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

Proposal for STAMP/STPA Enhancement through a Process Model Derivation Method

福島　祐子
yuko.fukushima@unisys.co.jp
日本ユニシス株式会社　総合技術研究所

発表要旨：

STAMP/STPA (Systems Theoretic Accident Model and Processes / System-Theoretic Process Analysis)は、数多くのシステムがつながることにより発生する事故の解析に有用とされており、安全性解析の新しい手法として注目されている。

従来の安全性解析手法（FTA、FMEA）では、事故を引き起こす原因はシステムの故障であるとしている。それに対して STAMP/STPA では、システムがシステムの状態を誤認識することにより、“安全ではないアクション”を実行することが事故の原因であり、それを特定するためにプロセスモデル（システムが認識するシステムの状態）の抽出が必要であるとしている。しかし、プロセスモデルの具体的な抽出方法については提示されておらず、分析者がアドホックに抽出するしかないという課題がある。

この課題に対し、MIT の John Thomas 氏は Extending STPA というコンテキスト（システムの状態）を分解してプロセスモデルを具体化していく手法を発表している。本提案は、この手法の前に、6W3H を適用してコンテキストを幅広く捉え、プロセスモデルの漏れを予防しようとするものである。

キーワード：

STAMP、STPA、安全性解析、ハザード分析、プロセスモデル

想定している聴衆

STAMP/STPA に興味がある方、適用している方

発表者の紹介（全角１００文字）：

長年、大規模システム開発向けの開発プロセス、要件定義手法の策定、適用に従事。
昨年から、安全性解析手法 STAMP/STPA の研究に着手。他に、システムズエンジニアリング、MBSE の研究も行っている。

* 副題は不要であれば行ごと削除してください

ソフトウェア品質シンポジウム2017
B1-1【経験発表】

UNISYS

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

2 課題解決策 ー Extending STPA

3 課題解決策の改良案

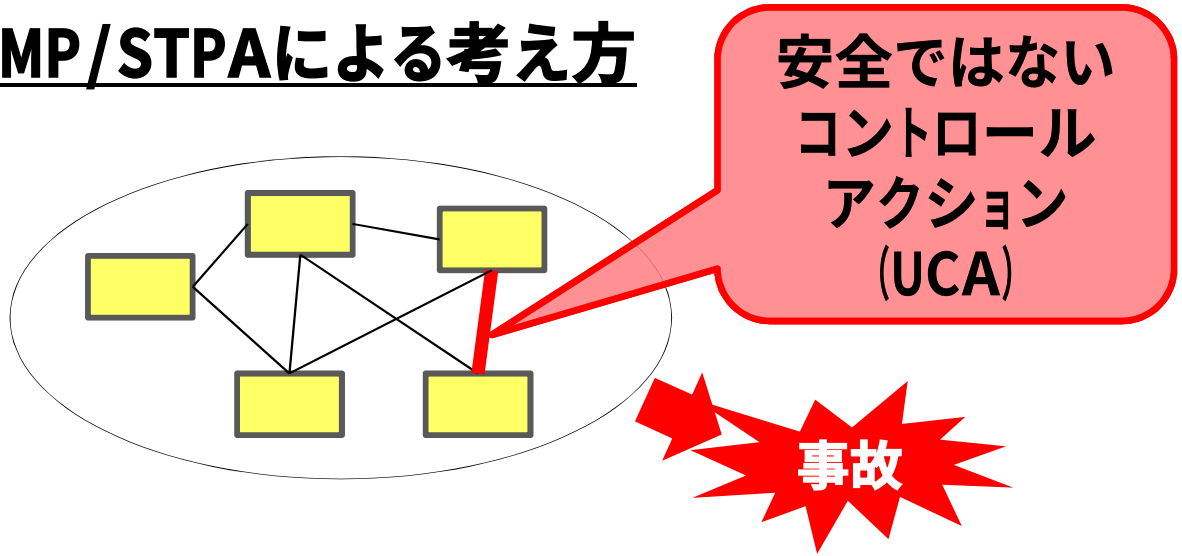
4 改良案の効果と提案

5 まとめ

STAMP/STPAの概要

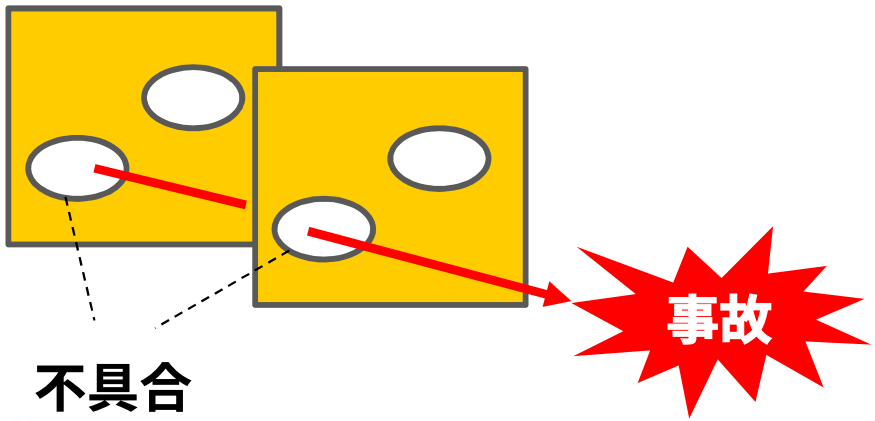
- 安全性解析（事故につながる原因を特定する）の新しい手法
- 多くの構成要素がつながるシステムにも対応

STAMP/STPAによる考え方



（Leveson, 2012）

従来の考え方（HAZOP、FMA等）



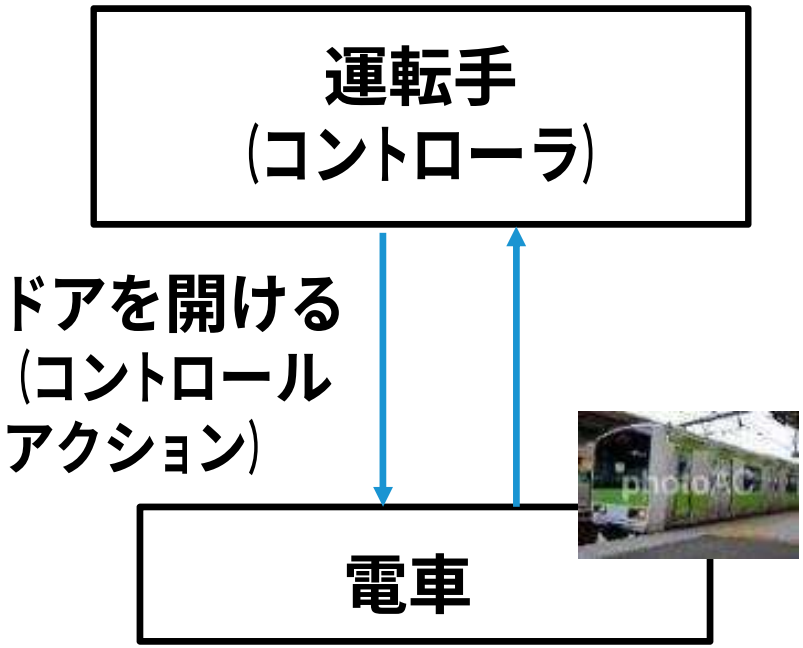
安全ではない
コントロールアクション（UCA）を
実行してはならない！

©2017 Nihon Unisys, Ltd. All rights reserved.

STAMP/STPAの概要

■「安全ではないコントロールアクション（UCA）」の原因

＜電車の例＞



UCA：
運転手が電車が走行中にドアを開ける

➡ 事故

原因：
運転手が「電車が停車中」と誤認識

プロセスモデル

コントローラがシステムの状態を誤認識することが原因。
原因の特定には、プロセスモデルを捉えることが重要！

©2017 Nihon Unisys, Ltd. All rights reserved.

STAMP/STPAの課題

■ STAMP/STPAによる分析ステップ

- 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
  - ◆4つのガイドワードによりハザードにつながるUCAを識別
- Step2：UCAの原因の特定
  - ◆UCAを引き起こす原因（ハザードシナリオ）を特定

※ハザードシナリオを特定する前にプロセスモデルが必要

(Leveson, 2012)

STAMP/STPAの課題：

プロセスモデルはどのように抽出するのか

©2017 Nihon Unisys, Ltd. All rights reserved.

Extending STPAの概要

■ UCAの構造を定義

＜電車の例＞

◆ 事故：　人が電車から落ちて負傷する
◆ ハザード：　電車がドアを開けたまま走行する

UCAの構造：

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：ソースコントローラ
- 電車が走行中に：コンテキスト：UCAであることが決まる
- 「ドアを開ける」：コントロールアクション
- 指示する：タイプ

運転手は、「ドアを開ける」を指示する

→ UCAであるのか不明

(Thomas, 2013)

©2017 Nihon Unisys, Ltd. All rights reserved.

Extending STPAの概要

■ 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)

コンテキスト変数	コンテキスト値
電車の動作	停車中
	走行中
電車の位置	プラットフォーム
	プラットフォーム以外

プロセスモデルとして捉える

コントロールアクション：運転手は「ドアを開ける」を指示する

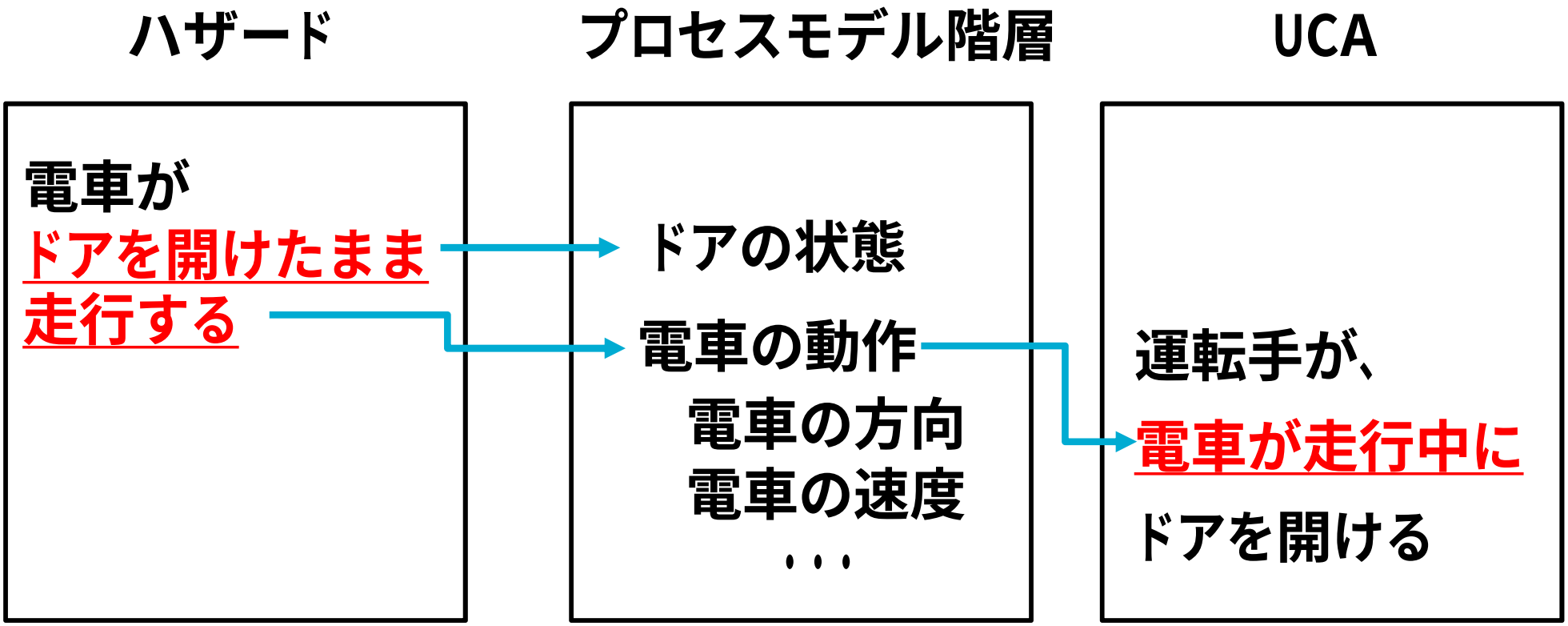
コンテキスト値の組み合わせ

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

©2017 Nihon Unisys, Ltd. All rights reserved.

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



©2017 Nihon Unisys, Ltd. All rights reserved.

Extending STPAの試行

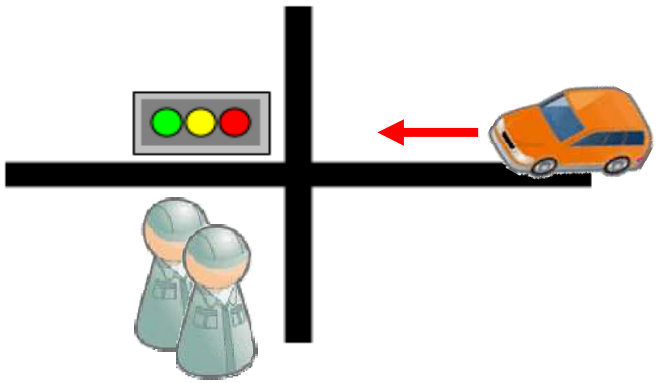
■ 題材：自動運転制御システム

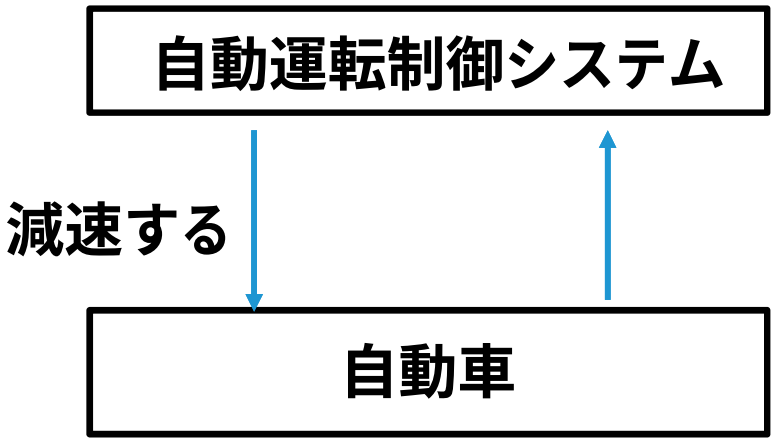
◆事故：

労働者が自動車に衝突して死亡する、あるいは重症を負う

◆ハザード（事故につながるシステムの状態）：

自動運転車が、信号が赤のときに交差点に進入する





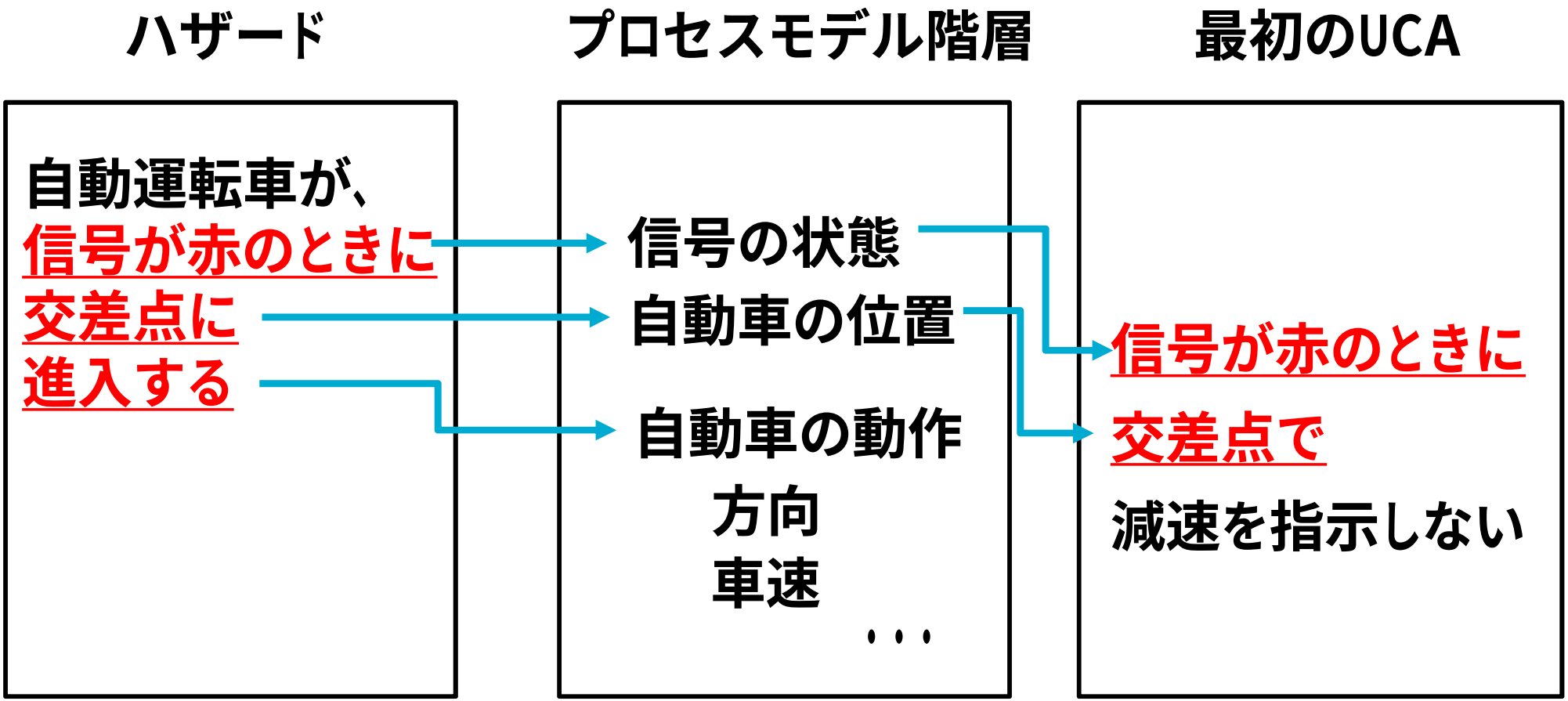
SERA（システムズエンジニアリング研究会）
http://sera.or.jp/index.html

©2017 Nihon Unisys, Ltd. All rights reserved.

Extending STPAの試行

■ 最初のUCAのコンテキストを特定

◆コントロールアクション：
自動運転制御システムは、自動車に減速を指示する



©2017 Nihon Unisys, Ltd. All rights reserved.

Extending STPAの試行

◆ 初期のUCA：

信号が赤のときに、交差点で、減速を指示しない

◆ 初期のコンテキスト：

信号の状態、自動車の位置、自動車の動作

◆ コンテキスト分解：

	コンテキスト変数	コンテキスト値
信号の状態 →	信号の状態	青、黄、赤、不明
自動車の位置 →	交差点までの距離	停止距離以上、停止距離未満
自動車の動作 →	車速	高速、中速、低速、停止

©2017 Nihon Unisys, Ltd. All rights reserved.

Extending STPAの試行

◆コントロールアクション：
自動運転制御システムは、自動車に減速を指示する

◆コンテキスト変数：　信号の状態、交差点までの距離、車速

◆UCA：

ガイドワード / CA	指示しないこと	指示すること	誤ったタイミング/順序	指示をやめるのが早すぎる/指示が長すぎる
減速を指示する	(UCA1) 信号が赤、黄のときに減速を指示しない	(UCA2) 停止距離未満の地点で減速を指示する	(UCA3) 減速の指示が遅れる	(UCA4) 停止していないのに減速の指示をやめる

◆ ハザードシナリオ：
・信号の状態のフィードバックが遅れる、誤ってフィードバックされる
・交差点までの距離の入力が遅れる、あるいは誤る。

上記を含め、10シナリオ

©2017 Nihon Unisys, Ltd. All rights reserved.

改良案

UCAのコンテキストをもっと幅広く捉えられないか

■ UCAの構造を6W3Hで捉える

運転手が、電車が走行中に、電車に「ドアを開ける」を指示する

誰が (Who)

誰に (Whom)

何を (What)

コンテキスト

©2017 Nihon Unisys, Ltd. All rights reserved.

改良案

■ コンテキストを6W3Hの視点から抽出

6W3Hの視点	ガイドワード	例
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。

◆ 新たなUCA：

運転手が、電車に「プラットフォームと逆サイドのドアを開ける」を指示する

©2017 Nihon Unisys, Ltd. All rights reserved.

改良案の試行

① 6W3Hの視点を適用

◆ コントロールアクション：
「自動運転制御システムは、自動車に減速を指示する」

誰に (Whom)	間違った自動車
いつ (When)	信号が赤、黄のとき
どこで (Where)	停止距離未満の地点で
どのくらい (How many)	不十分なブレーキ力

◆ 新たなUCA：

(UCA5) 間違った自動車に減速を指示する

(UCA6) 不十分なブレーキ力で減速を指示する

©2017 Nihon Unisys, Ltd. All rights reserved.

改良案の試行

② コンテキスト分解し、さらにプロセスモデルを詳細化

コンテキスト変数	コンテキスト値
信号の状態	青、黄、赤、不明
交差点までの距離	停止距離以上、停止距離未満
車速	高速、中速、低速、停止
自動車ID	ID1、ID2、・・・
ブレーキ力	強、中、弱

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

©2017 Nihon Unisys, Ltd. All rights reserved.

改良案の試行

③ ①のUCAと②のプロセスモデルからハザードシナリオを特定

◆ 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

◆ ハザードシナリオ：

- 自動車に誤った自動車IDを伝える。
- 自動車が間違ったIDをフィードバックする。
- 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、あるいは誤ってフィードバックする。

上記含め、15シナリオ

「自動運転制御システム」に対する安全要件：

- 自動車に間違った自動車IDを伝えない
- 車速、積載量、路面状態、タイヤの状態を正しく把握すること

©2017 Nihon Unisys, Ltd. All rights reserved.

改良案　試行結果と考察

■ 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
ハザードシナリオ	10	15

- ◆ 6W3Hの視点によりコンテキストが増えた。それによりUCA、プロセスモデル、ハザードシナリオが増えた。
- ◆ プロセスモデル階層の分解を行うことにより、具体的なプロセスモデル、ハザードシナリオを特定できた。

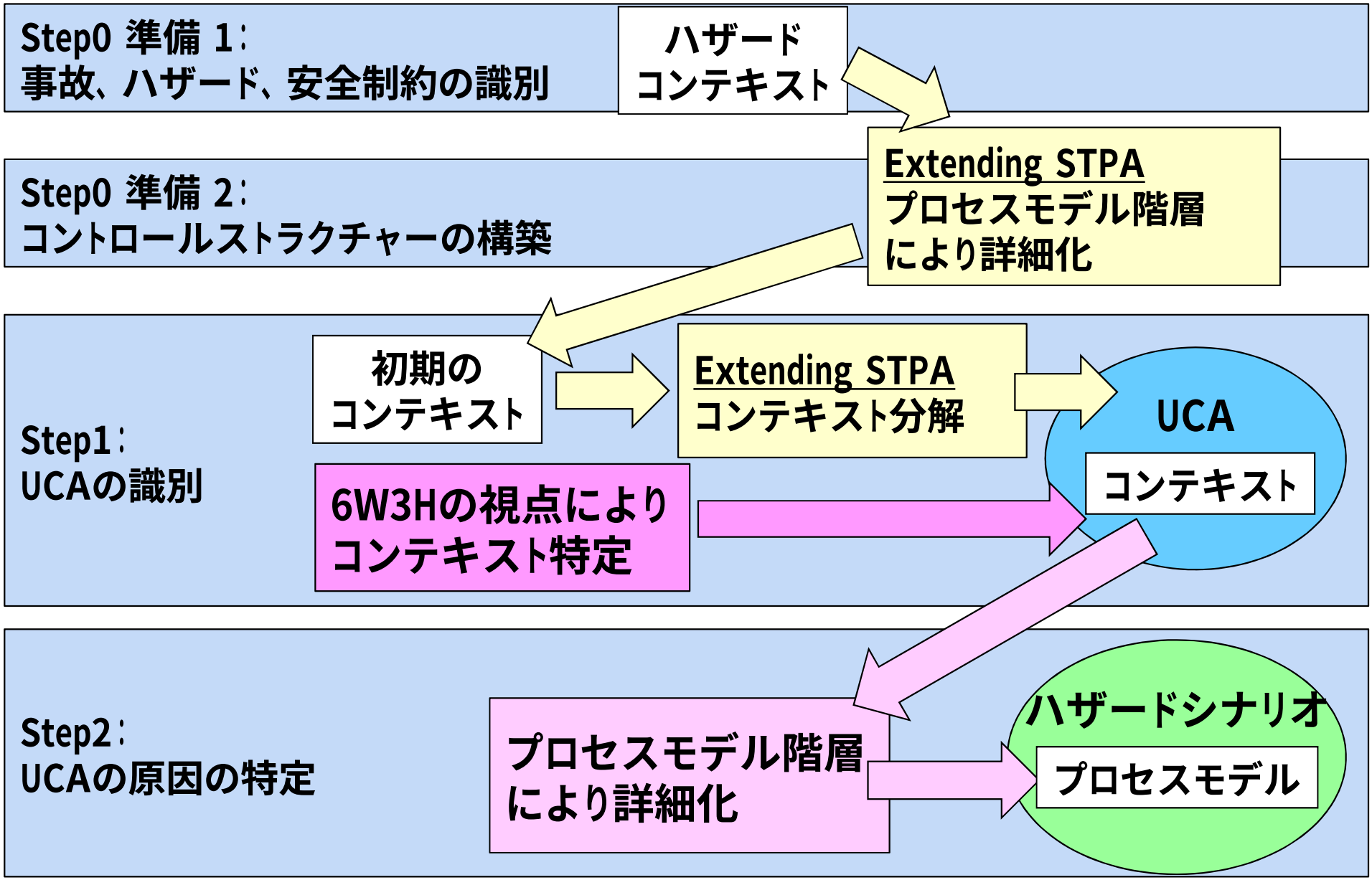
■ 考察

➢ Extending STPAの改良案により

- ◆UCA識別、ハザードシナリオ特定に効果がある
- ◆具体的な安全要件の特定への効果が期待できる

©2017 Nihon Unisys, Ltd. All rights reserved.

プロセスモデル抽出方法の提案



©2017 Nihon Unisys, Ltd. All rights reserved.

今後の課題

- STPA分析のレベルによるプロセスモデル等の抽象度をどう考えるか

- プロセスモデルの組み合わせの増大にともなうハザードシナリオ特定の負荷をどうするか

©2017 Nihon Unisys, Ltd. All rights reserved.

まとめ

- STAMP/STPAの課題
- Extending STPAの概要
- Extending STPAの改良案
- 改良案の試行と結果
- プロセスモデル抽出方法の提案

©2017 Nihon Unisys, Ltd. All rights reserved.

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

©2017 Nihon Unisys, Ltd. All rights reserved.

Foresight in sight

UNISYS

ご清聴ありがとうございました