HITACHI
Inspire the Next

STAMP/STPA,CAST分析を用いた 安全設計評価手法とインシデント対応事例の紹介

2024/9/12

株式会社 日立製作所
○斎藤 英一, 菊池 則孝, 高久 欣丈

E-mail：eiichi.saito.qv@hitachi.com

HITACHI
Inspire the Next

Contents

0．自己紹介

HITACHI
Inspire the Next

1993年入社以来、品質保証業務を担当
（電子機器開発, 道路システム, 電力システム･･･）

本発表に至った経緯
2018年頃～：産業用ロボットを活用した製品開発が本格化
⇒産業用ロボットの安全設計に関する社内有識者がいない

▼

“安全資格”要員認証制度[1]で知識を習得
2019年：セーフティサブアセッサ(SSA)資格取得
2020年：セーフティアセッサ(SA)資格取得
⇒資格試験で学んだ知識より、社内向け安全設計ガイドラインを作成

▼

2021年～：STAMP/STPA,CASTを知り、公開されている情報[2][3][4]や
SQiPシンポジウム他の発表を聴講し自己学習
業務適用により知見を収集中

[1] 日本認証株式会社, ”安全資格”要員認証委制度のご案内HPデーター【20220715】.pdf (japan-certification.com)
[2] STPA HANDBOOK 日本語版 Ver.0.2 http://psas.scripts.mit.edu/home/get_file2.php?name=STPA_handbook_japanese.pdf
[3] CAST HANDBOOK 日本語版 Ver.0.1 http://psas.scripts.mit.edu/home/wp-content/uploads/2021/06/CAST_HandbookJPN.pdf
[4] 独立行政法人情報処理推進機構（IPA） 複雑化したシステムの安全性確保：IPA 独立行政法人 情報処理推進機構

STAMP System-Theoretic Accident Model and Processes
STPA System-Theoretic Process Analysis / STAMP based Process Analysis
CAST Causal Analysis based on System Theory

HITACHI
Inspire the Next

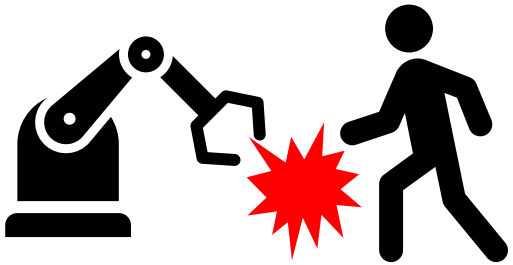
Contents

1.1 背景 “ロボットシステムの課題”

■ロボットを使用する場合、安全性の確保が重要な課題
■近年、ロボットを使用するシステムの動作が複雑化

課題

✓ ロボット制御はソフトウェア主体となり、
センサーデータや画像認識を使用することで動作が複雑化
✓ 人の意図しない行動や誤使用は予見が困難



システムが複雑化し、従来のリスク低減プロセスでは
危険事象を見つけることが難しくなってきている

1.2 背景 “ロボットシステムの課題”

HITACHI
Inspire the Next

リスク低減プロセス改善の取り組み

- 危険事象を見つけるために、STAMPを導入
- STAMP/STPAとSTAMP/CASTを融合した手法を検討

導入の経緯

STEP1 体系的に潜在的なリスク要因を分析できるSTAMP/STPAを導入

But リスク低減プロセスのみではインシデントが発生してしまうことがある。

例） ロボットの場合、安全柵などで人への危害リスクは低減していても、ロボットの異常動作で発生した物的被害が安全上のリスクになることがある。

STEP2 インシデントから学び、
発生したリスク要因を分析できるSTAMP/CASTを導入

目的/分析内容

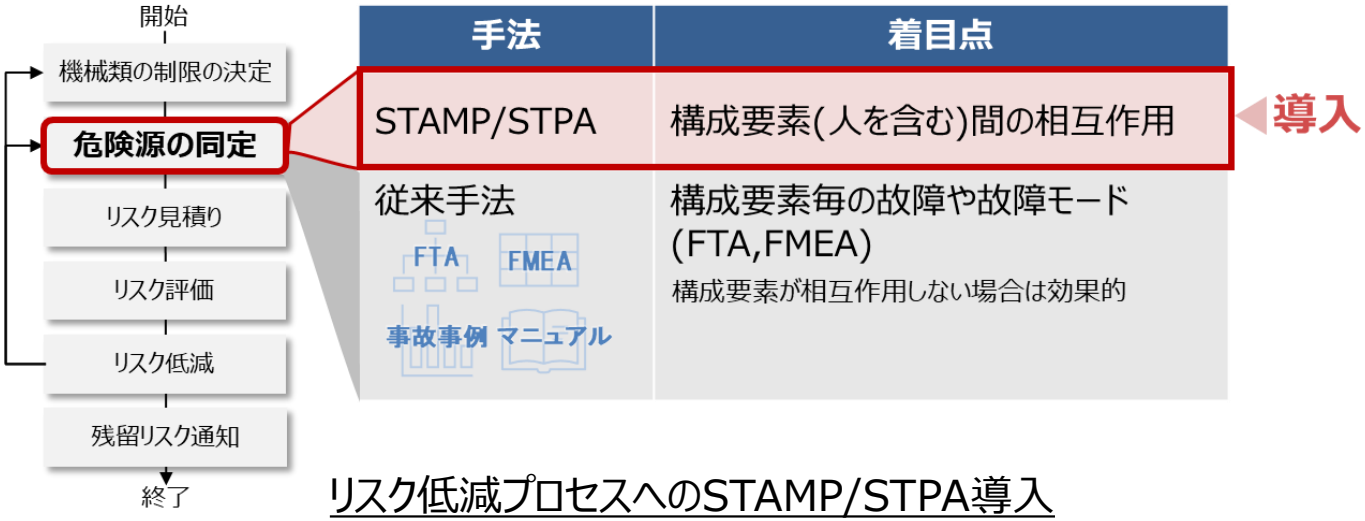
手法	目的	分析内容
STAMP/STPA	**事前解析**による**未然防止**	潜在的なリスク要因を分析
STAMP/CAST	**事後解析**による**再発防止**	発生したリスク要因を分析

HITACHI
Inspire the Next

STAMP/STPAの特徴と利点

STAMP/STPAの特徴

FTA,FMEAでは分析が難しい、構成要素が相互作用するシステムの分析が可能



リスク低減プロセスへのSTAMP/STPA導入

STAMP/STPA導入の利点

- STPA分析の成果物をリスク低減プロセスに取り込める
- システム全体を抽象化したモデルで分析するため、設計初期段階から導入が可能
  （要求仕様が確定すればシステム全体の安全構造を把握できる）
- 各Stepでの成果物が体系的に紐づいており、設計変更時の影響範囲検討が容易

FTA： Fault Tree Analysis
FMEA：Failure Mode and Effects Analysis

1.4 背景 “インシデント対応へのSTAMP/CAST導入”

HITACHI
Inspire the Next

STAMP/CASTの利点と分析手順

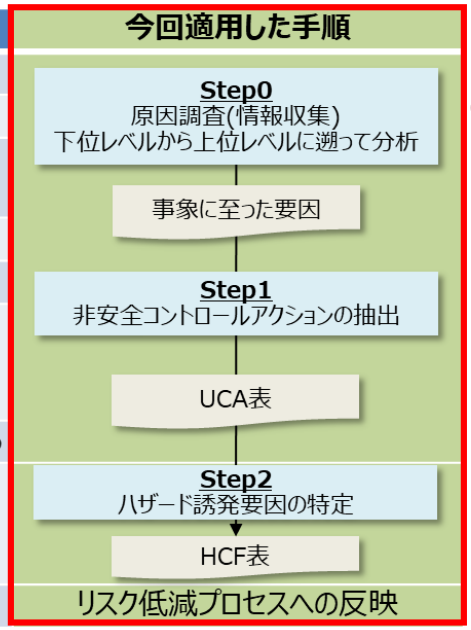
STAMP/CAST導入の利点

- 製品開発時のSTPA分析の成果物を利用できる
- 要因を分析する際に先入観の影響を抑制できる

STAMP/CASTの分析手順

一般的なCAST分析手順[5]を業務適用しやすい手順で実施

一般的なCAST分析手順	
CAST1	損失に関連するシステムとハザードを明らかにする
CAST2	ハザードに関連したシステムの安全制約やシステム要求を明らかにする
CAST3	ハザードを制御し安全制約を課すよう整備されている安全コントロールストラクチャーを記述する
CAST4	損失につながる近接したイベントを決定する
CAST5	損失を物理レベルで分析する
CAST6	安全コントロールストラクチャーの上位レベルに移り、如何にして、そして何故、より上位のレベルが現在のレベルにおける不適切な制御を許したかもしくは寄与したかを決定する
CAST7	損失に関与した共同作業、コミュニケーションの寄与者すべてを調査する
CAST8	損失に関連するシステムと安全コントロールストラクチャーの時間経過による動的な特性や変化、および安全コントロールストラクチャーの長期間での弱化を正確に定める
CAST9	改善勧告を出す



アイデアポイント

STPA分析の成果物と様式を合わせることで融合しやすくした

以下、STPAとCASTのサイクルにより、安全性の高いシステムへと改善した事例を紹介

[5] IPA STAMPガイドブック ～システム思考による安全分析～

HITACHI
Inspire the Next

Contents

2.1 製品開発への適用事例 “適用システムの概要”

HITACHI
Inspire the Next

コンテナ移載・カゴテナ運搬作業の自動化

人手で行っていたコンテナ移載・カゴテナ搬入/搬出をロボット・AGV作業に置換える

自動倉庫から
コンテナ出庫

作業者がコンベヤーから
カゴテナに移載

作業者がカゴテナ
を搬入

作業者がカゴテナ
を搬出

自動化導入前(人手による作業)

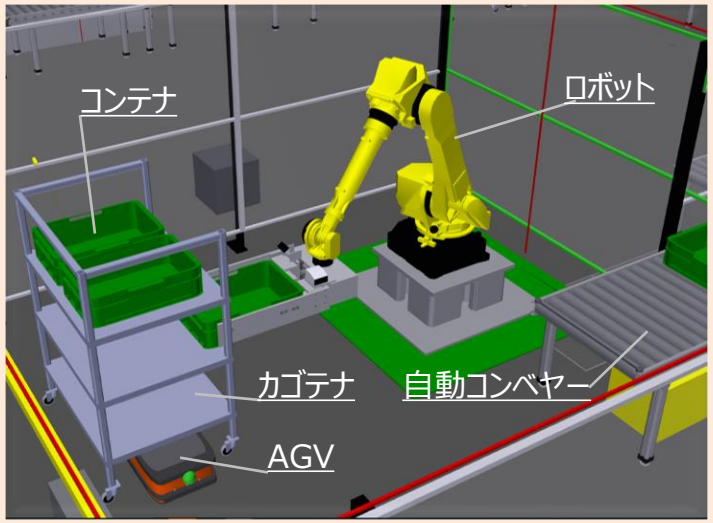
自動化

自動倉庫から
コンテナ出庫(**自動コンベヤー**)

ロボットがコンベヤーから
カゴテナに移載

AGVがカゴテナ
を搬入

AGVがカゴテナ
を搬出

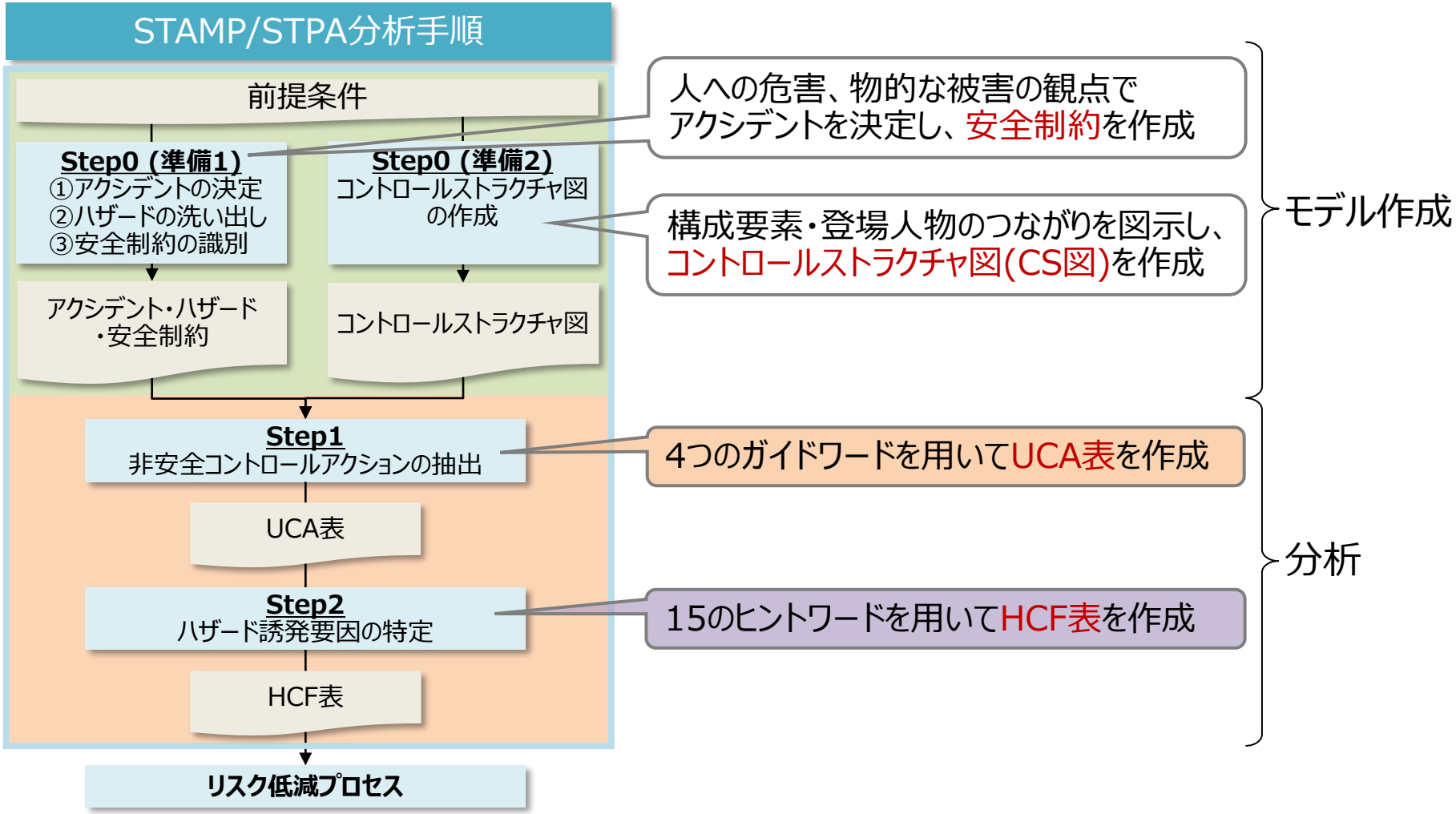


自動化導入イメージ

AGV　Automated Guided Vehicle：無人搬送車

2.2 STAMP/STPA分析手順

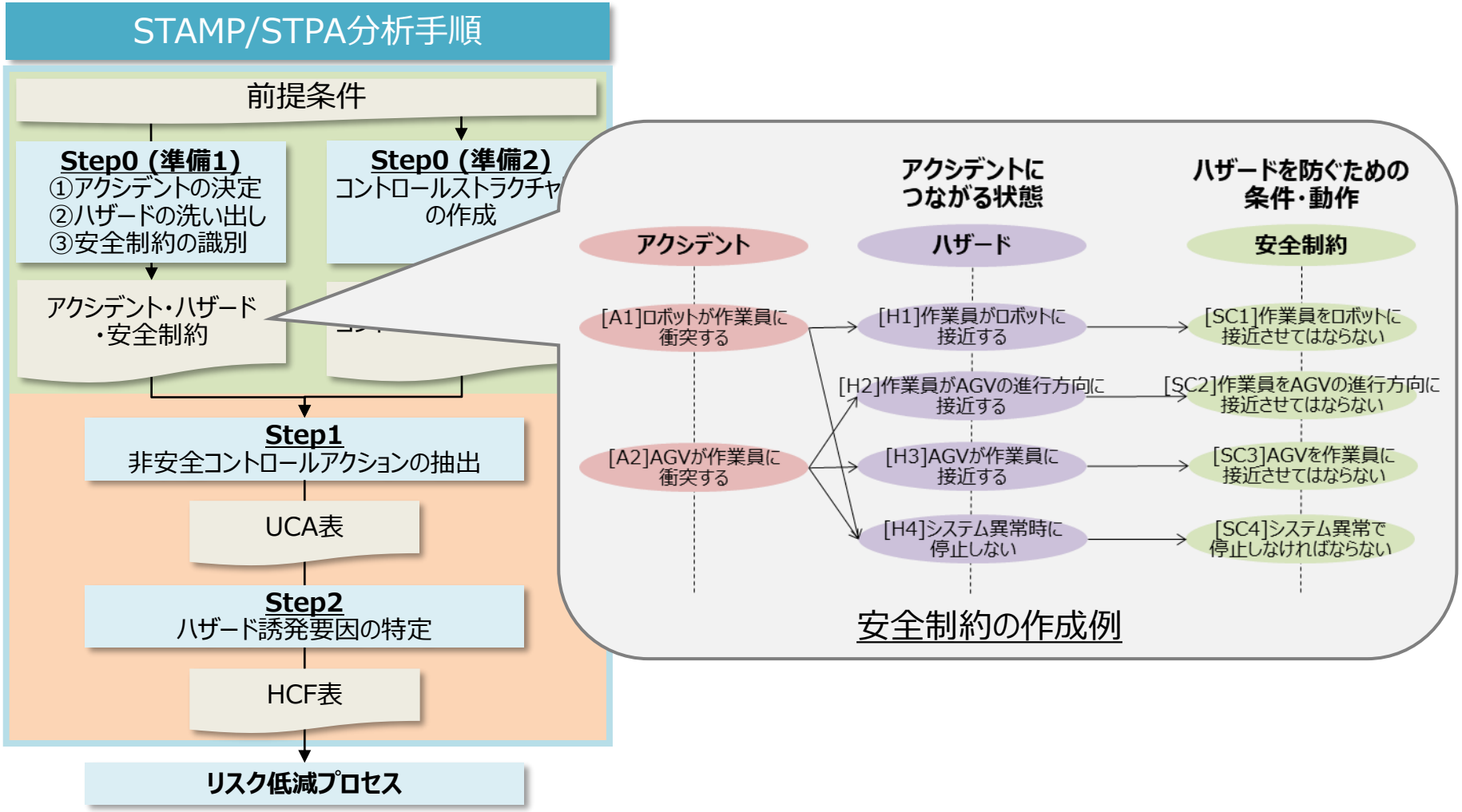
■ **モデル作成**(Step0)と**分析**(Step1,2)の大きく二つの手順を実施
■ 分析の成果物であるUCA表、HCF表をリスク低減プロセスに反映



UCA Unsafe Control Action
HCF Hazard Causal Factor

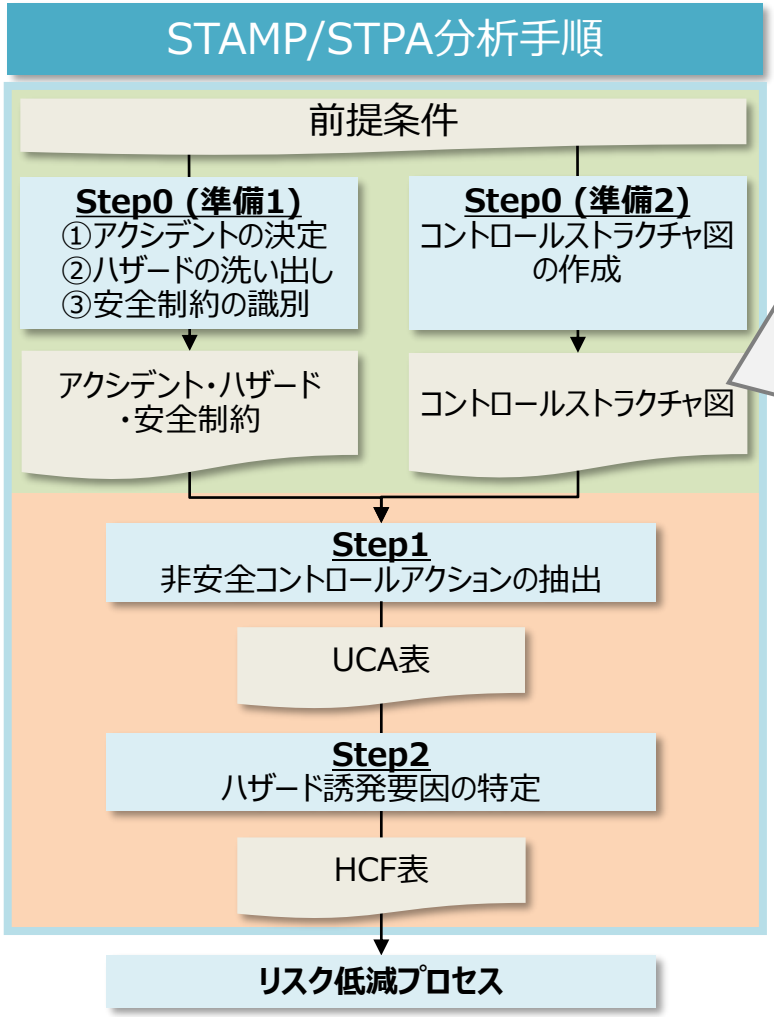
2.3 Step0(準備1) 安全制約の作成

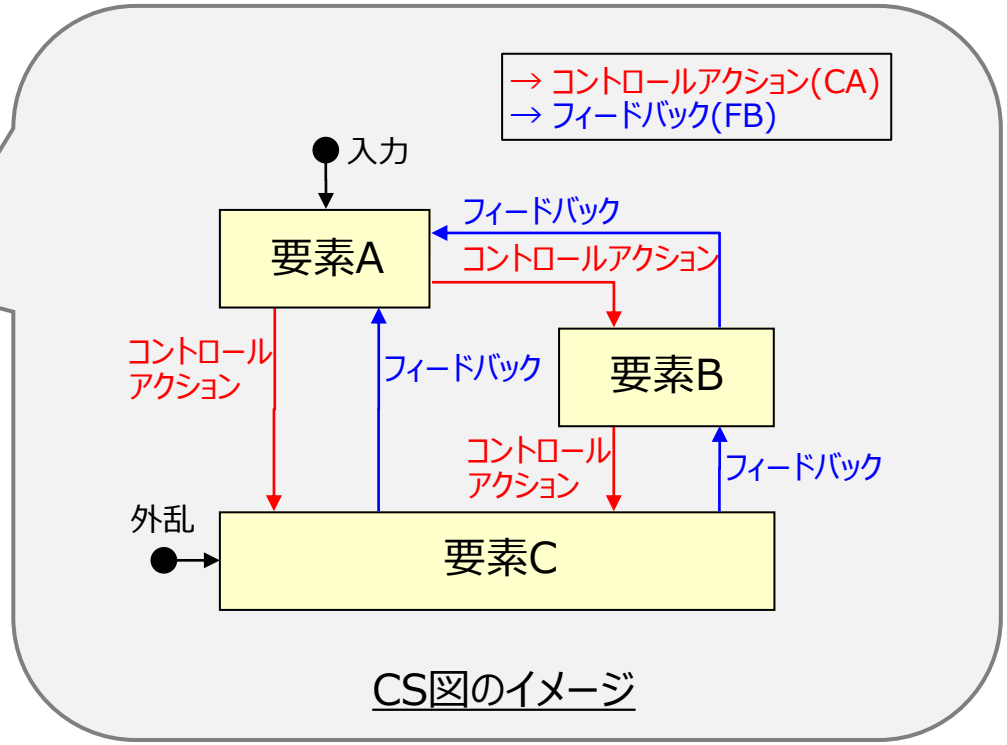
■ 人への危害、物的な被害の観点でアクシデントを決定し、安全制約を作成



2.4 Step0(準備2) CS図の作成

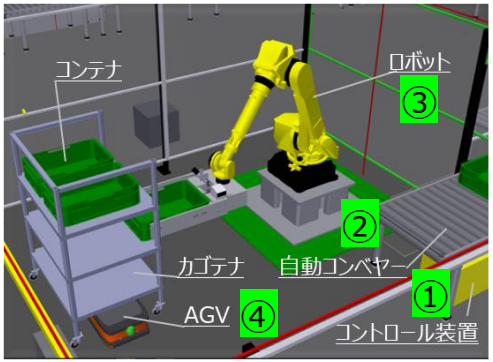
■構成要素・登場人物のつながりを明確化するために、CS図を作成



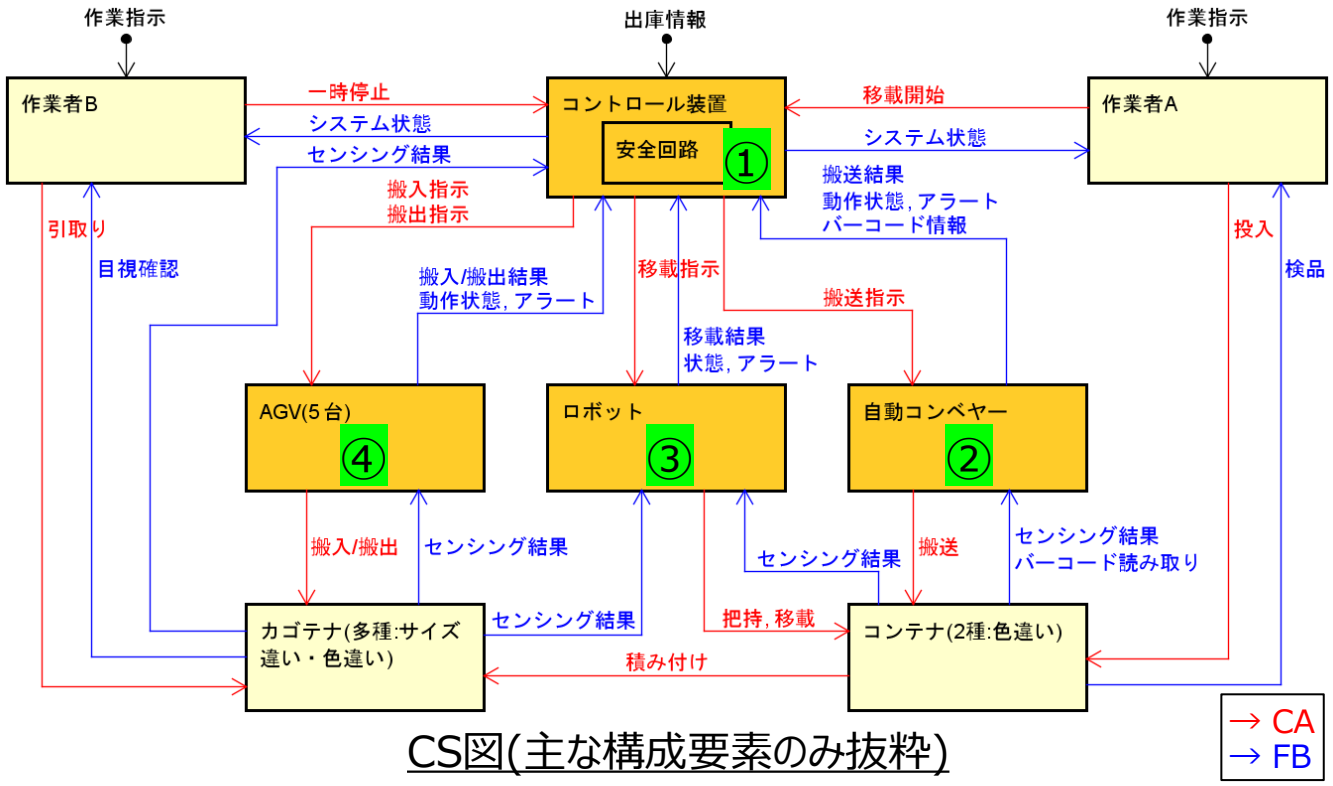


2.5 Step0(準備2) 自動化システムのCS図

■構成要素間のコントロールアクションとフィードバックに着目して作成



自動化導入イメージ



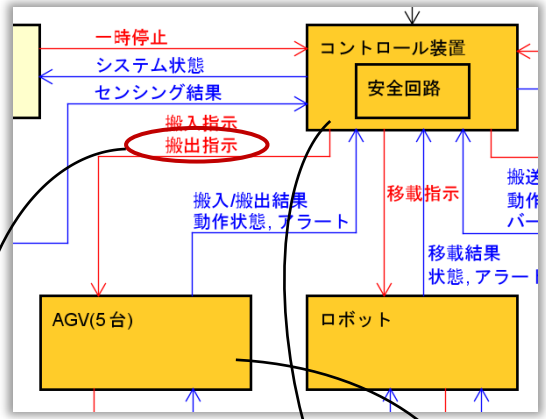
CS図(主な構成要素のみ抜粋)

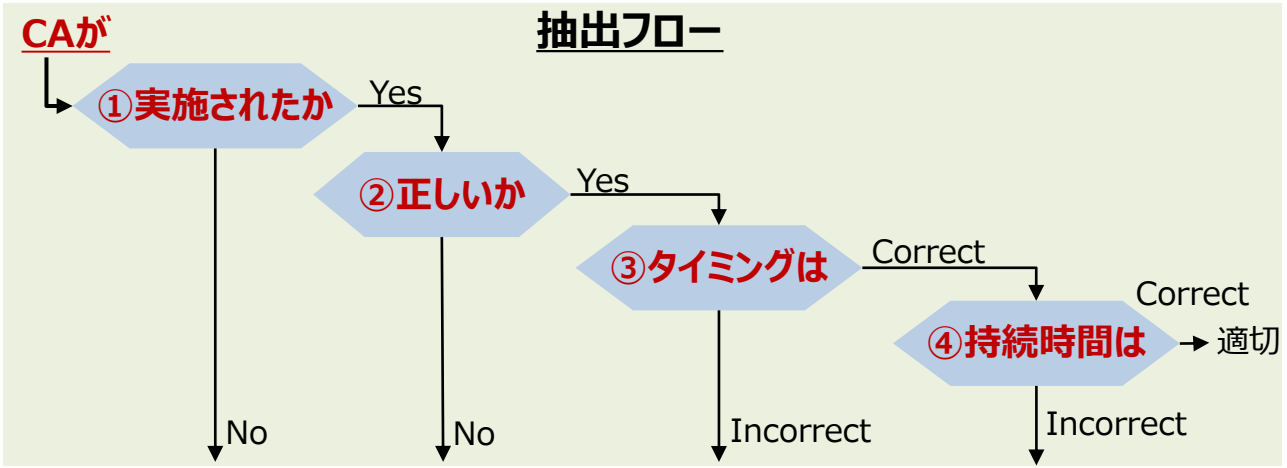
各装置の役割り

	構成機器	役割り
①	コントロール装置	ロボット-AGV-自動コンベヤー連携, UI, 他システム連携, 安全回路
②	自動コンベヤー	ロボット前までのコンテナ搬送
③	ロボット	カゴテナへのコンテナ積み付け
④	AGV	カゴテナ供給、搬送

2.6 Step1 非安全コントロールアクションの抽出

■CS図のCAに対してガイドワード①～④を用いて、安全制約に違反する非安全コントロールアクション(UCA)を抽出





UCA表の作成例

CA	コントローラー	被コントロールプロセス	(N)	(P)	(T)	(D)
搬出指示	コントロール装置	AGV	搬出指示なし	搬入前に搬出指示	(UCA1-T1) ロボット移載中に搬出指示 [SC8]*1	–
・・・						

UCAからHCF表を作成(Step2へ)

*1 紐づけられた安全制約違反の番号

2.7 Step2 ハザード誘発要因の特定

HITACHI
Inspire the Next

■UCAに対して、ヒントワード①～⑮を用いてハザード誘発要因(HCF)を洗い出し、HCF表を作成

UCA表

CA	コントローラー	被コントロールプロセス	(N)	(P)	(T)	(D)
搬出指示	コントロール装置	AGV	搬出指示なし	搬入前に搬出指示	(UCA1-T1) ロボット移載中に搬出指示 [SC8]	–

15のヒントワード(一部抜粋)

	ヒントワード
①	指示,外部情報の誤り,欠落,外乱
②	**制御アルゴリズムの欠陥(不具合,プロセス変更,不正確な修正)**
・・・	・・・
⑬	センサーの不十分な動作
⑭	**他コントローラーからの入力の誤り,欠落,衝突**
⑮	他コントローラーからの矛盾するコントロールアクション

ヒントワード②⑭より、以下のHCFが洗い出せる

HCF表の作成例

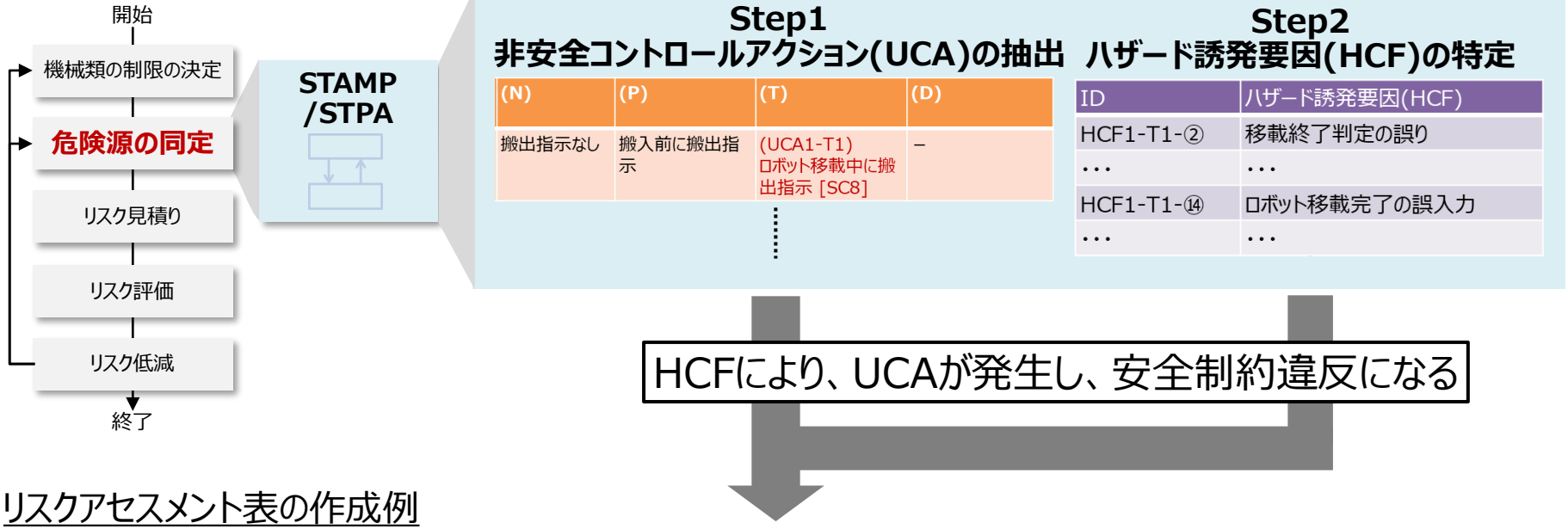
ID	ハザード誘発要因(HCF)
HCF1-T1-②	移載終了判定の誤り
・・・	・・・
HCF1-T1-⑭	ロボット移載完了の誤入力
・・・	・・・

リスク低減プロセスへ

2.8 リスク低減プロセスへの反映

STAMP/STPAの成果

成果物(UCA・HCF)をリスクアセスメント表に反映し、リスク見積り・評価とリスク低減を実施



リスクアセスメント表の作成例

No.	危険源の同定							リスク見積り			・・・
	危険源	作業区分	危険区分		危険事象	対象(●)		危害の程度	発生確率	リスクレベル	・・・
			原因	結果		人	物				
・・・	ロボット	・・・	・・・	・・・	移載終了判定の誤りにより、ロボット移載中に搬出指示が出て、ロボットアームがカゴテナに衝突する	●	●	・・・	・・・	・・・	・・・
・・・	ロボット	・・・	・・・	・・・	ロボット移載完了の誤入力により、ロボット移載中に搬出指示が出て、ロボットアームがカゴテナに衝突する	●	●	・・・	・・・	・・・	・・・

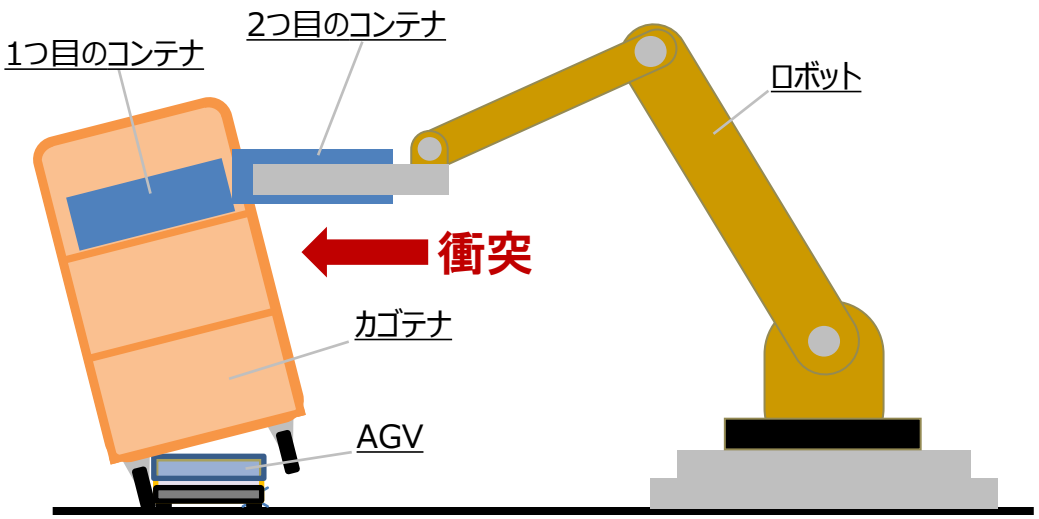
HITACHI
Inspire the Next

Contents

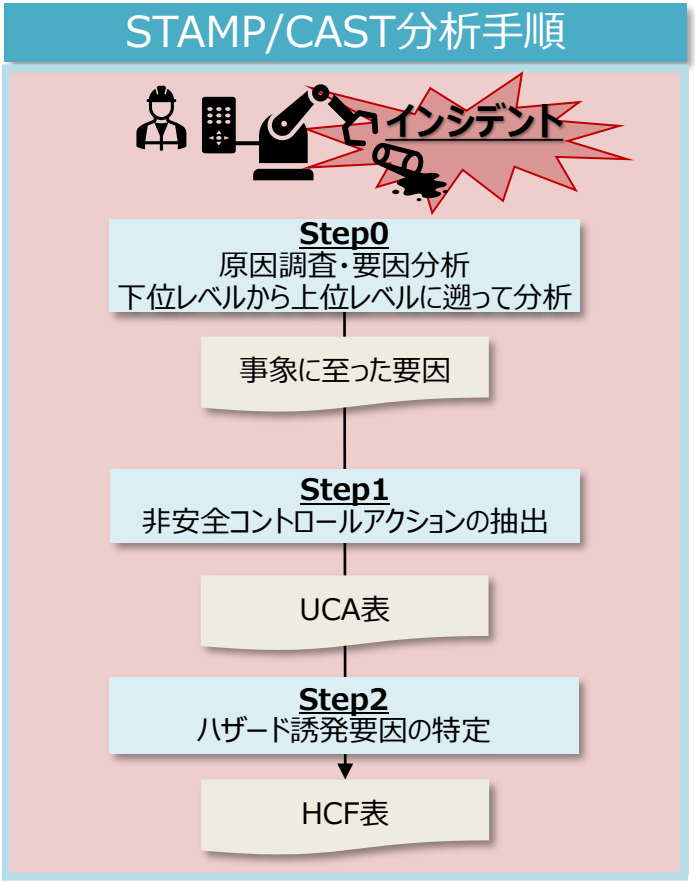
3.1 インシデント発生への適用事例

HITACHI
Inspire the Next

ロボットのコンテナ移載作業にて、既にカゴテナ内に積み付け済みコンテナがある場所に次のコンテナを積み付けようとしてコンテナ同士が衝突、カゴテナを押し倒そうとした



ロボットがカゴテナを押し倒そうとした事例

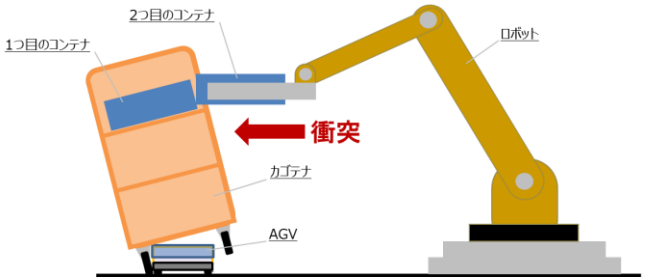


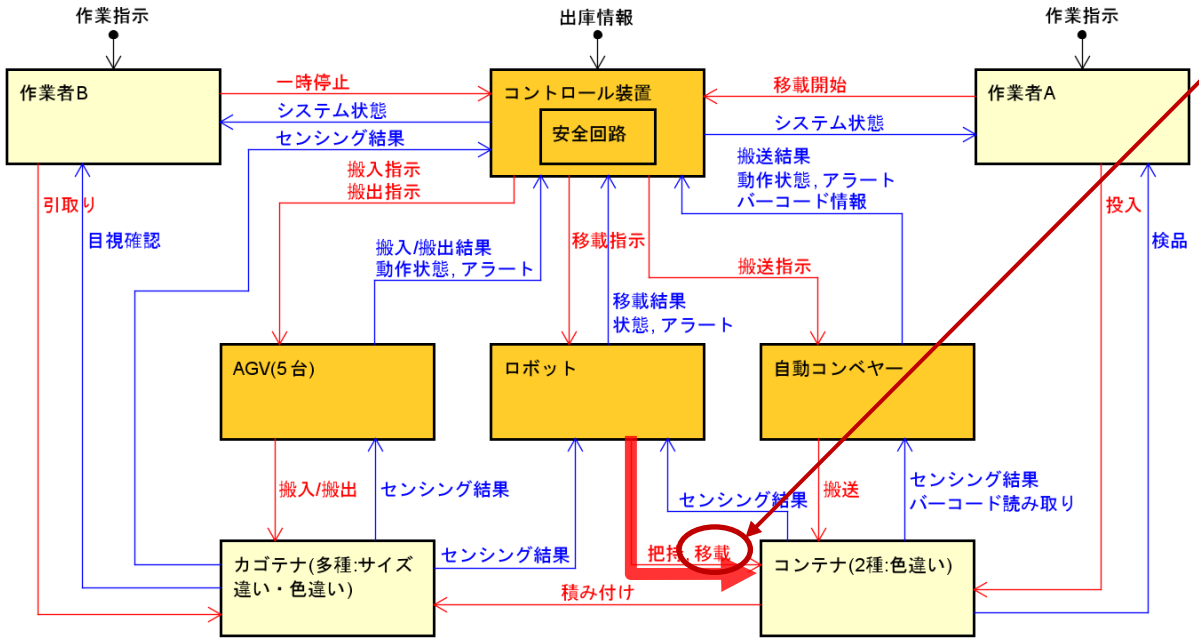
インシデントの要因分析にSTAMP/CASTを適用

3.2 Step0 原因調査・要因分析（１）

HITACHI
Inspire the Next

発生した事象からCS図の赤矢印(CA)を遡って分析を行った結果、複数の要因が重なって事象に至っていた





CS図(主な構成要素のみ抜粋)

事象発生に至った要因

【発生事象】**コンテナが既にある場所にコンテナ移載を実行**

【要因1】移載指示前に残留物検知センサーが検知せず

【要因2(直接原因)】コンテナ1個目の移載中に2個目のコンテナ到着待ちでタイムアウト発生

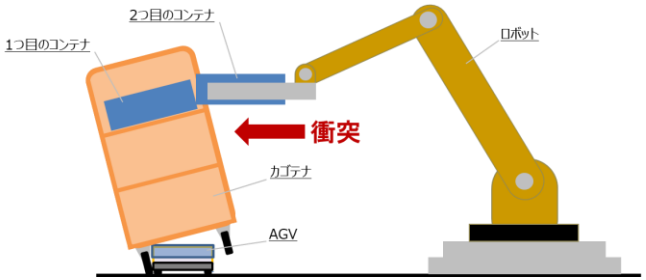
【要因3】タイムアウト発生時、コンテナ1個目の移載中であったため、移載完了数が0で作業エラー状態に遷移

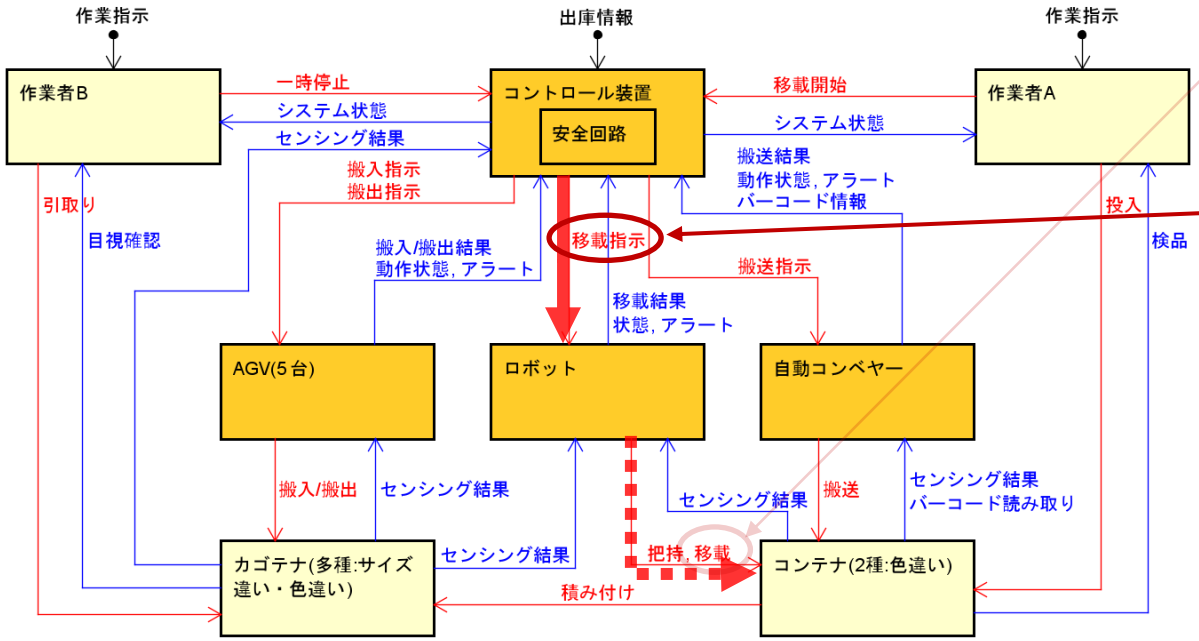
【要因4】作業者は、異常に気付かず、移載開始(復旧)ボタン押下

3.2 Step0 原因調査・要因分析（２）

HITACHI
Inspire the Next

発生した事象からCS図の赤矢印(CA)を遡って分析を行った結果、複数の要因が重なって事象に至っていた





CS図(主な構成要素のみ抜粋)

事象発生に至った要因

【発生事象】コンテナが既にある場所にコンテナ移載を実行

【要因1】移載指示前に**残留物検知センサーが検知せず**

【要因2(直接原因)】コンテナ1個目の移載中に2個目のコンテナ到着待ちでタイムアウト発生

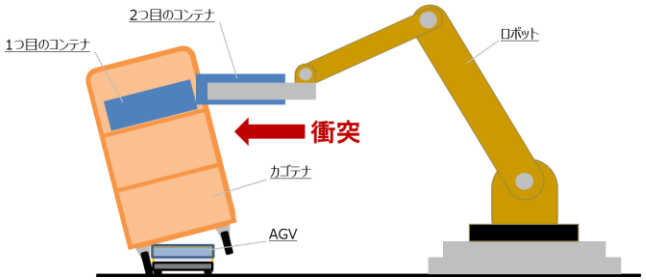
【要因3】タイムアウト発生時、コンテナ1個目の移載中であったため、移載完了数が0で作業エラー状態に遷移

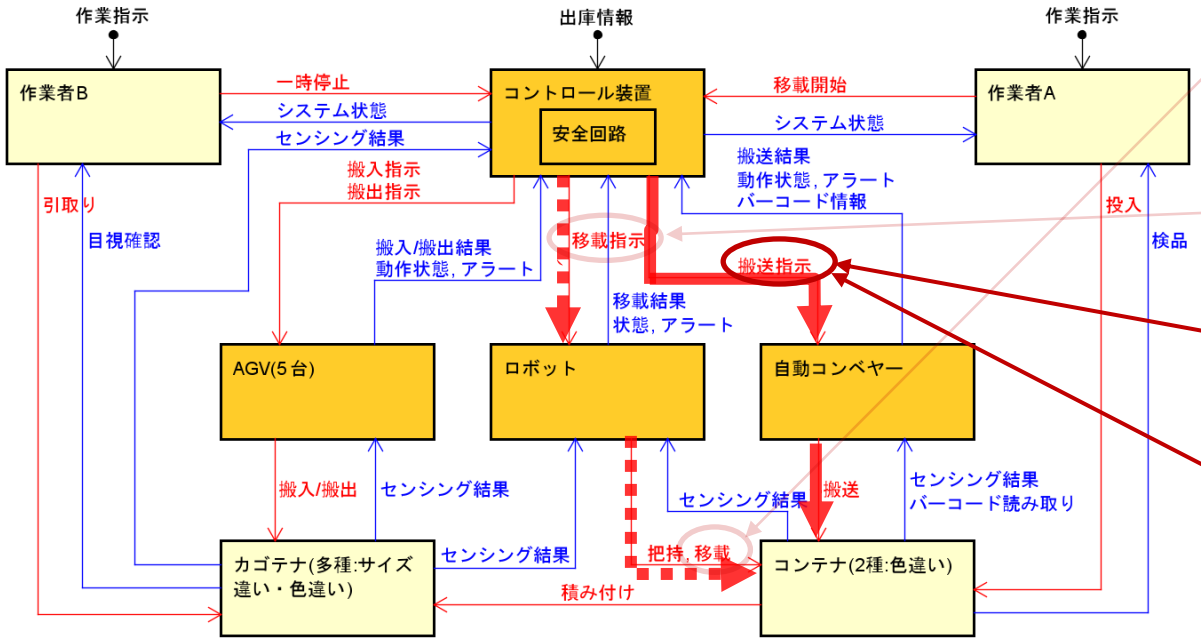
【要因4】作業者は、異常に気付かず、移載開始(復旧)ボタン押下

3.2 Step0 原因調査・要因分析（3）

HITACHI
Inspire the Next

発生した事象からCS図の赤矢印(CA)を遡って分析を行った結果、複数の要因が重なって事象に至っていた





CS図(主な構成要素のみ抜粋)

事象発生に至った要因

【発生事象】コンテナが既にある場所にコンテナ移載を実行

【要因1】移載指示前に残留物検知センサーが検知せず

【要因2(直接原因)】コンテナ1個目の移載中に2個目のコンテナ到着待ちで**タイムアウト発生**

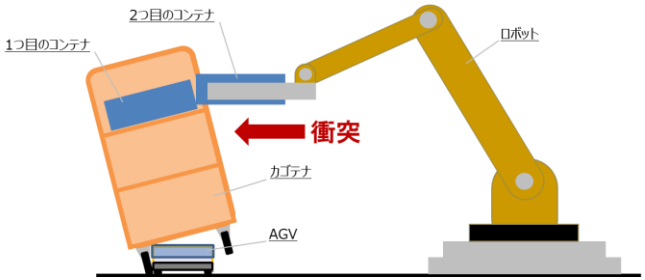
【要因3】タイムアウト発生時、コンテナ1個目の移載中であったため、**移載完了数が0で作業エラー**状態に遷移

【要因4】作業者は、異常に気付かず、移載開始(復旧)ボタン押下

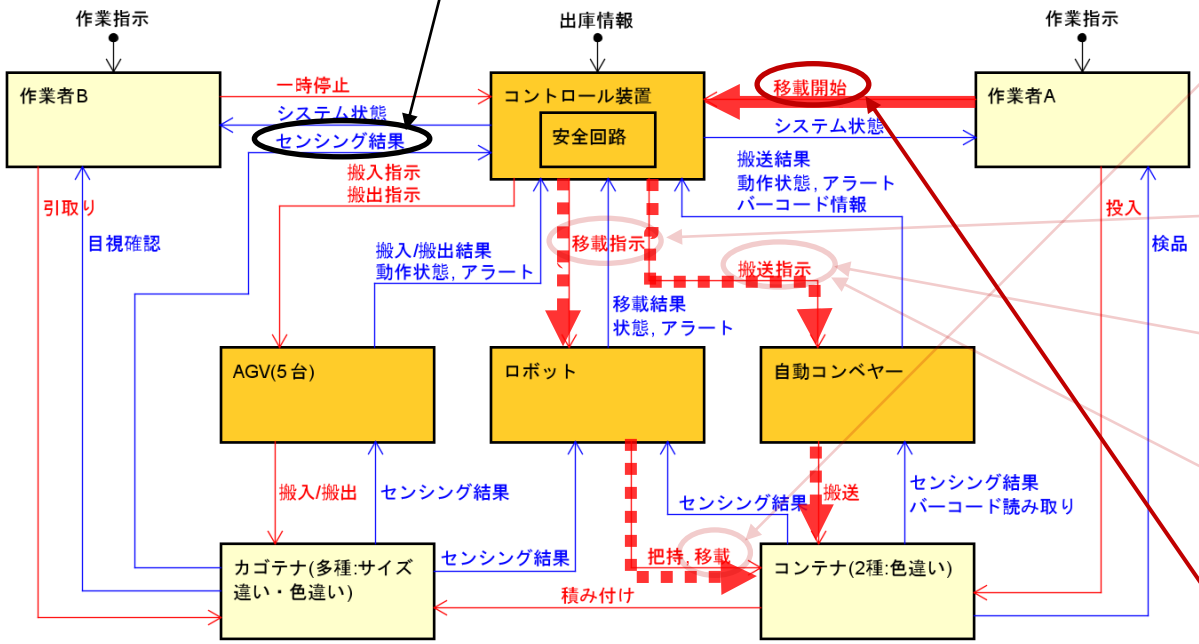
3.2 Step0 原因調査・要因分析（４）

HITACHI
Inspire the Next

発生した事象からCS図の赤矢印(CA)を遡って分析を行った結果、複数の要因が重なって事象に至っていた



最終的にカゴテナ位置ずれ検知センサーがカゴテナの傾きを検知し非常停止



CS図(主な構成要素のみ抜粋)

事象発生に至った要因

【発生事象】コンテナが既にある場所にコンテナ移載を実行

【要因1】移載指示前に残留物検知センサーが検知せず

【要因2(直接原因)】コンテナ1個目の移載中に2個目のコンテナ到着待ちでタイムアウト発生

【要因3】タイムアウト発生時、コンテナ1個目の移載中であったため、移載完了数が0で作業エラー状態に遷移

【要因4】作業者は、**異常に気付かず、移載開始(復旧)ボタン押下**

要因からUCA表を作成(Step1へ)

3.3 Step1 非安全コントロールアクションの抽出

HITACHI
Inspire the Next

原因調査・要因分析から判明した非安全コントロールアクションをUCA表に展開

UCA表

CA	コントローラー	被コントロールプロセス	(N)	(P)	(T)	(D)
移載指示	コントロール装置	カゴテナ	-	【要因1】[UCA1-P1] 移載指示前に**残留物検知センサーが検知せず**	-	-
搬送指示	コントロール装置	自動コンベヤー	-	-	【要因2(直接原因)】[UCA2-T1] コンテナ1個目の移載中に2個目のコンテナ到着待ちで**タイムアウト発生**	-
移載指示	コントロール装置	ロボット	-	【要因3】[UCA3-P1] タイムアウト発生時、コンテナ1個目の移載中であったため、**移載完了数が0で作業エラー状態**に遷移	-	-
移載開始	作業員A	コントロール装置	-	【要因4】[UCA4-P1] 作業者は復旧のため、**異常に気付かず、移載開始(復旧)ボタン押下**	-	-

▼

UCAの4項目に対し、HCF表で分析(Step２へ)

3.4 Step2 ハザード誘発要因の特定

CAST分析では、重要な観点を分析で考慮することが推奨[3]されているが、
今回、**重要な観点をヒントワードに加えることで、HCFの観点抜けを防止**

アイデアポイント

UCA表(抜粋)

CA	コントローラー	被コントロールプロセス	(N)	(P)	(T)	(D)
搬送指示	コントロール装置	自動コンベヤー	-	-	【要因2(直接原因)】[UCA2-T1] コンテナ1個目の移載中に2個目のコンテナ到着待ちで**タイムアウト発生**	-
・・・						

15+5のヒントワード(一部抜粋)

ヒントワード	
⑬	センサーの不十分な動作
・・・	・・・

アイデアポイント

ヒントワード+5
⑯コミュニケーションと調整
⑰安全情報システム ・・・前兆検出
⑱安全管理システムの設計
⑲安全文化
⑳経時変化とダイナミクス

ヒントワード⑬⑰より、以下のHCFが洗い出せる

HCF表の作成例

ID	ハザード誘発要因(HCF)
HCF1-T1-⑬	コンベヤーセンサー信号のチャタリング
・・・	・・・
HCF1-T1-⑰	過去の類似タイムアウト事象の見逃し
・・・	・・・

リスク低減プロセスへ

[3] CAST HANDBOOK 日本語版 Ver.0.1

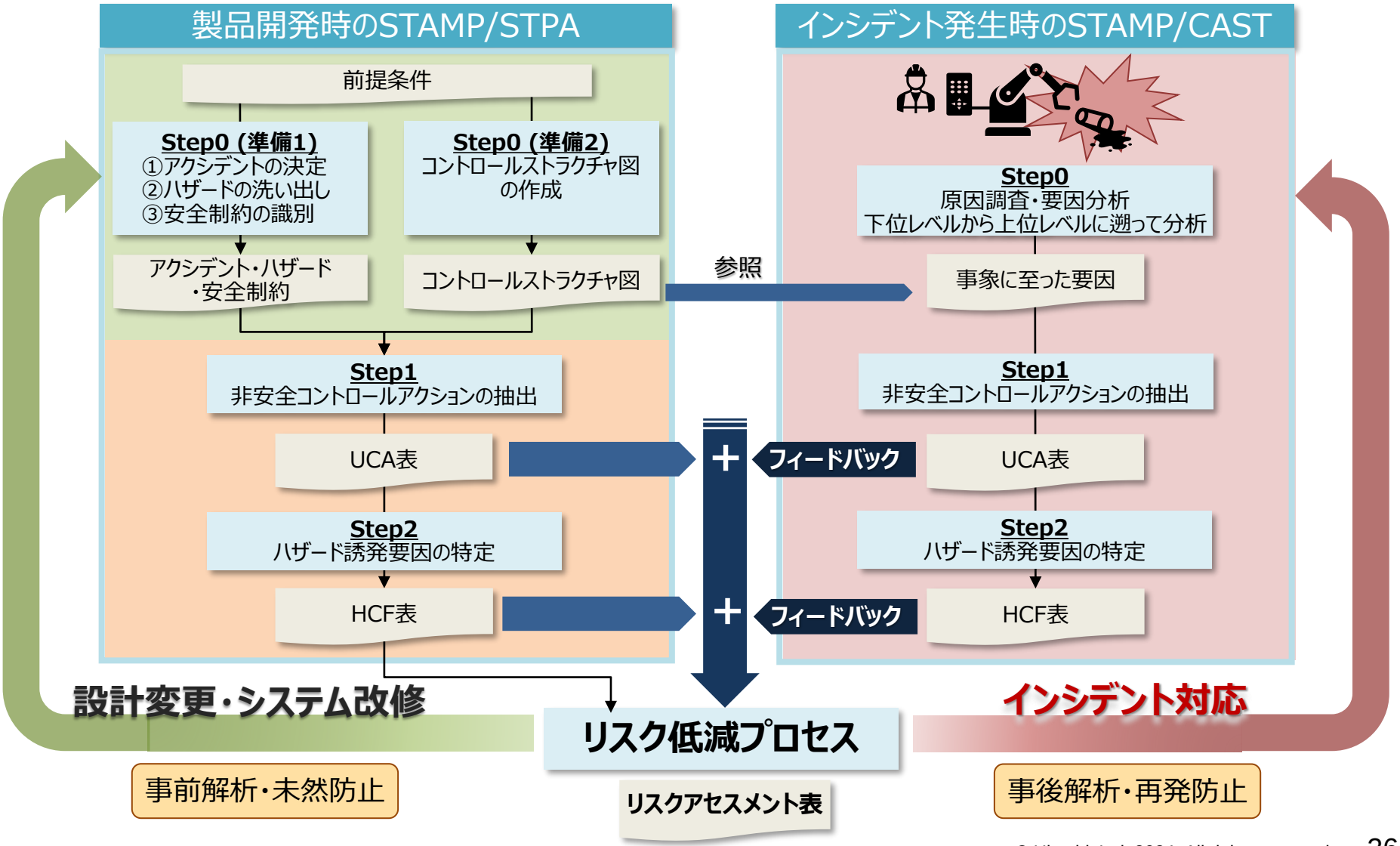
HITACHI
Inspire the Next

Contents

4.1 成果 “STPAとCASTのサイクルによるシステム改善”

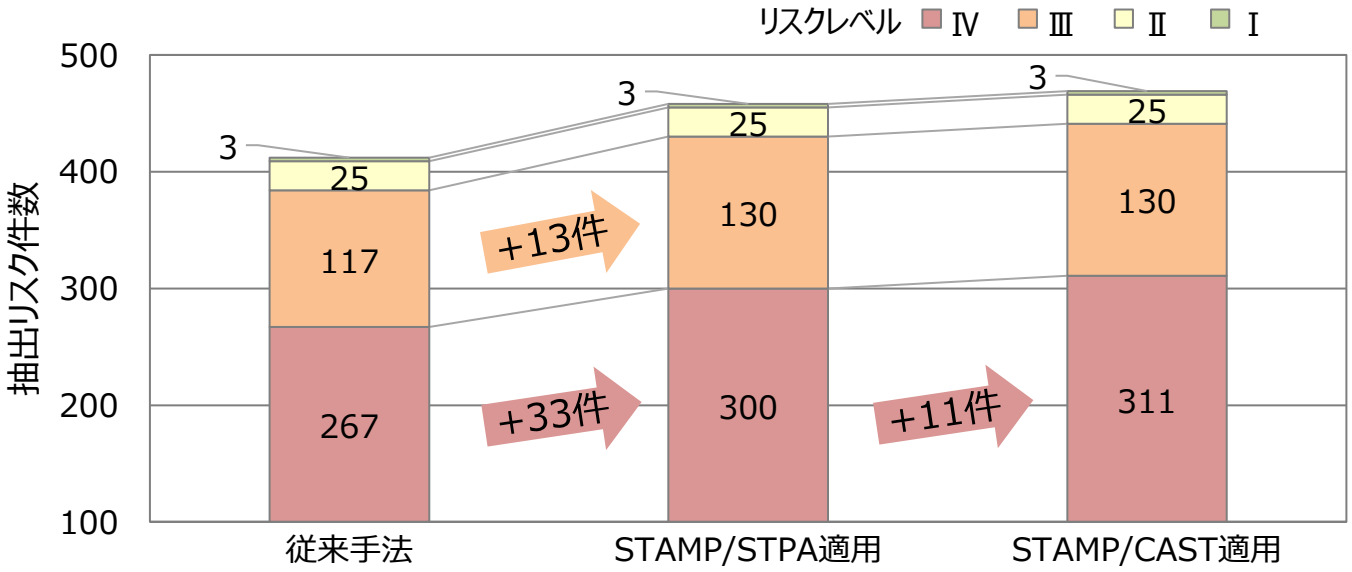
HITACHI
Inspire the Next

STAMP/STPA,CASTを適用することで、安全性の高いシステムへと効率よく改善できる



4.2 成果 “定量的評価”

- STAMP/STPA適用により、リスクレベルⅣ・Ⅲのリスクを46件追加抽出できた
- STAMP/CAST適用により、リスクレベルⅣのリスクを11件抽出できた



適用効果

リスクレベル表

危険の程度(S)		S4	S3	S2	S1
		破局的	重大	中程度	軽微
危険事象の発生確率(P)	判断規準	業務に復帰できない	どこかの時点で業務に復帰できる	同じ業務に復帰できる	業務時間が失われない
P4	ほぼ確実に発生する	Ⅳ	Ⅳ	Ⅳ	Ⅲ
P3	発生することがある	Ⅳ	Ⅳ	Ⅲ	Ⅱ
P2	発生しそうにない	Ⅲ	Ⅲ	Ⅱ	Ⅰ
P1	ゼロに近いほど発生しそうにない	Ⅱ	Ⅱ	Ⅰ	Ⅰ

Ⅳ：絶対に受け入れられない
Ⅲ：受け入れられない
Ⅱ：許容可能
Ⅰ：無視可能

5. まとめと今後の課題

HITACHI
Inspire the Next

まとめ

- ロボットシステムの安全性評価へのSTAMP/STPA活用で、より多くのハザード誘発要因を洗い出しシステムの安全性を高めることができた。
- インシデント対応へのSTAMP/CAST活用で、関連する要因の洗い出しと再発防止策が立案できた。このサイクルを繰り返すことで、安全性の高いシステムへと効率よく改善することができると考える。

今後の課題

- STAMPは使いこなしにある程度の知見が必要であるため、本事例で得られた知見を元に社内向けのSTAMP利用ガイドを作成し、適用事例の拡大とノウハウ蓄積に務める。
- 作業効率を向上させるためにツールなどを充実させ、STAMPの利用を促進する。


Hitachi Social Innovation is
POWERING GOOD