第3回 STAMPワークショップ

UNISYS

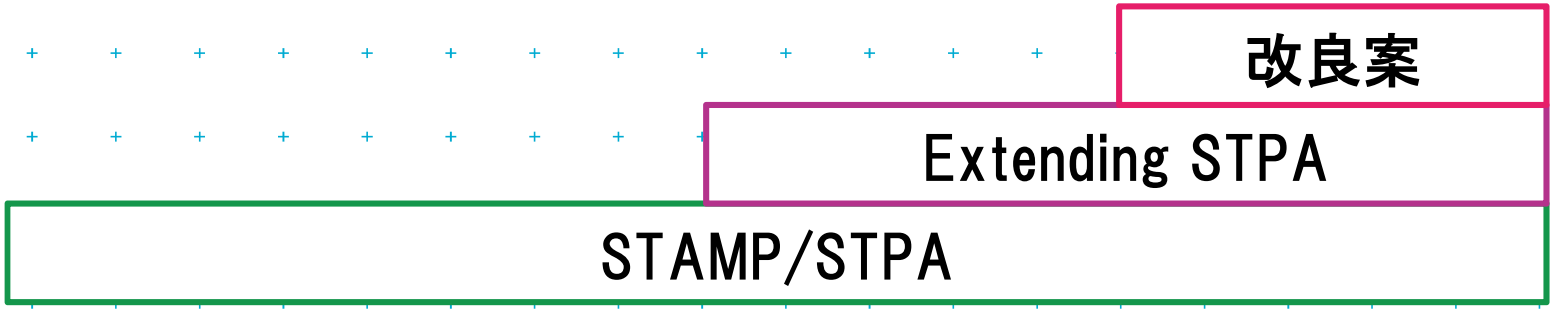
Extending STPAをベースとしたプロセスモデル抽出の実践

2018年 12月
日本ユニシス株式会社
総合技術研究所
福島 祐子

アジェンダ

1. STAMP/STPA適用上の課題
2. Extending STPAの概要
3. Extending STPAの改良案
4. 実システムに対する改良案の適用
5. まとめ

昨年お話した内容



1 STAMP/STPA適用上の課題

2 Extending STPAの概要

3 Extending STPAの改良案

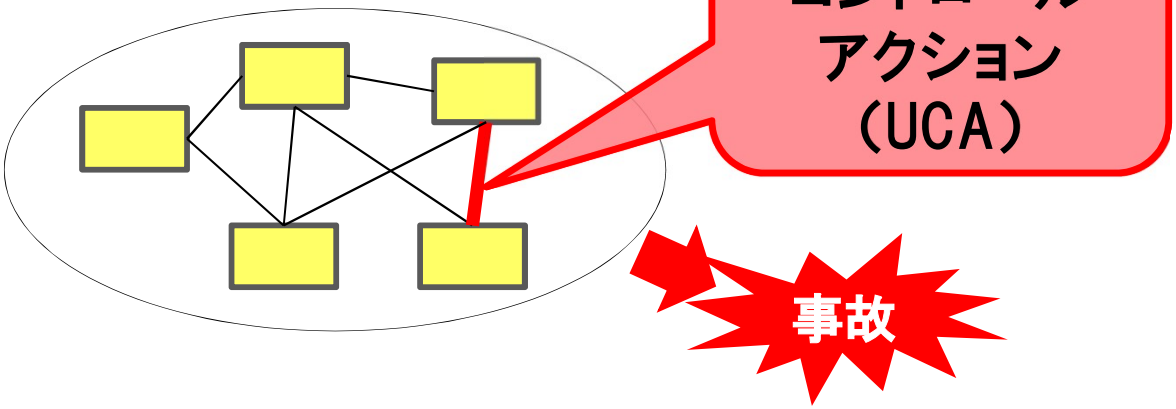
4 実システムに対する改良案の適用

5 まとめ

STAMP/STPAの特徴

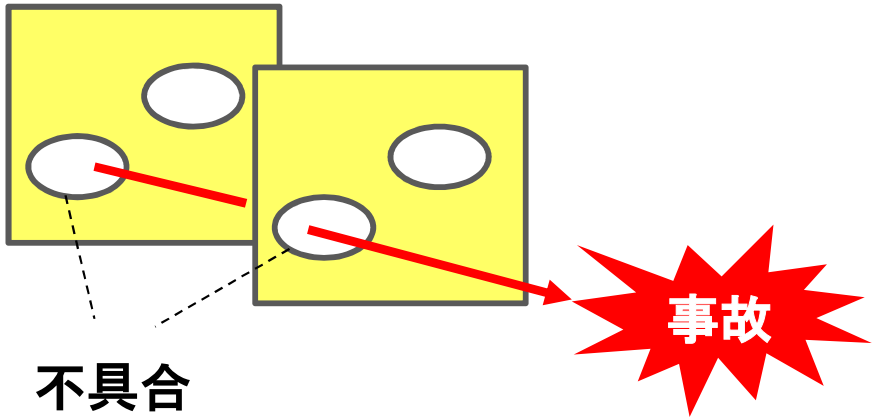
- 多くの構成要素がつながるシステムにも対応

STAMP/STPAによる考え方



(Leveson, 2012)

従来の考え方(FTA、FMEA等)

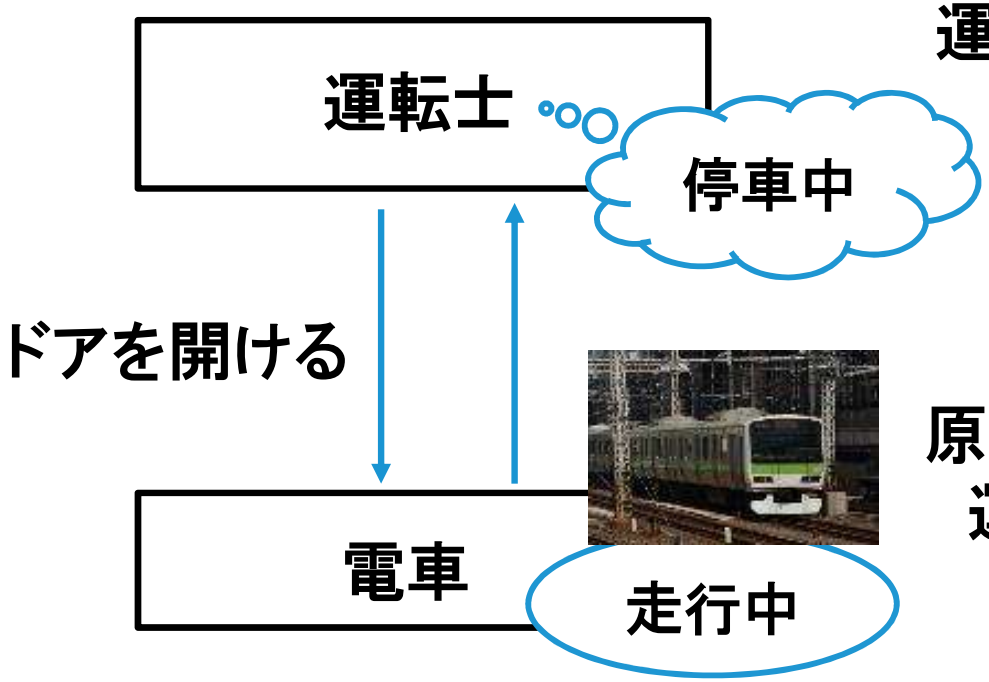


安全ではない
コントロールアクション(UCA)を
実行してはならない！

STAMP/STPAの特徴

■ 安全ではないコントロールアクション(UCA)

＜電車の例＞



UCA:
運転士が電車が走行中にドアを開ける

ハザード:
電車がドアを開けたまま走行する

➡ 事故

原因:
運転士が「電車が停車中」と認識

プロセスモデル

システムの状態とプロセスモデルとの不一致が原因。
原因の特定には、プロセスモデルを捉えることが重要！

STAMP/STPAの課題

STAMP/STPAの分析ステップ

Step0 準備 1:事故、ハザード、安全制約の識別

Step0 準備 2:コントロールストラクチャーの構築

Step1:安全ではないコントロールアクション(UCA)の識別

Step2:UCAの原因の特定

原因を特定する前にプロセスモデルが必要

(Leveson, 2012)

STAMP/STPA適用上の課題:

プロセスモデル抽出の考え方が具体的に示されていない

1 STAMP/STPA適用上の課題

2 Extending STPAの概要

3 Extending STPAの改良案

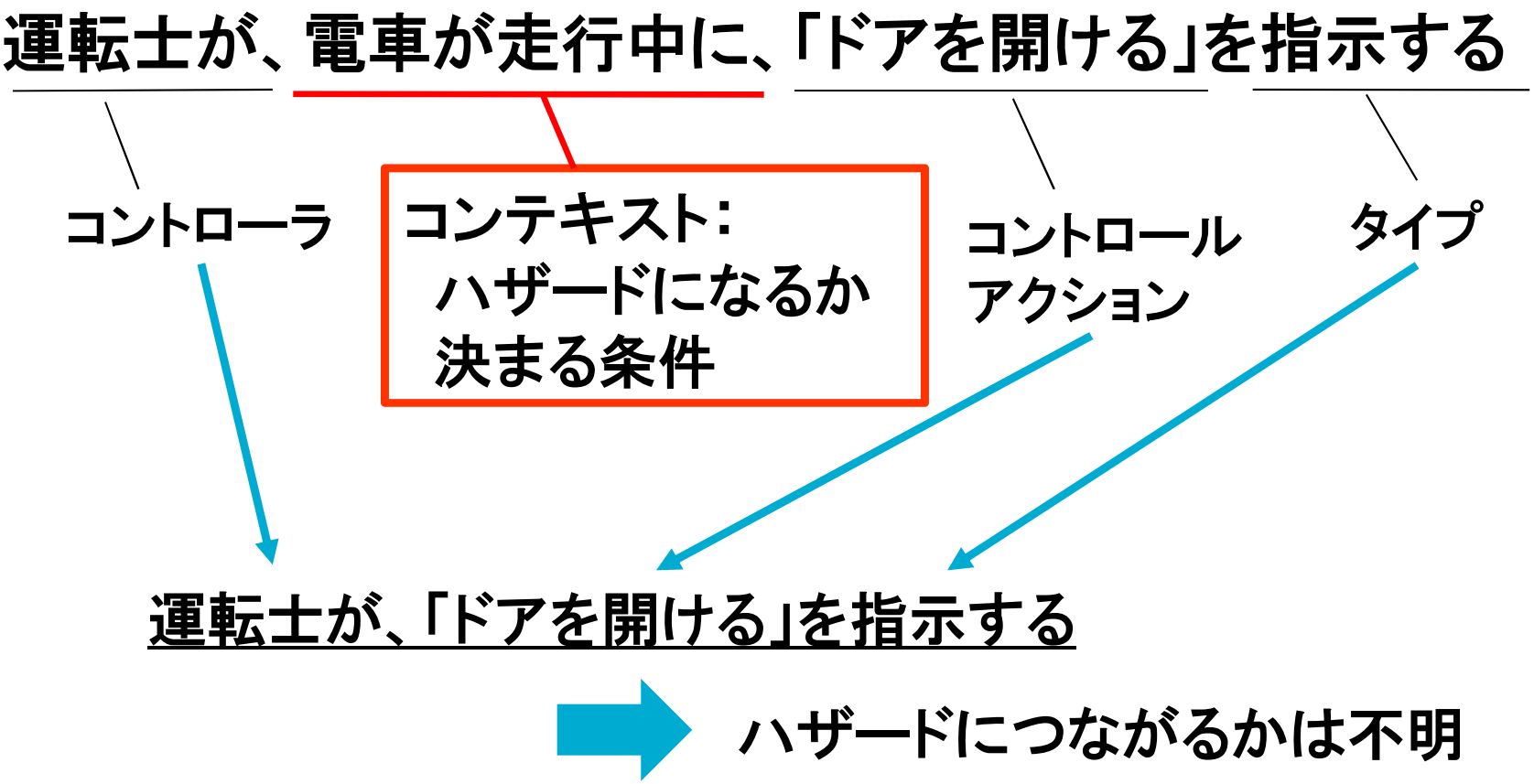
4 実システムに対する改良案の適用

5 まとめ

Extending STPAの概要

UCAの構造を定義

＜電車のUCA例＞

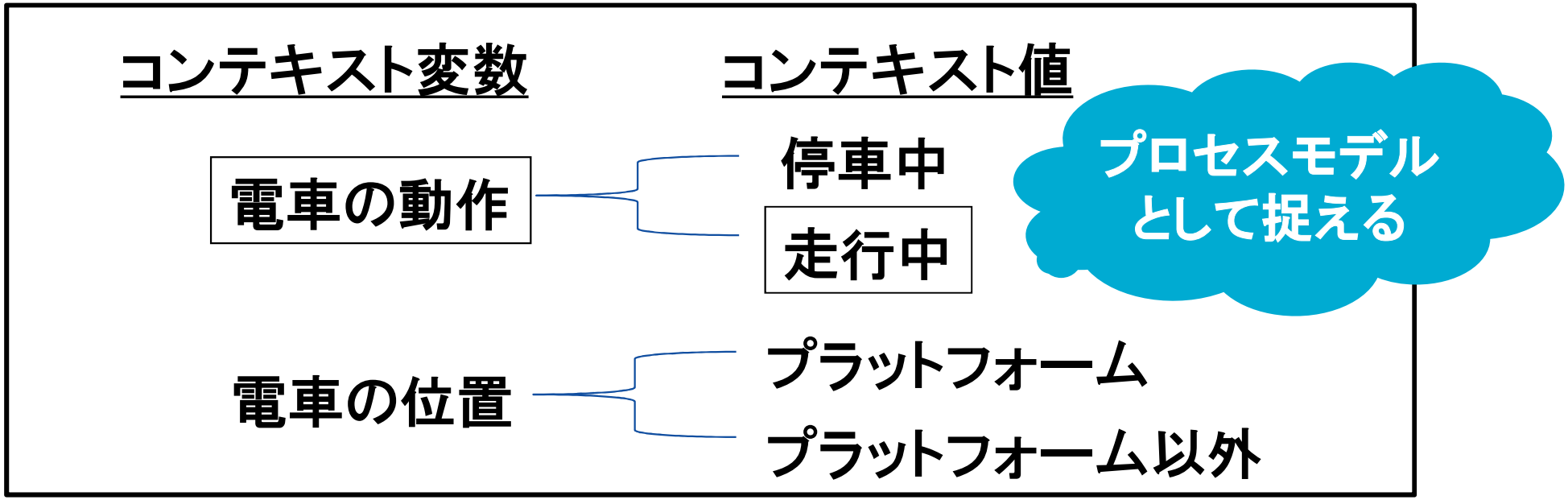


(Thomas, 2013)

Extending STPAの概要

■ 最初のコンテキストを分解して、追加のガイダンスを得る

コンテキスト「電車の走行中」の分解例：　(Thomas, 2013)



運転士が「ドアを開ける」

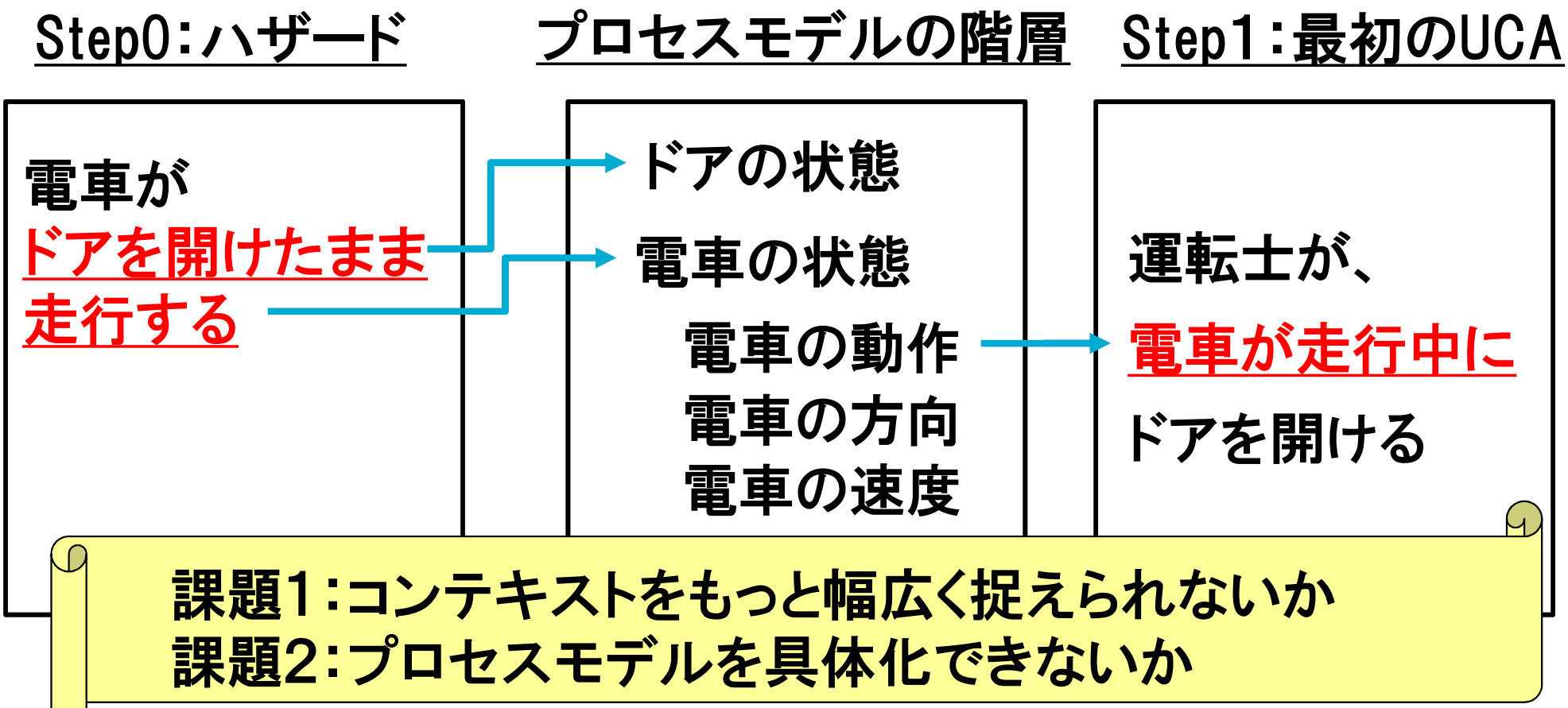
コンテキスト
の組み合わせ

電車の動作	電車の位置	ハザード？
停車中	プラットフォーム	No
停車中	プラットフォーム以外	Yes

Extending STPAの概要

- 最初のUCAのコンテキストをどのように特定するか
  - ハザードからプロセスモデルを得る
  - プロセスモデルを階層化する

コントロールアクション：
「ドアを開ける」



1 STAMP/STPA適用上の課題

2 Extending STPAの概要と試行

3 Extending STPAの改良案

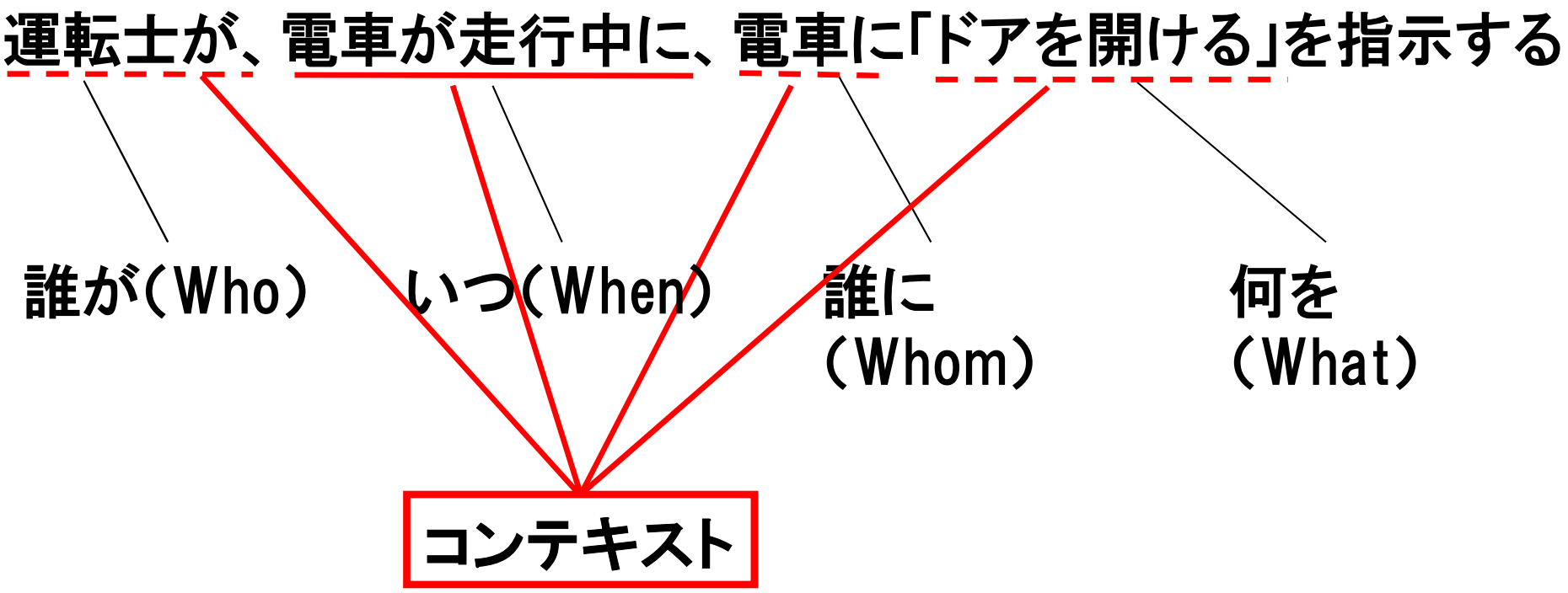
4 実システムに対する改良案の適用

5 まとめ

改良案1：6W3Hの視点によるコンテキストの導出

- UCAの構造を6W3Hで捉える

＜電車のUCA例＞



改良案1：6W3Hの視点によるコンテキストの導出

コントロールアクション：「ドアを開ける」

6W3Hの視点	ヒントワード	コンテキスト
誰が(Who)	間違った人	ー
誰に(Whom)	間違った相手	ー
何を(What)	間違ったもの・こと	間違ったドア
いつ(When)	間違ったとき	走行中
どこで(Where)	間違った場所	プラットフォーム以外
どのくらい (How many)	間違った量・程度	全開
いくら(How much)	間違った金額	ー
どのように(How)	間違った方法	間違った操作で

※「なぜ(Why)」はStep2で考えるため除く。

改良案1：6W3Hの視点によるコンテキストの導出

- コンテキスト分解(Extending STPA)

「間違ったドア」

コンテキスト変数	コンテキスト値
開けるドアの位置	プラットフォームに面している プラットフォームに面していない

- 新たなUCA：

運転士が、電車に「プラットフォームに面していないドアを開ける」を指示する

改良案2：Step2におけるコンテキストの詳細化

コンテキストの詳細化

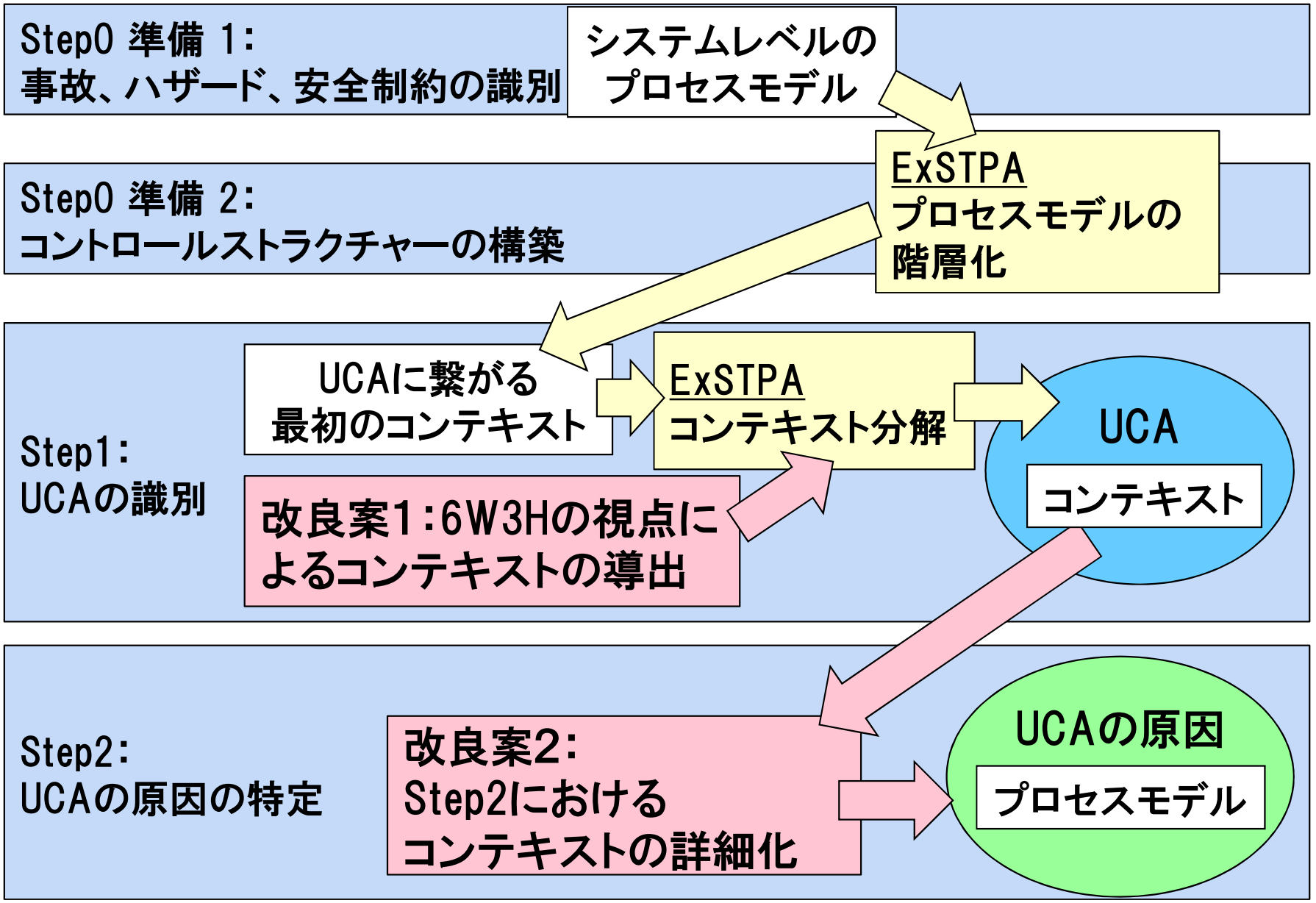
開けるドアの位置
- プラットフォームに対するドアの方向
  （プラットフォーム側、プラットフォームと反対側）
  - 電車に対するプラットフォームの方向 （右、左）

UCA：
運転士が、電車に「プラットフォームに面していないドアを開ける」を指示する

◆ UCAの原因：

運転士は、プラットフォームの方向を誤って認識する
（実際には左側なのに、右側と認識する）

プロセスモデル抽出方法



1 STAMP/STPA適用上の課題

2 Extending STPAの概要と試行

3 Extending STPAの改良案

4 実システムに対する改良案の適用

5 まとめ

改良案適用の概要

- STPA分析ワークショップ(A、B)を開催
  - ワークショップ時間:約10時間(2，3回に分けて実施)
  - 実システムに対して改良案を適用
- ワークショップ進め方

  ①STPA (Extending STPAを含む)の概要説明

  ②STPA (Extending STPAを含む)による分析

  ③改良案の説明

  ④改良案による分析
- 改良案の効果の測定
  - ②STPAによる分析結果と④改良案による分析結果の比較
  - 追加されたUCAの数、具体化されたHCFの数

ワークショップAの概要

概要

企業：検査用機器の部品メーカー

対象システム：検査用機器の部品

参加者：2名（部品の開発担当者、STPA未経験）

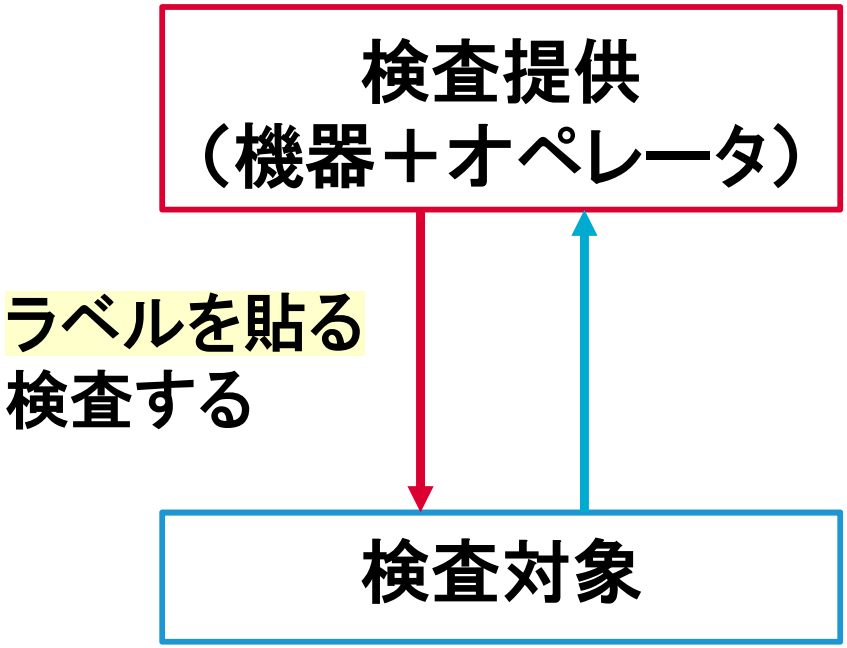
分析概要

事故：

検査対象がダメージを受ける

ハザード：

間違った検査を行う



ワークショップAにおける比較結果

■ UCA識別結果

対象CA：ラベルを貼る

＜STPA＞

識別できたUCA：1個

例）UCA：誤った検査対象にラベルを貼る

＜改良案1：6W3Hの視点の適用＞

追加されたUCAの数 ：10個

例）

6W3Hの視点	ヒントワード	コンテキスト
何を（What）	間違ったもの	誤った内容のラベル 判別できないラベル
どこで（Where）	間違った場所	間違った場所

追加UCA ： 判別できないラベルを貼る

ワークショップAにおける比較結果

対象UCA：
判別できないラベルを貼る

■ HCF識別結果

＜STPA＞

識別できたHCF ： 3個

（例）HCF：ラベルが判別できないことに気が付かない

＜改良案2:コンテキストの詳細化＞

具体的なHCF ： 15個

（例）判別できない ― 印字が薄い
　　　　　　　　　 ― 汚れている　　など5個のコンテキスト

具体化HCF1 ： 印字が薄いことに気が付かない
具体化HCF2 ： 汚れていることに気が付かない

3個のHCFに対して新たなコンテキストを反映

ワークショップBの概要

- 概要

  企業：業務用機器の部品メーカー

  対象システム：業務用機器の部品

  参加者：2名（部品の開発担当者、STPA未経験）

- 比較結果
  - UCA識別（1CAを対象）
    - STPAによるUCA数：10
    - 改良案1により追加できたUCA数：9
  - HCF識別（1UCAを対象）
    - STPAによるHCF数：9
    - 改良案2により具体化できたHCF数：14

分析結果詳細(ご参考)

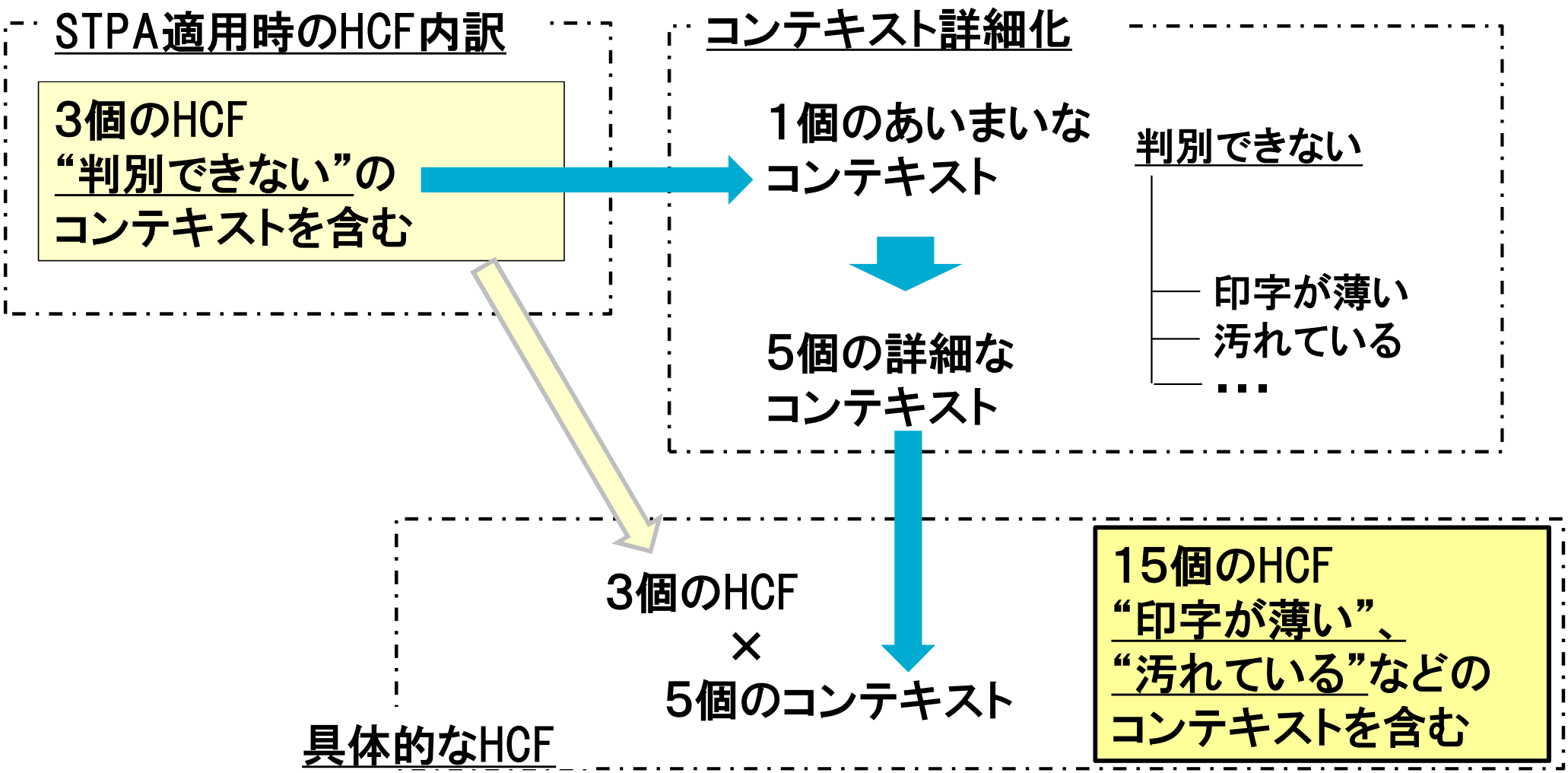
■ 改良案1:6W3Hの視点により見つけたコンテキスト数

6W3Hの視点	ヒントワード	ワークショップA	ワークショップB
誰が(Who)	間違った人		
誰に(Whom)	間違った相手		
何を(What)	間違ったもの・こと	4	
いつ(When)	間違ったとき	2	5
どこで(Where)	間違った場所	2	3
どのくらい(How many)	間違った量・程度	1	
いくら(How much)	間違った金額		
どのように(How)	間違った方法	1	1

分析結果詳細(ご参考)

■ 改良案2:コンテキスト詳細化と具体的なHCFの特定

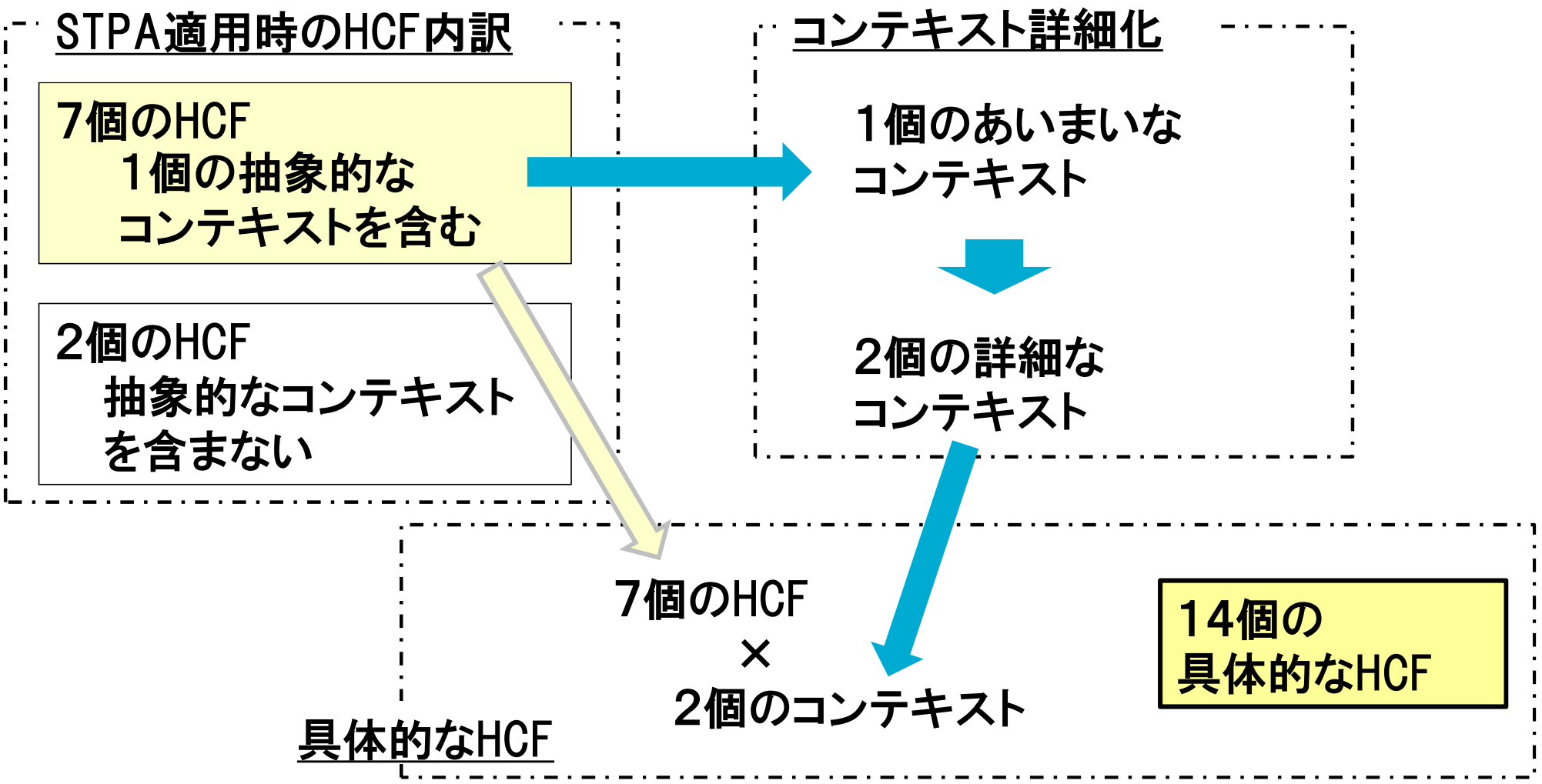
＜ワークショップA＞



分析結果詳細(ご参考)

■ 改良案2:コンテキスト詳細化と具体的なHCFの特定

＜ワークショップB＞



比較結果による考察

- 改良案1（6W3Hの視点によるUCA識別）
  - 具体的な利用シーンを考えるきっかけとなり、特にSTPAビギナーの発想を促すのに有効。視点の見落としの再考にも適用できる。
  - 対象システム、対象UCAの種類によって、有効となる視点が異なる。

- 改良案2（コンテキスト詳細化によるHCF特定）
  - 意識的にコンテキストの詳細化を行うことが可能となり、特にSTPAビギナーには有効。
  - コンテキストを詳細化することにより、同じコンテキストを含むすべてのHCFを具体化できる。
  - HCFを具体化することにより、原因の深堀りが可能になり、具体的な対策に結びつく可能性がある。

ワークショップA参加者の感想

- STPAについて
  - STPAのコントロールアクションに注目して分析するやり方はよいと思うが、全てを網羅しないと思う。他の手法と連携しながら適用するのがよいかもしれない。
  - ワークショップでは、部分的に分析したが、実際にSTAMPで分析しようとすると時間がかかりそうである。
  - 用語について、日本語と英語が混在して混乱した。
- 改良案について
  - 6W3Hの視点の適用は、悪くはなさそうである。
  - 6W3Hの視点については、コントローラ、コントロール対象プロセスなど、どの部分に関係するのか対応付けた方が、適用する際に分かりやすそうである。

ワークショップB参加者の感想

- STPAについて
  - UCAを識別することにより、総合テスト用の具体的なシナリオを書けそうである。
  - 損失、ハザードの定義は、部品を対象とすると難しい。どのように分析するのか工夫が必要。
  - 用語が難しい。

- 改良案について
  - 6W3Hの視点は、日本人に合っていて、非常によい。いろいろなメンバーで考えると、コンテキストを多く抽出できそうである。
  - “環境”、“背景”といったヒントワードがあると、コンテキストはもっと広がりそうである。

1 STAMP/STPA適用上の課題

2 Extending STPAの概要と試行

3 Extending STPAの改良案

4 実システムに対する改良案の適用

5 まとめ

今後の課題

- 改良案に対する改善検討
  - システム、UCAの種類別に、有効となる6W3Hの視点に違いはあるか？
  - ドメイン、システムの種類によって、6W3Hのヒントワードを変えた方がよいか？

- 対象システムが部品の場合の分析の進め方

お話した内容

- STAMP/STPA適用上の課題
- Extending STPAの概要
- Extending STPAの改良案
- 実システムに対する改良案の適用

Foresight in sight

UNISYS

ご清聴ありがとうございました

参考文献

- はじめてのSTAMP/STPA ～システム思考に基づく新しい安全性解析手法～, IPA/SEC, 2016, http://www.ipa.go.jp/files/000051829.pdf
- Nancy Leveson, An STPA Primer, http://psas.scripts.mit.edu/home/wp-content/uploads/2015/06/STPA-Primer-v1.pdf
- Nancy Leveson, Engineering a Safer World, The MIT Press, 2012
- John Thomas, Extending and Automating a Systems-Theoretic Hazard Analysis for Requirements Generation and Analysis, http://sunnyday.mit.edu/JThomas-Thesis.pdf
- 福島祐子,安全性解析手法STAMP/STPAにおけるプロセスモデル抽出方法の提案,ソフトウェア品質シンポジウム, 2017, http://www.juse.jp/sqip/library/shousai/download/index.cgi/B1-1.pdf?id=361