UNISYS

ソフトウェア品質シンポジウム2017
B1-1【経験発表】

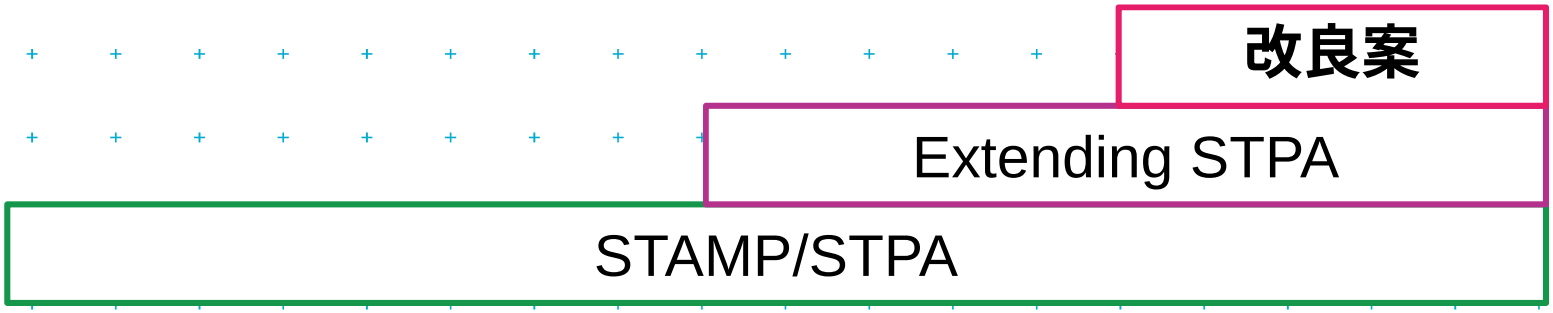
安全性解析手法STAMP/STPAにおけるプロセスモデル抽出方法の提案

2017年 9月
日本ユニシス株式会社
総合技術研究所
福島　祐子
e-mail：yuko.fukushima@unisys.co.jp

Foresight in sight

アジェンダ

1. 背景と課題ー STAMP/STPAの概要と課題
2. 課題解決策 ー Extending STPAの概要
3. 課題解決策の改良案ー Extending STPAの改良案
4. 改良案の試行と効果
5. まとめ



1 背景と課題ー STAMP/STPAの概要と課題

2 課題解決策 ー Extending STPAの概要

3 課題解決策の改良案ー Extending STPAの改良案

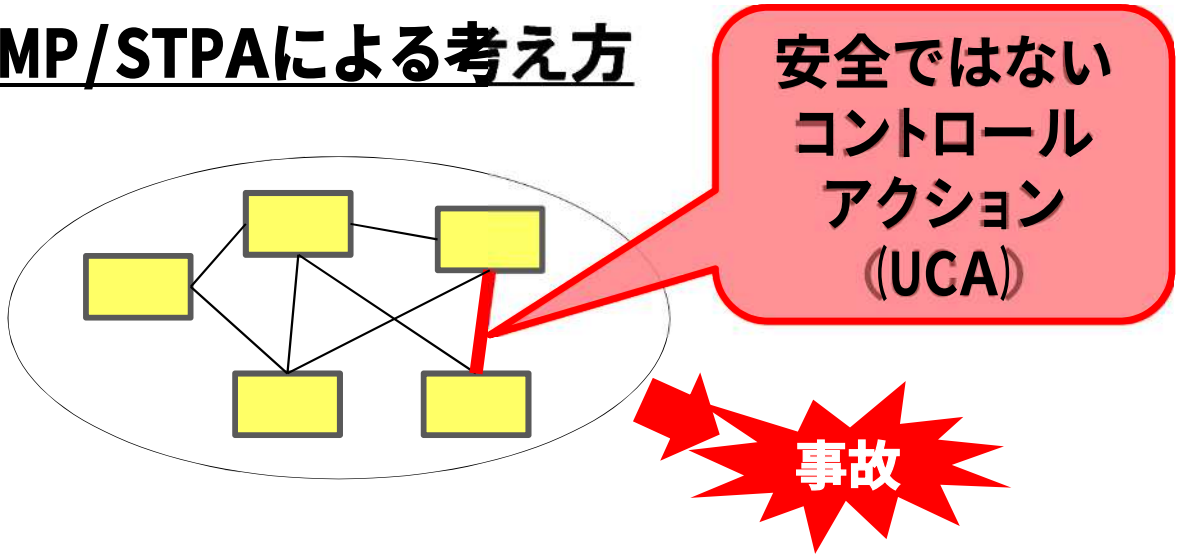
4 改良案の試行と効果

5 まとめ

STAMP/STPAの概要

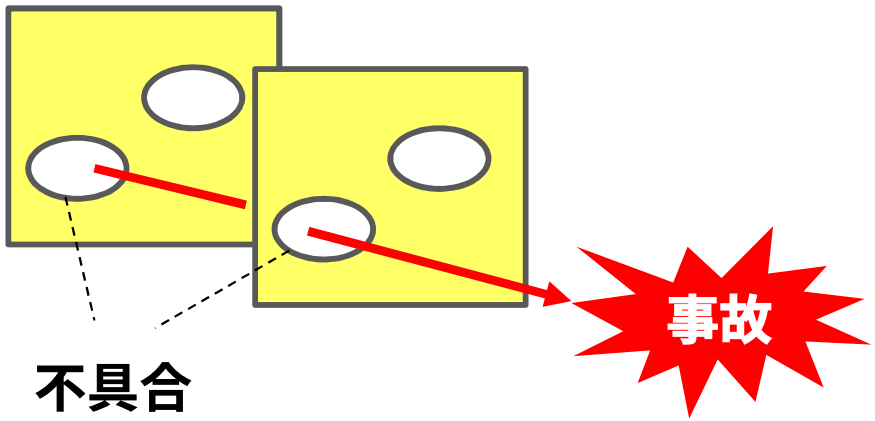
- 安全性解析（事故につながる原因を特定する）の新しい手法
- 多くの構成要素がつながるシステムにも対応

STAMP/STPAによる考え方



（Leveson, 2012）

従来の考え方（FMA、FMEA等）

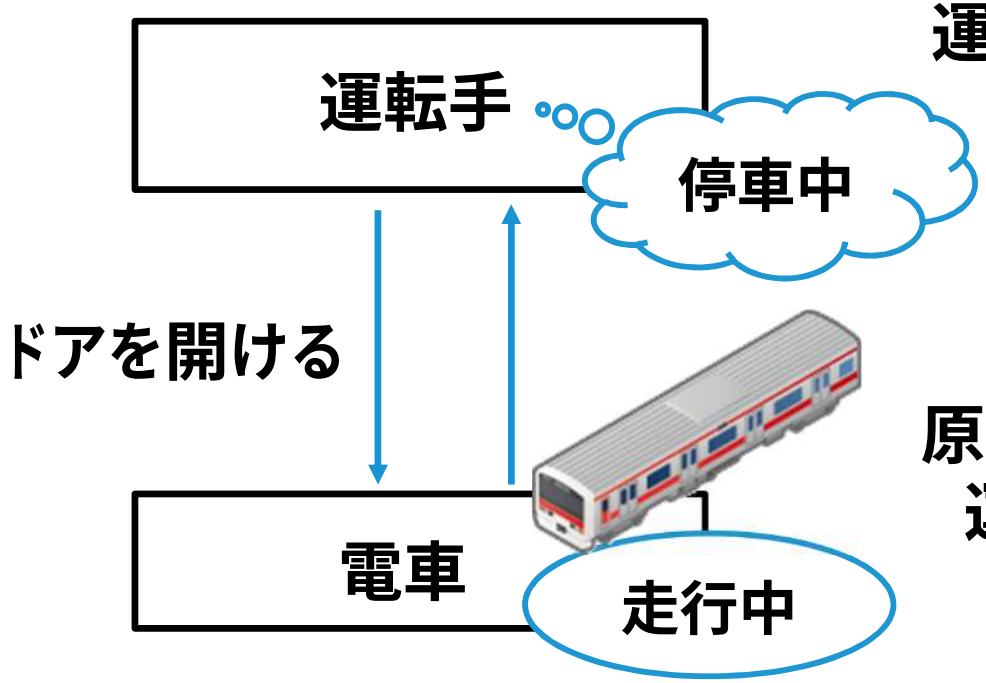


安全ではない
コントロールアクション（UCA）を
実行してはならない！

STAMP/STPAの概要

■ 安全ではないコントロールアクション（UCA）

＜電車の例＞



UCA：
運転手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：
運転手が「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の課題：

プロセスモデルを抽出する考え方が示されていない

1 背景と課題－ STAMP/STPAの概要と課題

2 課題解決策 － Extending STPAの概要

3 課題解決策の改良案－ Extending STPAの改良案

4 改良案の試行と効果

5 まとめ

Extending STPAの概要

UCAの構造を定義

＜電車のUCA例＞

運転手が、電車が走行中に、「ドアを開ける」を指示する

- 運転手が：コントローラ
- 電車が走行中に：コンテキスト：ハザードになるか決まる条件
- 「ドアを開ける」を：コントロールアクション
- 指示する：タイプ

運転手が、「ドアを開ける」を指示する

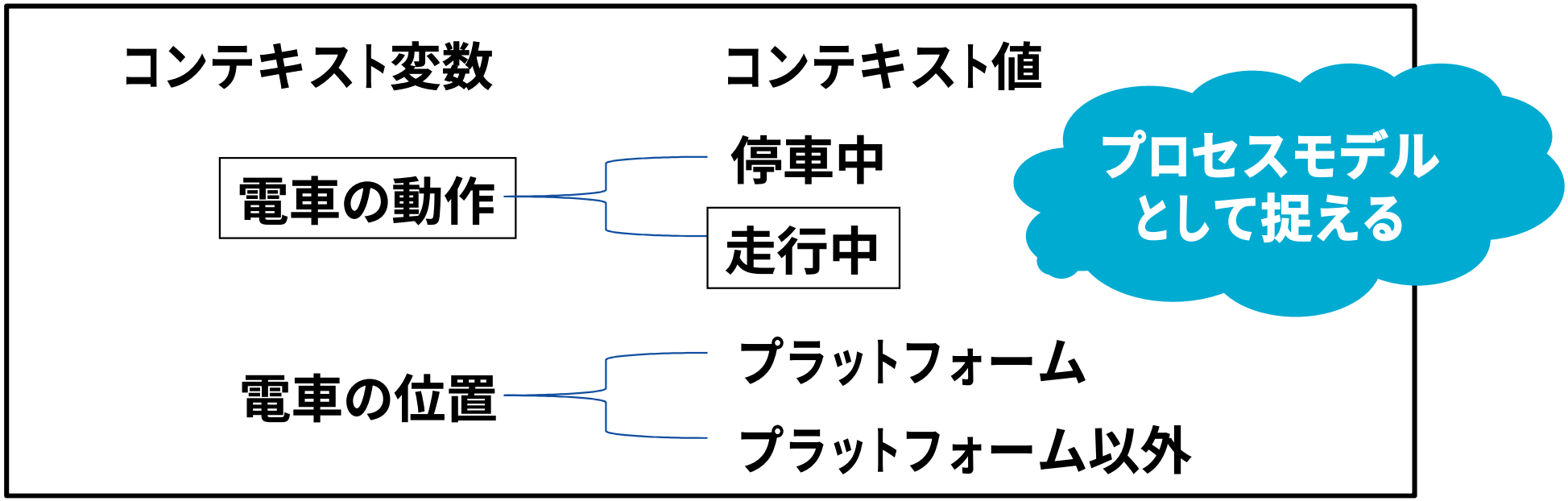
⇒ ハザードにつながるかは不明

(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)



運転手が「ドアを開ける」

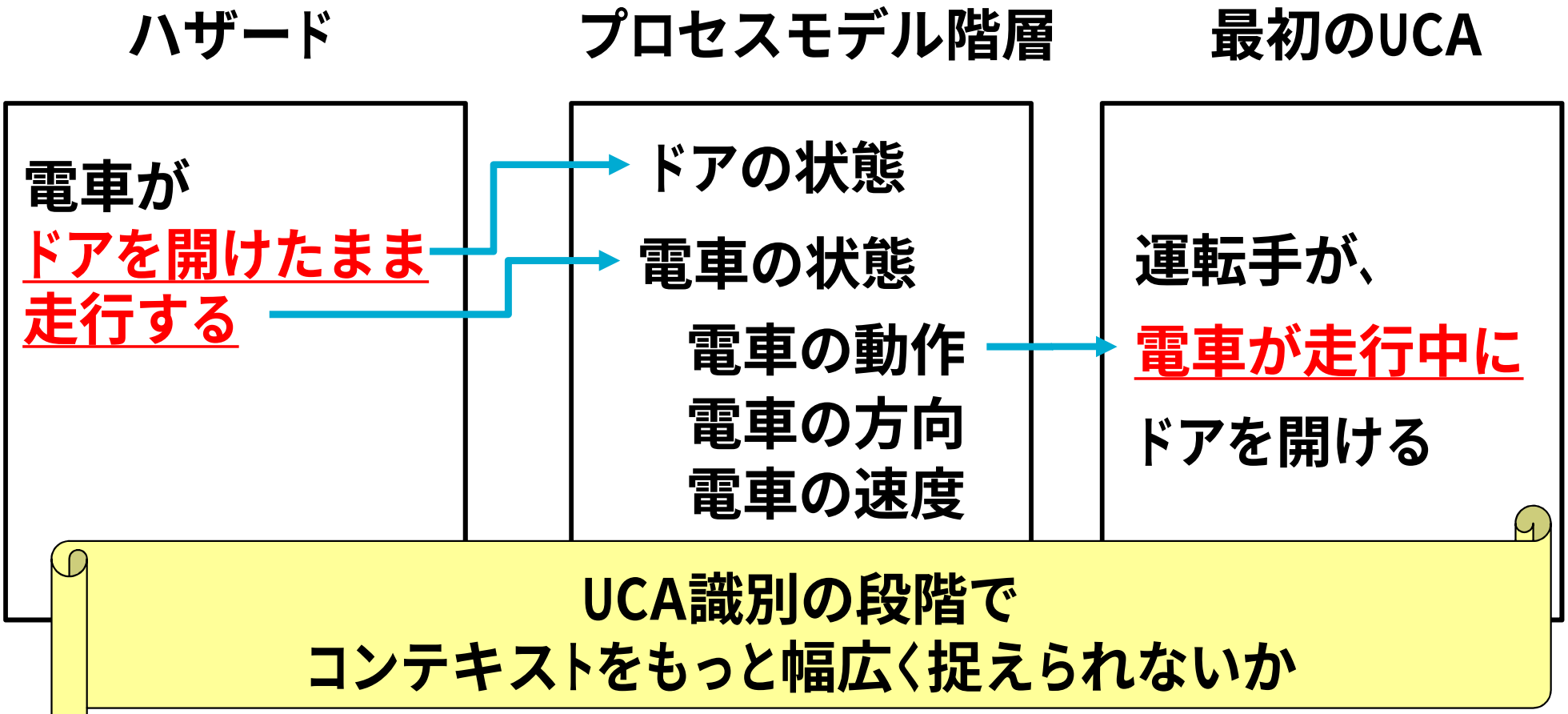
プロセスモデル
の組み合わせ

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
  - ハザードからコンテキストを得る
  - プロセスモデル階層により詳細化

コントロールアクション：
「ドアを開ける」



1 背景と課題－ STAMP/STPAの概要と課題

2 課題解決策 － Extending STPAの概要と試行

3 課題解決策の改良案－ Extending STPAの改良案

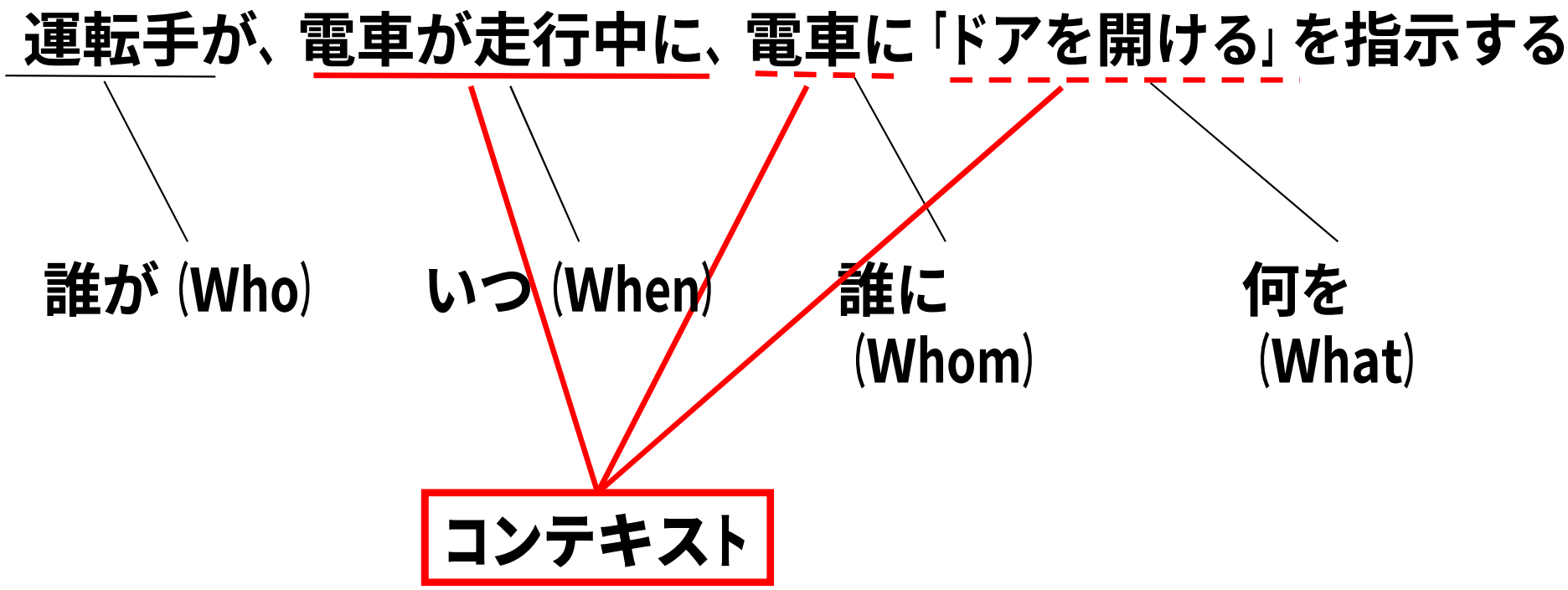
4 改良案の試行と効果

5 まとめ

改良案

UCAの構造を6W3Hで捉える

＜電車のUCA例＞



改良案

① UCA識別において6W3Hの視点からコンテキストを抽出

コントロールアクション：
「ドアを開ける」

6W3Hの視点	ガイドワード	コンテキスト
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	間違ったボタンを押して

※「なぜ (Why)」はStep2で考えるため除く。

改良案

◆ コンテキスト分解 (Extending STPA)

「間違ったドア」

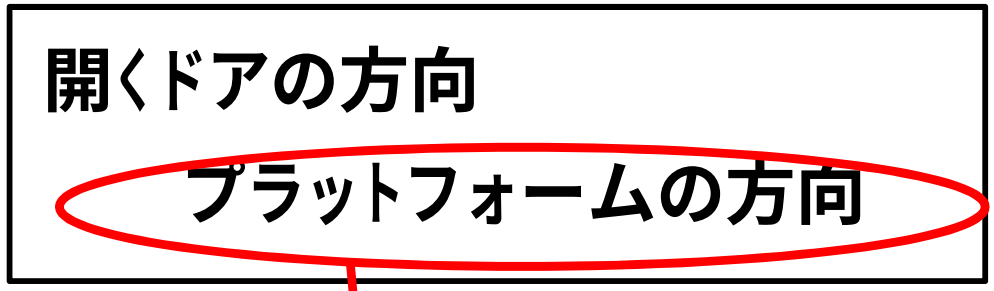
コンテキスト変数	コンテキスト値
開くドアの方向	プラットフォーム側 プラットフォームと反対側

◆ 新たなUCA：

運転手が、電車に「プラットフォームと反対側のドアを開ける」を指示する

改良案

② UCAの原因特定の前にプロセスモデルを詳細化

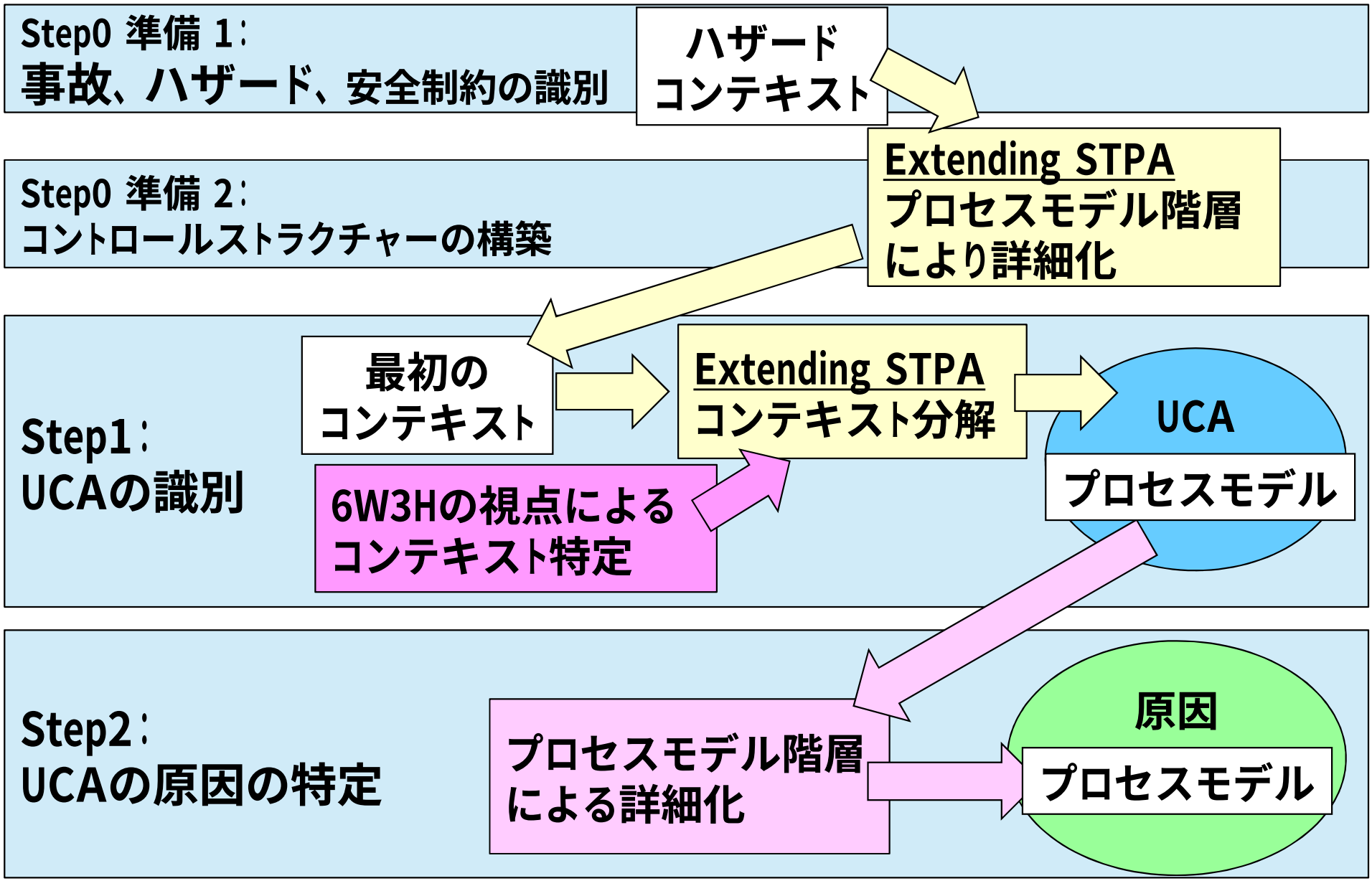


UCA：
プラットフォームと反対側のドアを開ける

◆UCAの原因：

プラットフォームは実際には右側にあるのに、
運転手は左側にあると認識する

プロセスモデル抽出方法



1 背景と課題－ STAMP/STPAの概要と課題

2 課題解決策 － Extending STPAの概要と試行

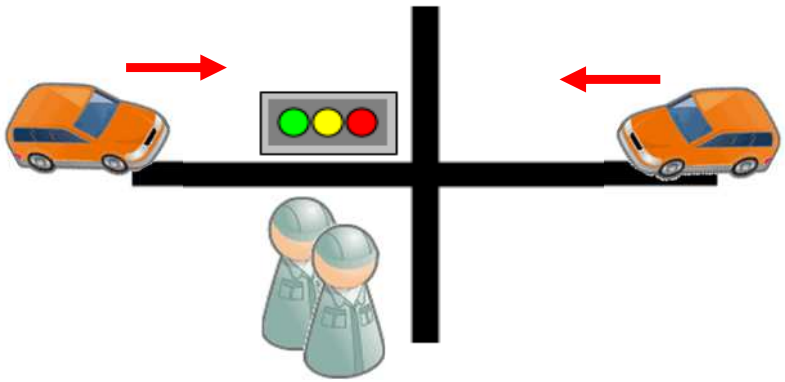
3 課題解決策の改良案－ Extending STPAの改良案

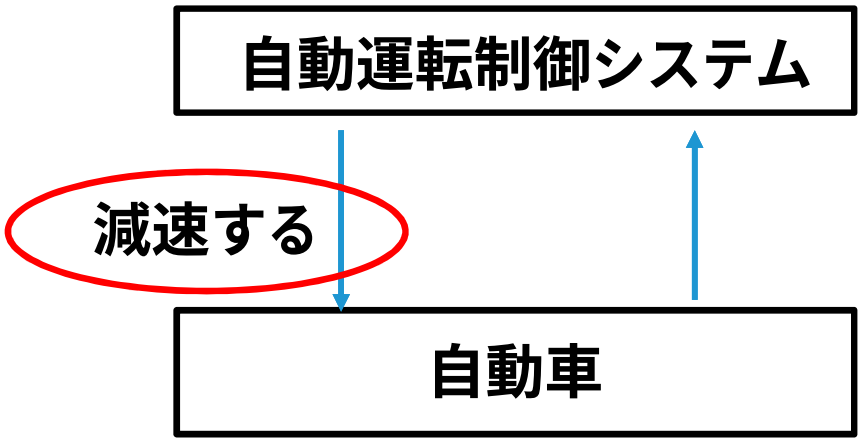
4 改良案の試行と効果

5 まとめ

改良案の試行

- 題材：自動運転制御システム
  - ◆事故：
    自動車が労働者に衝突する
  - ◆ハザード：
    自動車が、信号が赤のときに交差点に進入する





SERA（システムズエンジニアリング研究会）
http://sera.or.jp/index.html

改良案の試行

① コンテキストを6W3Hの視点から抽出

コントロールアクション：
減速する

6W3Hの視点	ガイドワード	コンテキスト
誰に (Whom)	間違った相手	間違った自動車
いつ (When)	間違ったとき	信号が赤、黄のとき
どこで (Where)	間違った場所	停止に不十分な地点で
どのくらい (How many)	間違った量・程度	不十分なブレーキ力

◆ 新たなUCA：

・間違った自動車に減速を指示する
・不十分なブレーキ力で減速を指示する

改良案の試行

② プロセスモデルの詳細化

◆ コンテキスト分解 (Extending STPA)

「停止に不十分な地点で」

コンテキスト変数	コンテキスト値
交差点までの距離	停止するのに十分、不十分

停止距離

車速	高速、中速、低速、停止
減速力	強、中、弱

ブレーキ力	強、中、弱
積載量	軽い、重い
路面状態	乾燥、半湿、湿潤
タイヤ状態	正常、磨耗している

改良案の試行

◆ UCA：

・間違った自動車に減速を指示する
・停止に不十分な地点で減速を指示する

◆ プロセスモデル：

信号の状態
交差点までの距離
停止距離
　車速
　減速力
　　ブレーキ力
　　積載量
　　路面状態
　　タイヤの状態
自動車ID

◆ UCAの原因：

- 自動運転制御システムが、自動車に誤った自動車IDを伝える。
- 自動車は、自動運転制御システムに車速、積載量、路面状態、タイヤの状態をフィードバックしない。

改良案の効果

試行結果

	ExSTPAのみ適用	ExSTPA＋改良案
コンテキスト	3	5
UCA	4	6
プロセスモデル	3	10
原因	10	15

考察

- 改良案により、具体的なプロセスモデルを数多く抽出

UCA識別、原因の特定に効果がある

1 背景と課題－ STAMP/STPAの概要と課題

2 課題解決策 － Extending STPAの概要と試行

3 課題解決策の改良案－ Extending STPAの改良案

4 改良案の試行と効果

5 まとめ

今後の課題

- プロセスモデルの組み合わせの増大にともなう原因特定の負荷をどうするか
- さらにコンテキストを幅広く捉えるにはどうするか

お話した内容

- STAMP/STPAの課題
- Extending STPAの概要
- Extending STPAの改良案
- 改良案の効果

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