にぶつかる。		

（分類）クレーン本体故障（含む設定不良）
◇オペレータBは操作していないが、クレーン側のコントローラの暴走などにより、クレーンが勝手に動き吊荷が落下する。

（分類）外部要因（風、地震、低温など）
◇急操作などにより玉掛け具やワイヤが破断し、吊り荷が落下する。

安全対策のグループ化と機能・運用・教育の区分け（Step-5）

（システム安全方針）　（シナリオごとの安全対策）　（対策の分類）

対策表	分類	ID	安全対策の要約	機能	運用	教育	対策対象
①相互監視手段、停止手段の確保	監視支援	C1	A, A', C, DまたはBへの死角を補う機能	○			操作コンソール A, A', B, C, D
		C2	複数人での安全確認（遠隔と現場で）		○		A, A', B, C, D
	停止支援	C3	制御停止：緩停止（現場作業者A, A', C, D）	○			クレーン側遠隔機器 A, A', C, D
		C4	非常停止：動力源停止（クレーン近くのA, A'）	○			クレーン A, A', C, D
		C5	動力源停止機能（オペレータB）	○			操作コンソール B
②クレーン動作の最終判断はオペレータB	判断明示	C6	操作の復唱、明示する。		○		B
		C7	遅延の理解：移動開始、停止の遅れ			○	A, A', B, C, D
③指示系統の確保	指示支援	C8	指示明確化、誰から誰へか	○	○		操作コンソール A, A', B, C, D
		C9	音声伝達手段の確保	○			操作コンソール A, A', B, C, D
④通信確保：現場―操作コンソール間	通信確保	C10	通信遅延対策、表示	○			操作コンソール クレーン側遠隔機器
		C11	現場に合わせた通信方式の選定		○		施工現場 A, B
⑤異常の通知	自己診断	C12	自己診断：クレーン側、操作側	○			操作コンソール クレーン側遠隔機器
⑥作業環境の確認	現場環境、機械状況の確認	C13	他の現場作業者への表示や音声警告	○		○	クレーン 周囲作業者
		C14	気象確認、風検知など	○	○		施工現場 A
		C15	オペに機能、クレーン状態を通知：旋回フリー、緩停止、傾斜情報	○			操作コンソール
		C16	作業範囲の立ち入り制限		○		A, A', B, C, D
⑦確実な作業前点検の実施。	作業前点検	C17	作業前点検、動作不良の確認		○		クレーン A, B
⑧動力源の始動判断は現場側	始動方法	C18	動力源の始動は現地作業者の許可（確認）を得てから		○		A, A', C, D

安全対策のグループ化と機能・運用・教育の区分け（Step-5）

（システム安全方針）　（シナリオごとの安全対策）　（対策の分類）

対策表	分類	ID	安全対策の要約	機能	運用	教育	対策対象
①相互監視手段、停止手段の確保	監視支援	C1	A, A', C, DまたはBへの死角を補う機能	○			操作コンソール A, A', B, C, D
		C2	複数人での安全確認（遠隔と現場で）		○		A, A', B, C, D
	停止支援	C3	制御停止：緩停止（現場作業者A, A', C, D）	○			クレーン側遠隔機器 A, A', C, D
		C4	非常停止：動力源停止（クレーン近くのA, A'）	○			クレーン A, A', C, D
		C5	動力源停止機能（オペレータB）	○			操作コンソール B
②クレーン動作の最終判断はオペレータB	判断明示	C6	操作の復唱、明示する。		○		B
		C7	遅延の理解：移動開始、停止の遅れ			○	A, A', B, C, D
③指示系統の確保	指示支援	C8	指示明確化、誰から誰へか	○	○		操作コンソール A, A', B, C, D
		C9	音声伝達手段の確保	○			操作コンソール A, A', B, C, D
④通信確保：現場―操作コンソール間	通信確保	C10	通信遅延対策、表示	○			操作コンソール クレーン側遠隔機器
		C11	現場に合わせた通信方式の選定		○		施工現場 A, B
⑤異常の通知	自己診断	C12	自己診断：クレーン側、操作側	○			操作コンソール クレーン側遠隔機器
							クレーン

CA:39→UCA:58→LS:246→
対策:344→18（重複無し）→8種の安全方針

まとめ(1)　分析項目数と人工実績

- CA:39、UCA58、LS:246、対策：344→18（重複無し）
  - 単一UCAに対し複数のLS(損失シナリオ)が導出される。対策も、一つのLSに対し複数の対策が導出される。特に、人の作業に対しては、多重の対策で安全を確保することが大事になる。しかし、結果的に導出される対策は類似のものが多くあるため、UCAやLSよりも少なくなる
  - 18種得られた安全対策はグルーピングにより8種の安全方針としてまとめられた。LSごとの安全対策の羅列ではなく、システム全体の安全を考えてグルーピングすることにより、関係者の間の情報共有が可能になる他、次世代への技術継承にも役立つ。ボトムアップ的作業であるが、STPA4ステップの後のStep-5として重要である。
- 今回の分析にかかった人工は、月1回の検討会で4人日（準備作業と検討時間）x12回（1年間）で、合計48人日程度と見積もれる。（用語理解と手順の習得も含む）

まとめ(2)　分析結果の評価

■　STPAは、システム全体の事故シナリオを網羅的に見れ、新たな気づきもあり有効な手段であった。

- C2：複数人での安全確認、C8：誰から誰への指示か明確化、などについては導出されると当たり前ではあるが、その重要性を再認識できた
- 複数の停止手段も想定はしていたが、その必要性を再認識できた
- 分析結果の可視化により、複数の関係者でその是非を議論でき、機能改善に役立てた（動力源の再始動の指示を現地と遠隔地で行うなど）
- 動作試験での不具合も、事前のシナリオの範囲であり、冷静に対応できた
- 社内の専門家（クレーンオペレータ）の評価としても、合理的なシナリオと安全対策が導出されているとのことであった。分析結果を整理して可視化でき、関係者のレビューが容易にできた
- 通常のクレーン作業でも安全につながる気づきもあり、STPAは有効であった

教訓

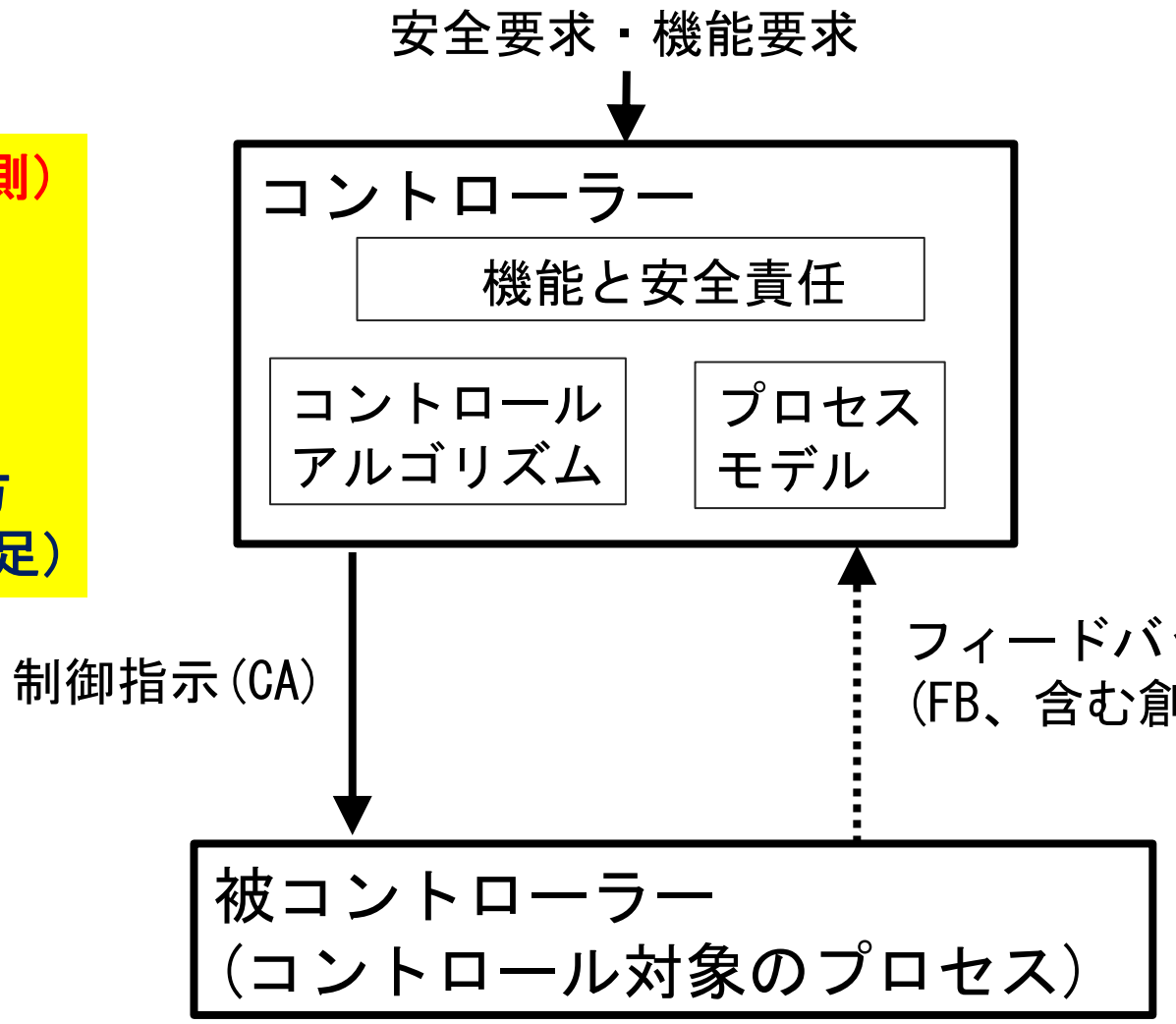
- ハザードは、UCAと損失シナリオまで導出した後に見直してもよい。特に、事故の兆候が明確でないシナリオがある場合（今回の例では吊り上げワイアが突然切れてしまう場合など）には、その兆候を考察しなおすことが大事である。
- システム全体の安全を考えて、コンポーネント安全対策を整理（グルーピング）することは、ボトムアップ作業で手間はかかるが、関係者の理解の共有化や、次世代への技術継承のために大事である（STPA　Step-5の必要性）
  - コンポーネント安全対策は、損失シナリオが明確でないと導出できないが、異なる損失シナリオでも同じ安全対策がでてくることが多いので、それまでの導出対策を参照し選択できるとよい
- 制御構造図の可視化では、複数の断面で表示することで理解しやすくなる。複数の関係者でレビューする際には非常に大事になる

- **第3者に分析結果をレビューしてもらうには、上記の機能は欠かせない！**

制御構造図と複合要因の推察の大切さ(発表者の解釈)

複合要因(制御指示側)
コントローラ側
・間違った指示
・**あいまいな指示**
被コントローラ側
・**間違った受け止め方**
(不注意、スキル不足)

担当管制官から海保機への指示・復唱では、双方にコミュニケーションミスの責任がある。
海保機の機長と副操縦士の間のコミュニケーションにもミスがある。



複合要因(フィードバック側)
被コントローラ側
・FBの欠如
・間違ったFB
・**あいまいなFB**
・**創発的なFB**
(事前に気づかなかった情報)
コントローラ側
・プロセスモデルの間違い
・制御アルゴリズムの間違い

ビジネス分野では「報連相」の大事さが教えられる。
担当管制官と連携管制官の責任分担があいまいで、あいまいなFBとなって、海保機の滑走路侵入を見逃した。
夕方の滑走路と海保機の視認性が悪く(同じ白色灯の使用)海保機の見逃しにつながった

ご静聴ありがとうございました。質問などがあれば、
JASAの安全性向上委員会に問い合わせください。

（JASA技術本部事務局：JASAINFO@JASA.OR.JP）