HITACHI
Inspire the Next

第3回STAMPワークショップ

STPA の損失シナリオ特定時における シナリオ記述への木構造の導入

2018/12/04

(株)日立製作所 研究開発グループ
システムイノベーションセンタ
竹下 若菜 †
峯　博史

† 現(株)アート

HITACHI
Inspire the Next

目次

1. 背景
2. 課題
3. 提案手法
4. 評価
5. まとめ

1-1. 背景

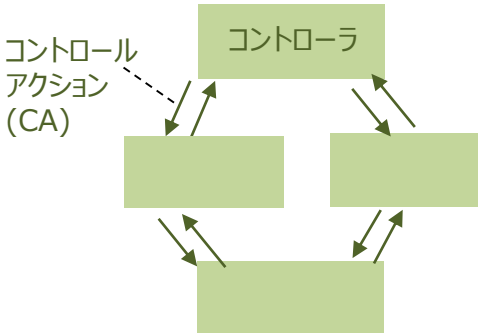
HITACHI
Inspire the Next

準備ステップ+2ステップによる，ガイドワードを用いたシステマティックな分析

準備（Step0）

分析のためのSTAMPモデルの構築

コントロールストラクチャ



分析の対象の選定

アクシデント/ハザード/安全制約を識別

Step1

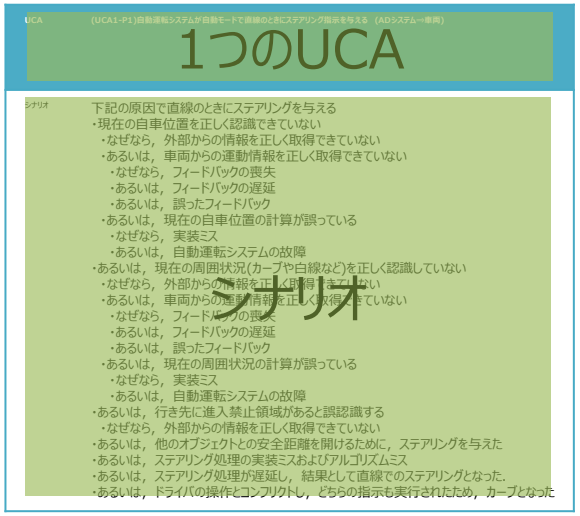
4つのガイドワードを使ってUCAを導出

UCA表

Step2

13個のヒントワードを使ってシナリオ/ファクタを導出

コントロールストラクチャ図
+13個のヒントワードから導出



分析工数削減のために似たSTAMPモデルを持つ
システムに分析結果を一部利用したい。
手法の改良ができないか．．．

HITACHI
Inspire the Next

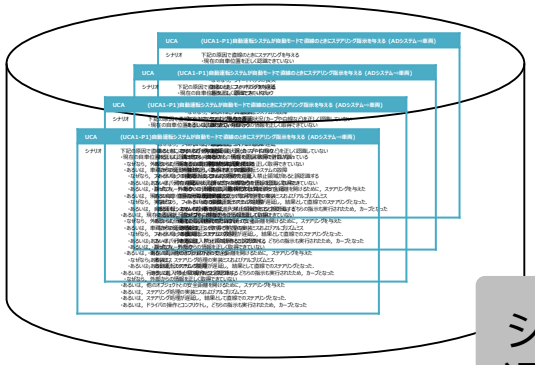
目次

2-1. 分析結果再利用時の課題

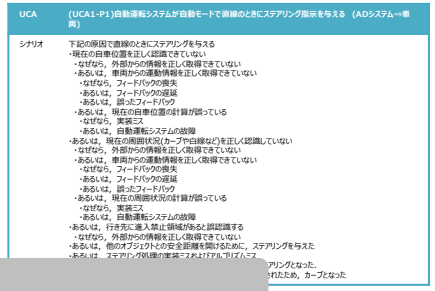
HITACHI
Inspire the Next

課題 1　過去に抽出した損失シナリオの一部を他の分析時に適用(再利用)することが困難

過去シナリオデータベース



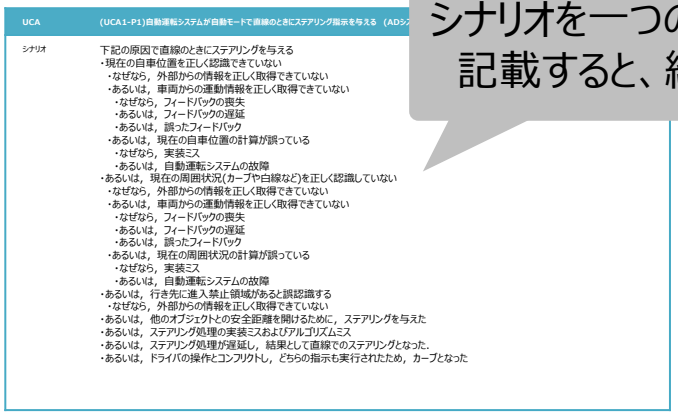
シナリオ



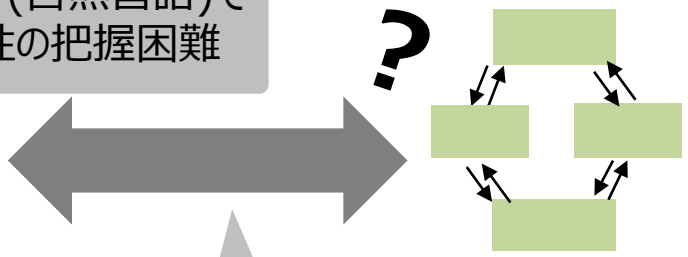
シナリオを一つの文書(自然言語)で記載すると、
過去の複数の損失シナリオの一部を再利用困難

課題 2　分析結果(損失シナリオ)の網羅性の把握ができず、レビューが困難

シナリオ



シナリオを一つの文書(自然言語)で
記載すると、網羅性の把握困難



コントロールループとの
対応付けも不明確

HITACHI
Inspire the Next

目次

1. 背景
2. 課題
3. 提案手法
4. 評価
5. まとめ

3-1.提案手法

HITACHI
Inspire the Next

- 過去分析結果再利用時の課題
  1. **一つの文書(自然言語)によるシナリオ記載**では、過去分析結果の一部を再利用が難しい
  2. **コントロールアクション(CA)との対応が不明確**であり過去分析結果の網羅性が把握できないため、妥当性レビューが難しい

抽出したシナリオ(の一部)を再利用可能な形式的な表記方式を適用し、かつその表記方式において各シナリオまたはシナリオを形成するファクタに対応するCA情報を付与する。

これにより、過去分析結果再利用による分析時間の削減と網羅性の把握が可能になり妥当性レビューの容易性が見込まれる。

3-2.提案手法

HITACHI
Inspire the Next

- 損失シナリオ(の一部)を再利用可能にする形式的な表記方式の要件
  1. 自然言語で表現した全損失シナリオが抽出できること
  2. 損失シナリオの一部を抽出することができること
  3. 対応するCA情報の付与が容易であること

- 解決木構造表現による損失シナリオの記載による解決

  FTA木に似たツリー構造を使用して、損失シナリオを表現
  1. ノードを辿ることにより、損失シナリオを抽出することが可能
  2. シナリオの一部を形成するノード群を抽出することが可能
  3. 各ノードに対応するCA情報を付与することが可能

損失シナリオの記載を木構造で表現することで、
過去の分析結果を再利用する際に発生する
課題を解決できる

3-3.提案手法

HITACHI
Inspire the Next

Step1

UCA表

CA	Not Providing Causes Hazard	Providing Causes Hazard	Wrong Timing or Order Cause Hazard	Stopped Too Soon or Applied Too Long
1 ステアリング，ブレーキ，加速（ADシステム⇒車両）	自動運転システムが手動制御時に直線でステアリング，ブレーキ，アクセル，反力指示を与えない	(UCA1-P1-1)自動運転システムが手動制御時に直線でステアリング，反力指示を与える (UCA1-P1-2)自動運転システムが手動制御時に直線で操作指示をしていないのに反力指示を与える 自動運転システムが手動制御時に直線で加減速，反力指示を与える	(UCA1-T1-1)自動運転システムが手動制御時に直線でステアリング，ブレーキ，アクセル，反力指示を早く与える (UCA1-T1-2)自動運転システムが手動制御時に直線でステアリング，ブレーキ，アクセル，反力指示を遅く与える	(UCA1-D1-1)自動運転システムが手動制御時に直線でステアリング，ブレーキ，アクセル，反力指示を必要以上に多く与える 自動運転システムが手動制御時に直線でステアリング，ブレーキ，アクセル，反力指示をすぐにやめてしまう

ガイドワード

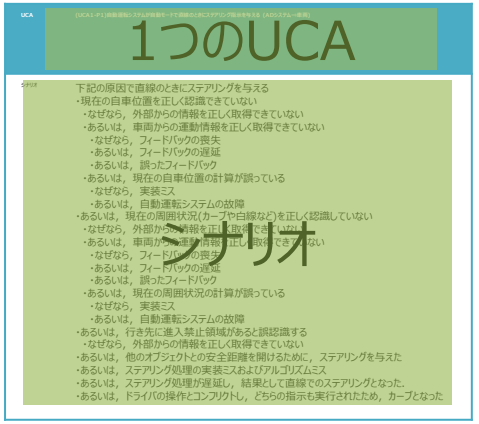
CA

UCA

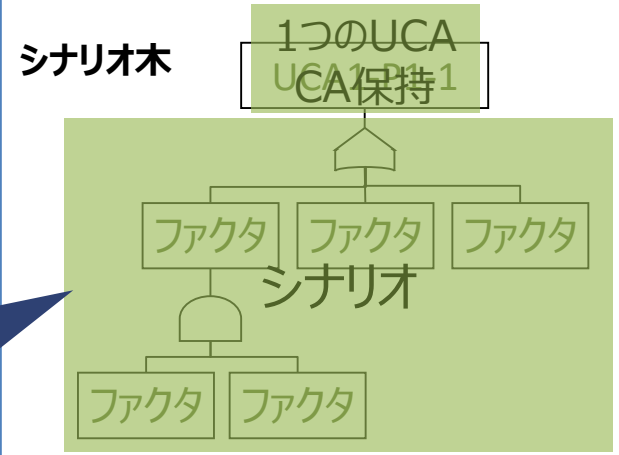
シナリオ

Step2

従来手法：自然言語で記述

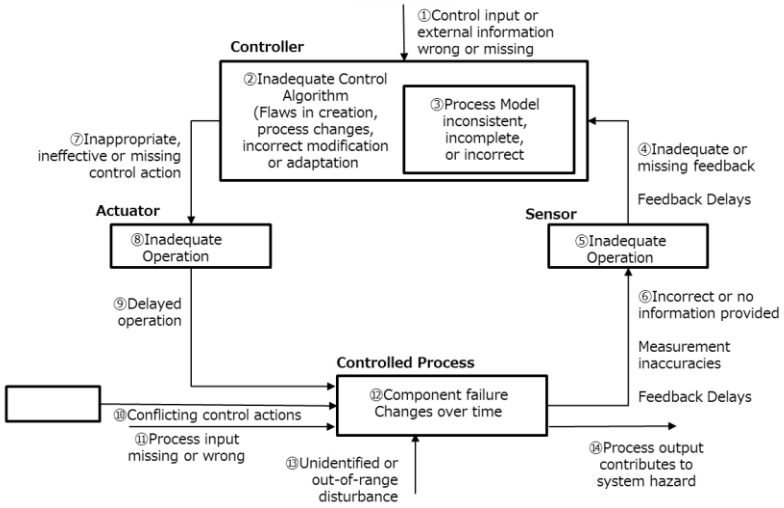


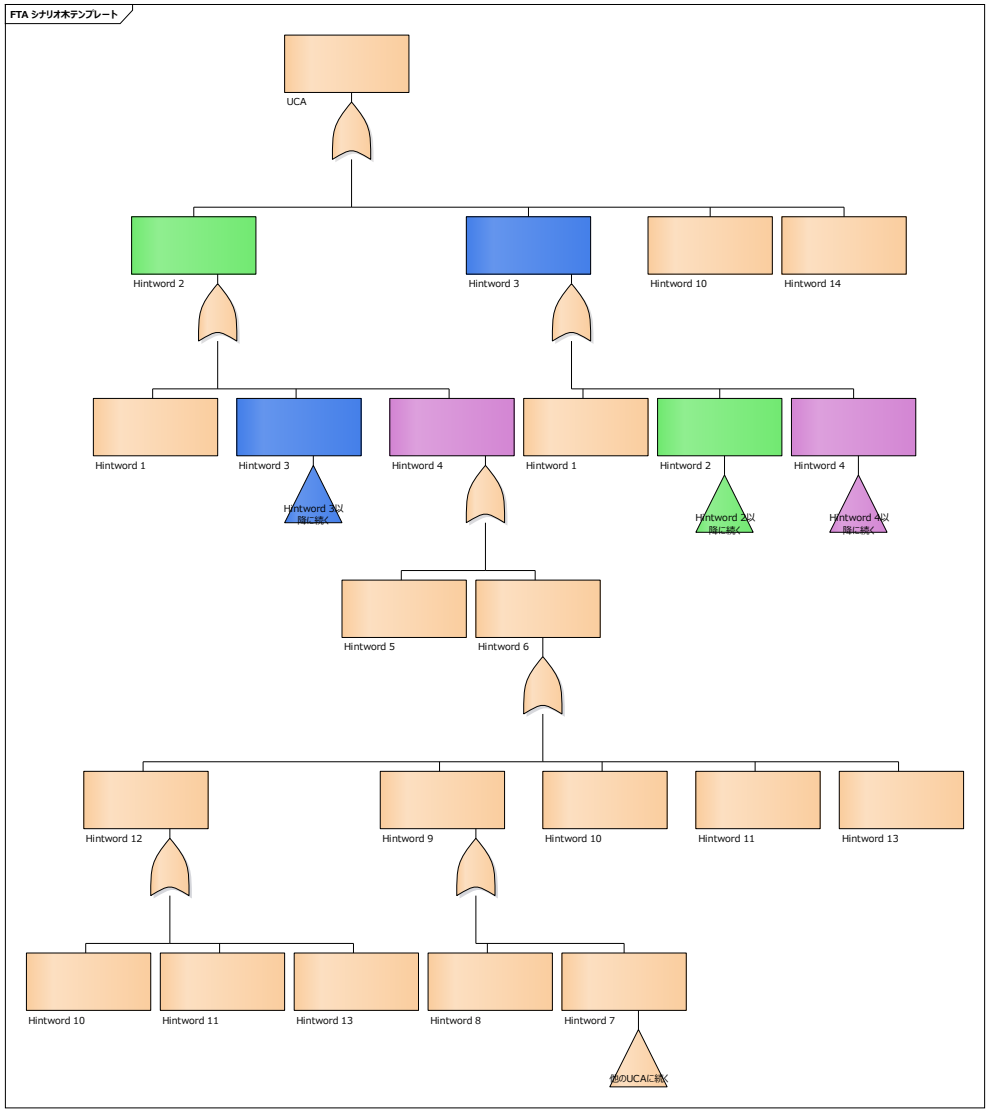
提案手法：木構造で記述



1つのUCAに対する損失シナリオを木構造で表現
シナリオの「あるいは」がOR、「かつ」がANDに対応

3-4.提案手法

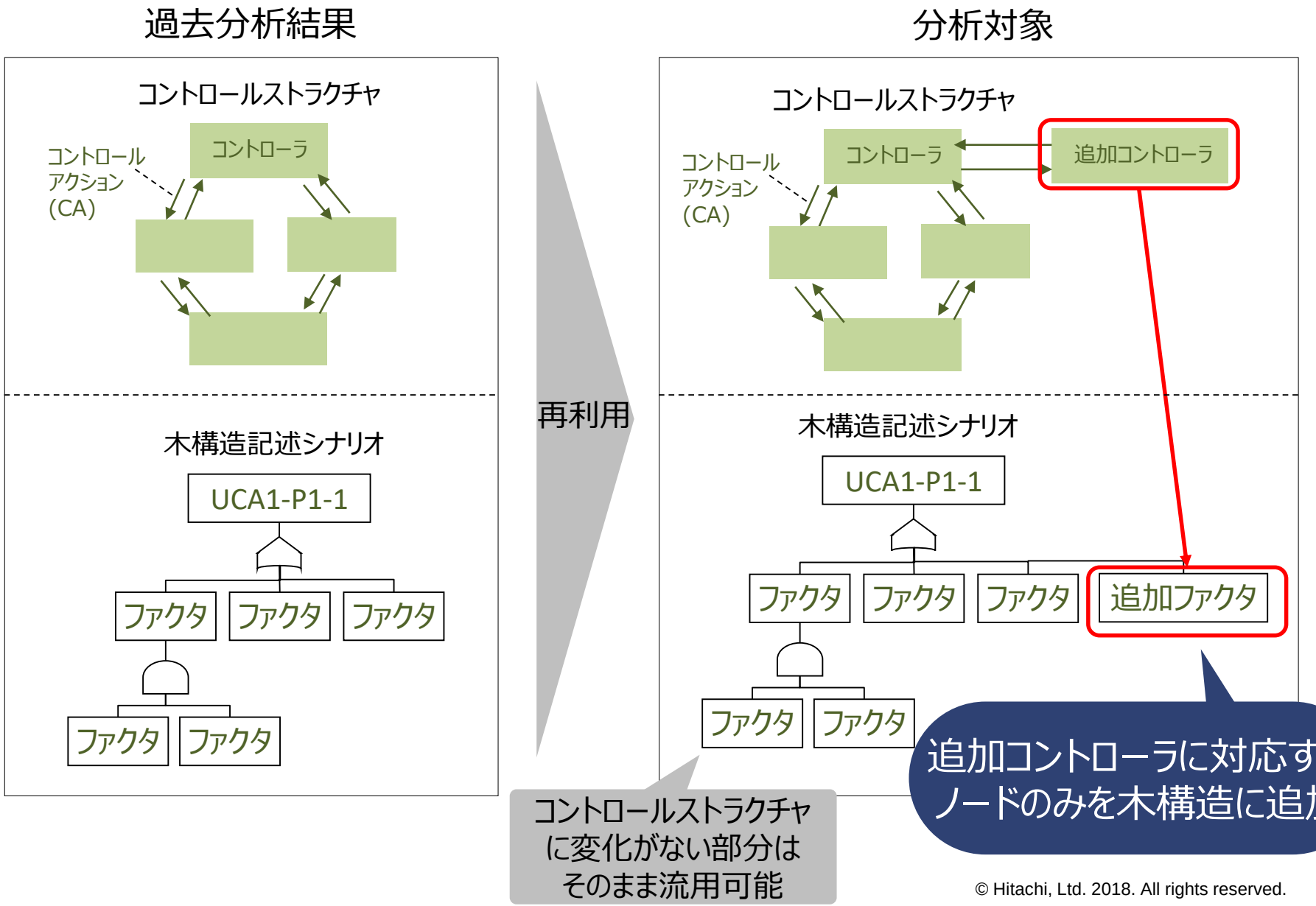




UCAに至るシナリオ(各ノード)は
13のヒントワードを用いて抽出する

3-5.提案手法

HITACHI
Inspire the Next



3-6.提案手法の適用例

HITACHI
Inspire the Next

(例）単線の踏切制御装置(IPA発行「はじめてのSTAMP/STPA」より抜粋)

コントロールストラクチャ図

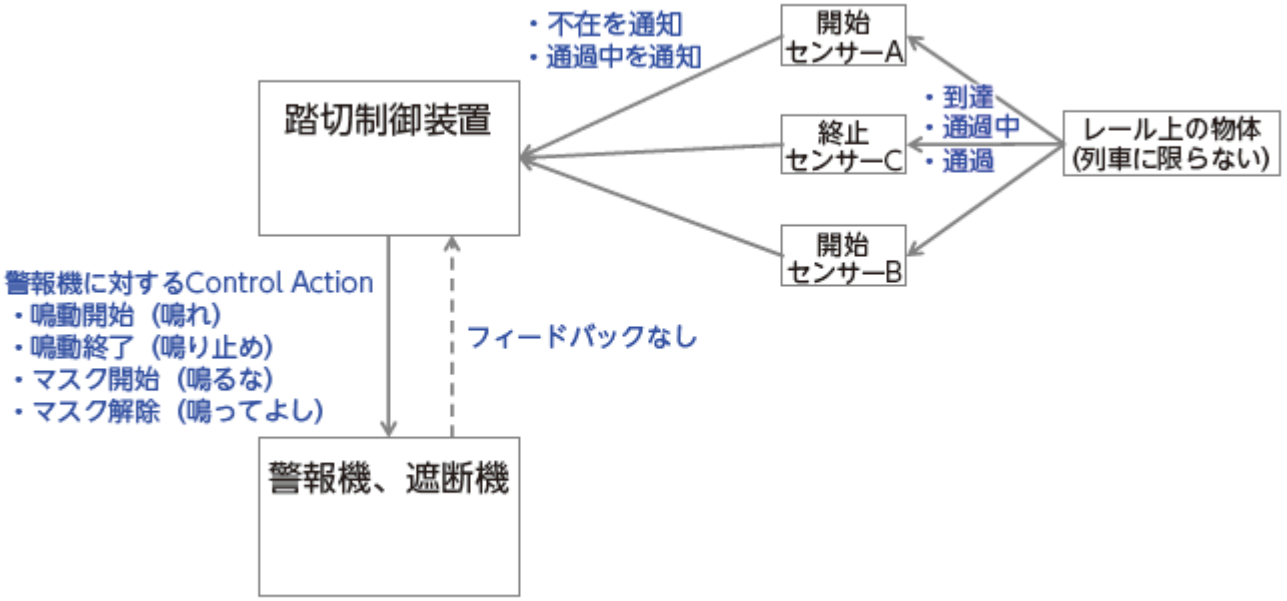


図 4.3-2　実施例：Step0　コントロールストラクチャーの構築

3-7.提案手法の適用例

HITACHI
Inspire the Next

(例) 単線の踏切制御装置(IPA発行「はじめてのSTAMP/STPA」より抜粋)

UCA例

(UCA4) 列車が来ないのにマスク指示し、警報鳴動しない
(UCA4) 反対側の開始センサーにもマスク指示し、警報鳴動しない

シナリオ例

(シナリオ4-1)「②コントロールアクションが不適切　and/or ⑥不十分な制御・アルゴリズム」列車がA, Cを通過してBのみをマスクすべきところ、Aもマスクしたため、後続列車がきても警報鳴動しない
対策：マスク解除するときには、AとCの両方のマスクを解除する。踏切制御装置が状態を持つと、状態制御に関連する誤りが発生しうる。誤りがあっても対応できるようにする必要がある。

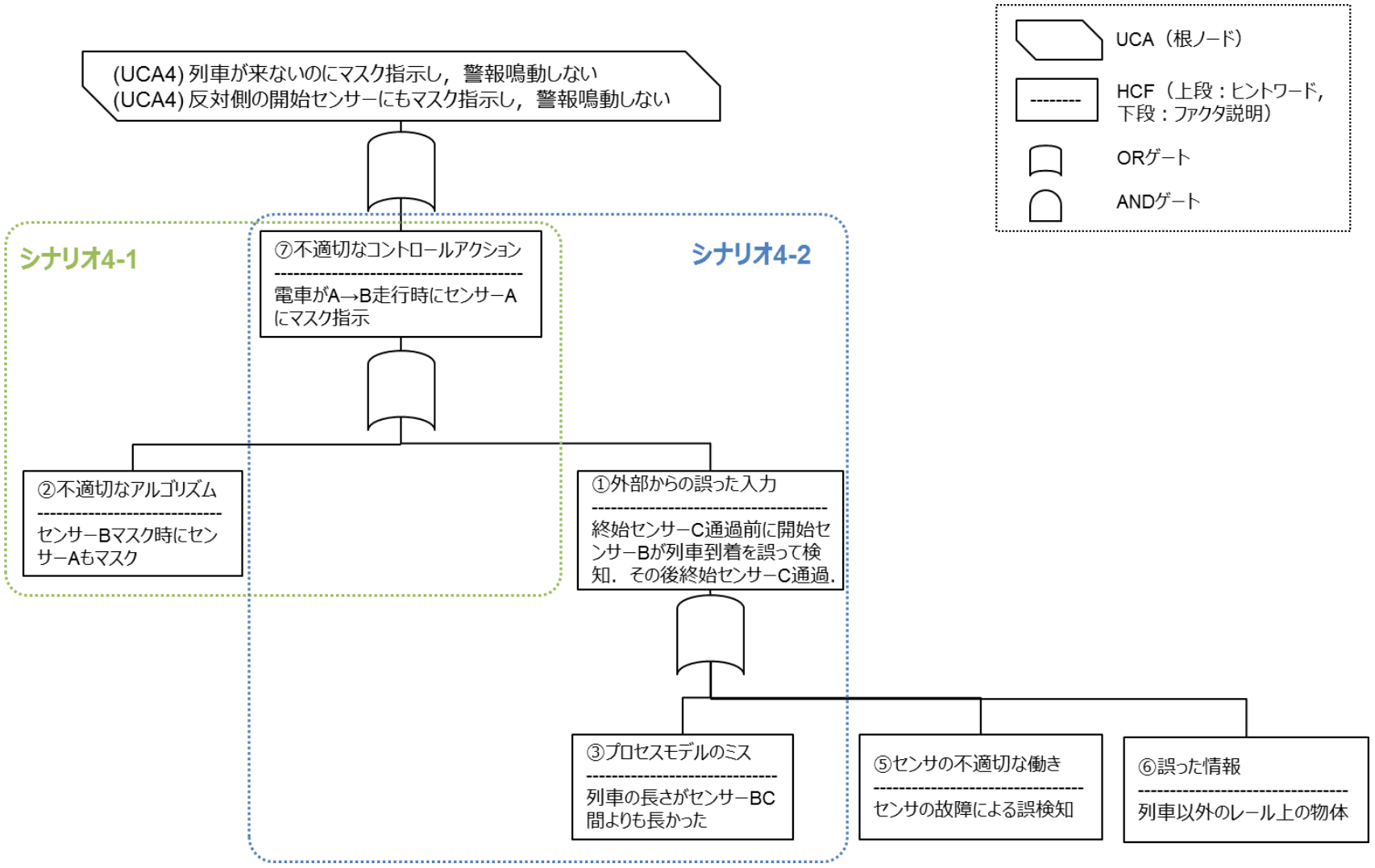
(シナリオ4-2)「③動作の遅れ」+「⑥不十分な制御・アルゴリズム」A方向から来たセンサーBC間よりも長い列車が終始センサーCを通過中、開始センサーBが列車を検知し、警報再鳴動する。終始センサーCを通過後Bへマスク指示を出し列車がBを通過後マスクを解除する。一方終始センサーCはセンサーBから検知を受けているため列車が通過後Aにもマスク指示を出すが、列車はAを通過することはないので、マスクが残りA方向から後続列車が来ても警報鳴動しない。

シナリオ4-1および4-2を木構造で表現

3-8.提案手法の適用例

HITACHI
Inspire the Next

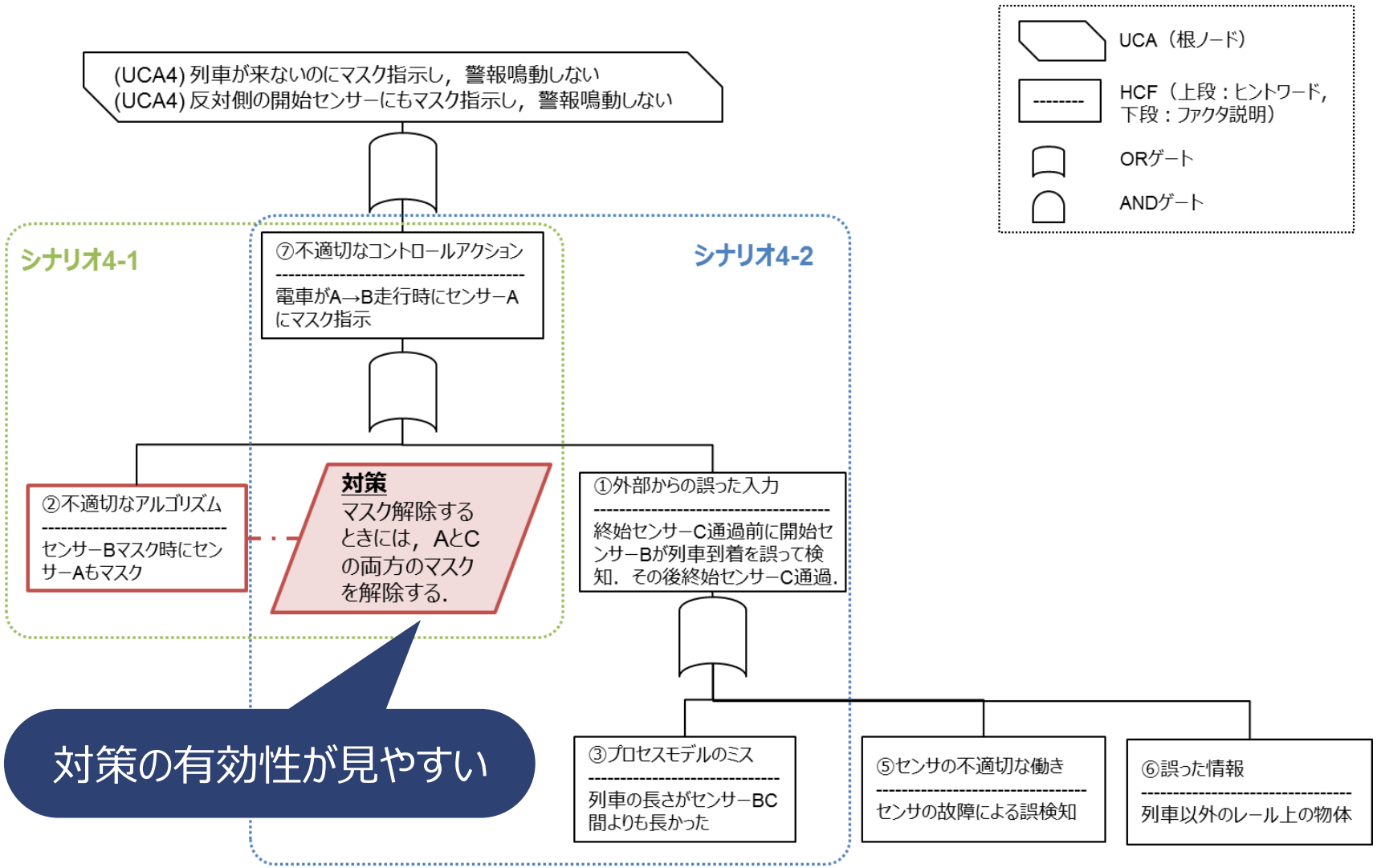
シナリオ4-1および4-2の木構造表現



3-9.提案手法の適用例

HITACHI
Inspire the Next

シナリオ4-1および4-2の木構造表現



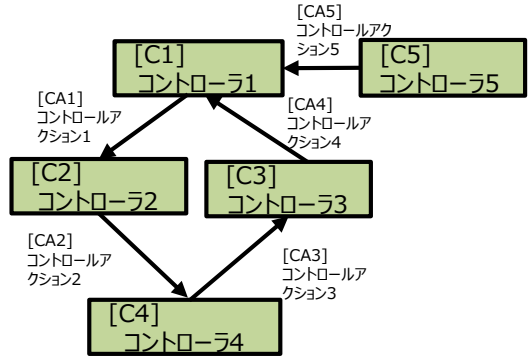
3-10.提案手法の応用例

HITACHI
Inspire the Next

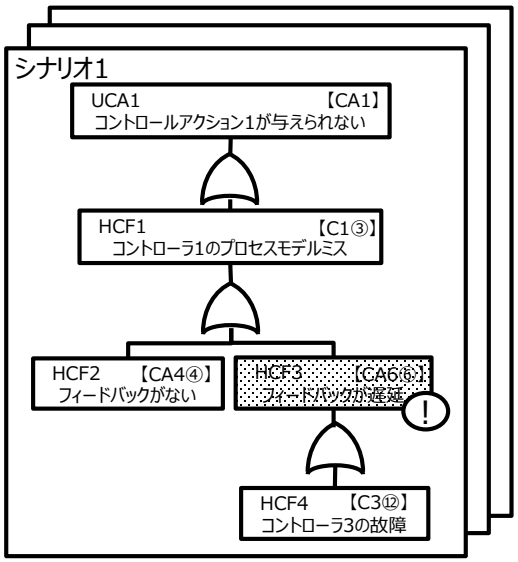
STAMP/STPA分析時に使用可能なハザードシナリオリコメンデーション

ユーザ入力

【コントロール図】



【シナリオ】

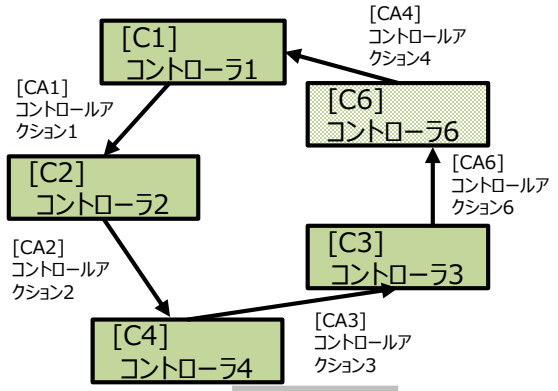


類似度の高い制御ループを含む図を検索

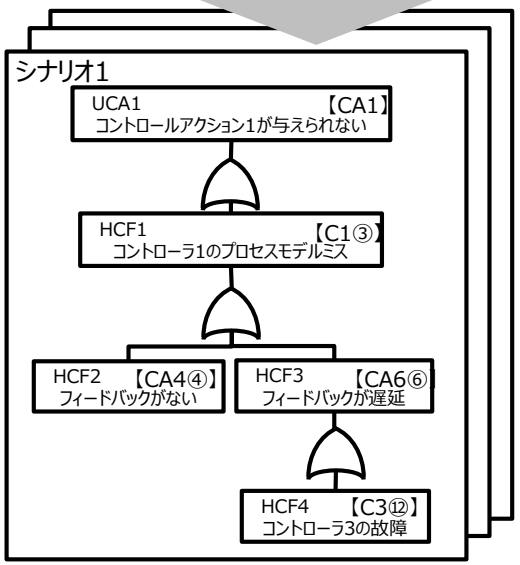
入力されたコントロール図から過去DBを探索し，推奨される**ハザードシナリオを出力**

リコメンデーション

過去分析結果DB



【シナリオ】 取得



ハザードシナリオが**コントロール図との対応関係を持ち，各ノードにガイドワード番号を持つツリー構造**として過去DBに蓄積

HITACHI
Inspire the Next

目次

1. 背景
2. 課題
3. 提案手法
4. 評価
5. まとめ

4-1. 評価

HITACHI
Inspire the Next

評価目的

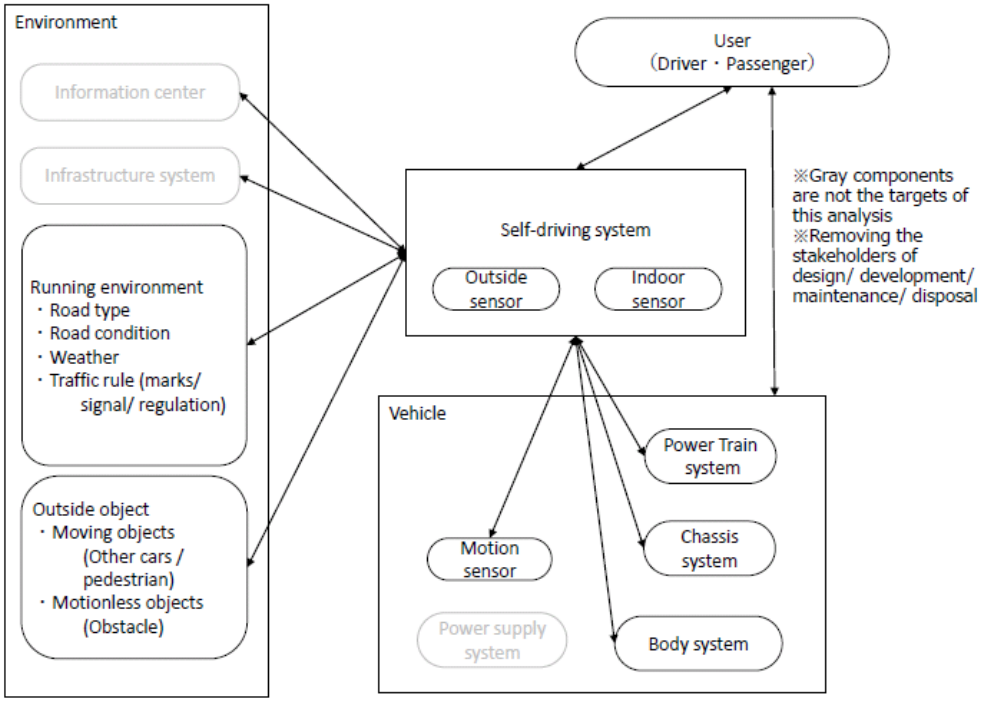
1. STAMP/STPA step2における木構造表現化可否の確認
2. 同一システム内の異なるUCAの分析過程での再利用性の確認

分析対象システム

自動運転システム

分析の前提

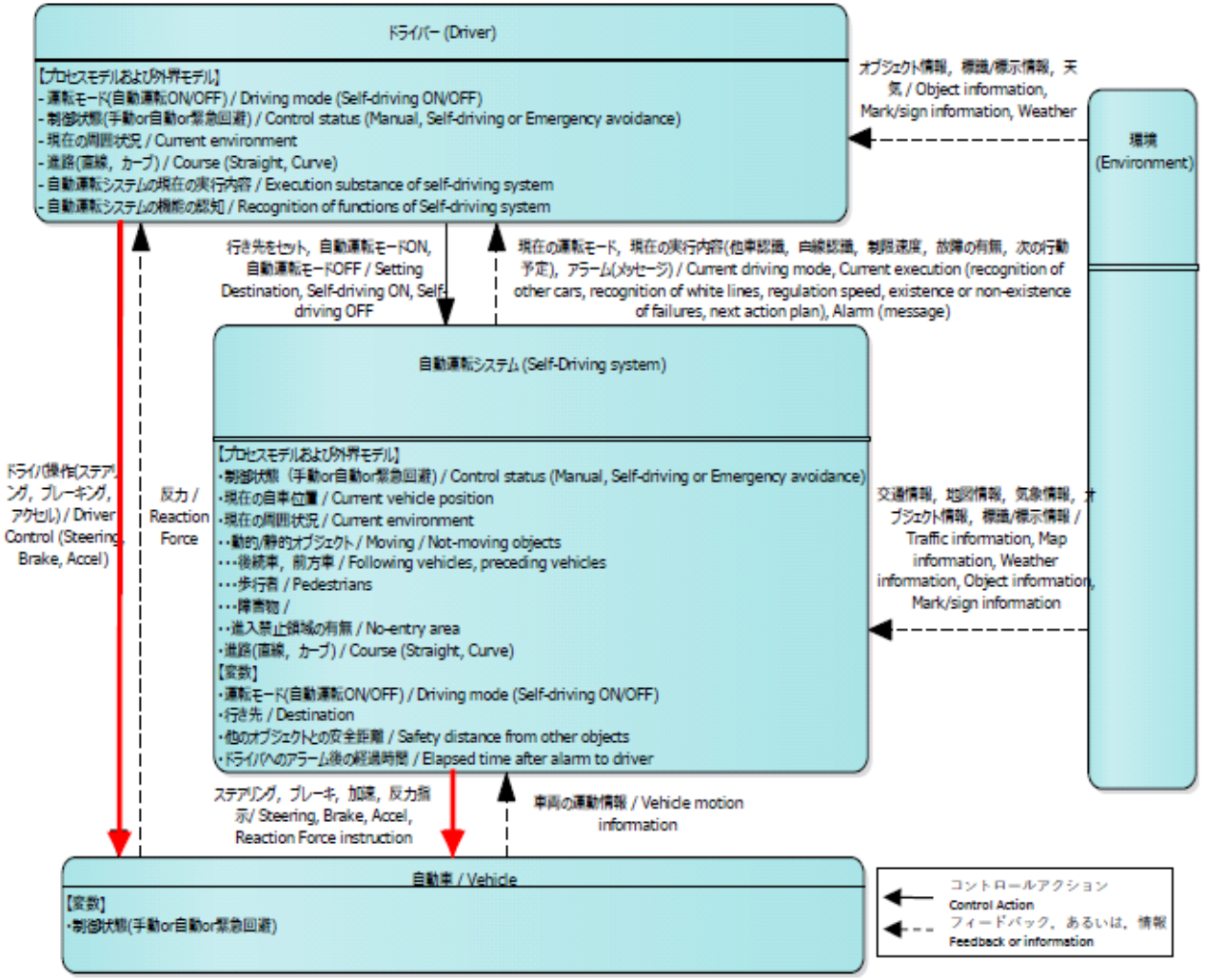
- 「他オブジェクトへの衝突」を分析対象とする
- ミッションの失敗などは分析対象としない
- 「自動運転する」機能のみを分析/比較



4-2. 評価

HITACHI
Inspire the Next

分析対象のコントロールストラクチャ



4-3. 評価

HITACHI
Inspire the Next

評価に使用した自動運転システムのUCAテーブル(一部抜粋)

GuideWords

Control Action	Context	"Not providing causes hazard"	"Providing causes hazard"	"Too early, Too late, Wrong order causes hazard"	"Stopping too soon/ Applying too long"
UCA594 ドライバ操作(ステアリング，ブレーキング，アクセル) / Driver Control (Steering, Brake, Accel) ドライバー (Driver) → 自動車 / Vehicle	制御状態：手動 設定 範囲：カーブ	UCA591 ドライバが手動制御にカーブ旋回時にステアリングしない [Hazard575,Hazard577]	UCA592 ドライバが手動制御にカーブ旋回時に，逆方向のステアリングを与える [Hazard575,Hazard577]	UCA593 ドライバが手動制御にカーブ旋回時にステアリング，ブレーキ，アクセルを誤与える [Hazard575,Hazard577]	UCA594 ドライバが手動制御にカーブ旋回時にステアリングをすぐに戻してしまう [Hazard575,Hazard577]
		UCA597 ドライバが手動制御にカーブ旋回時に，ブレーキング，アクセルを与えない [Hazard575,Hazard577]	UCA598 ドライバが手動制御にカーブが必要な際に，ブレーキが必要な箇所でアクセルを，アクセルが必要な箇所でブレーキを与える [Hazard575,Hazard577]	UCA599 ドライバが手動制御にカーブ旋回時にステアリング，ブレーキ，アクセルを誤与える [Hazard575,Hazard577]	UCA600 ドライバが手動制御にカーブ旋回時にステアリングを必要以上に多く与える [Hazard575,Hazard577]
		UCA905 [Hazard575,Hazard577]	UCA906 ドライバが手動制御にカーブが必要な際に，逆にステアリング，ブレーキ，アクセルを与える [Hazard575,Hazard577]	UCA907 [Hazard575,Hazard577]	UCA908 ドライバが手動制御にカーブ旋回時にブレーキ，アクセルをすぐに戻してしまう [Hazard575,Hazard577]
		UCA910 [Hazard575,Hazard577]	UCA911 [Hazard575,Hazard577]	UCA912 [Hazard575,Hazard577]	UCA913 ドライバが手動制御にカーブが必要な際に，ブレーキ，アクセルを必要以上に多く与える [Hazard575,Hazard577]
制御状態：自動 設定 範囲：カーブ		UCA898 ドライバが自動制御にカーブ旋回時にステアリング，ブレーキ，アクセルを与えない [Hazard575,Hazard577]	UCA899 ドライバが自動制御にカーブが必要な際に逆方向にステアリングを与える [Hazard575,Hazard577]	UCA900 ドライバが自動制御にカーブ旋回時にステアリング，ブレーキ，アクセルを誤与える [Hazard575,Hazard577]	UCA901 ドライバが自動制御にカーブが必要な際にステアリング，ブレーキ，アクセルを必要以上に多く与える [Hazard575,Hazard577]
		UCA1138 [Hazard575,Hazard577]	UCA1139 ドライバが自動制御にカーブが必要な際に，ブレーキが必要な箇所でアクセルを，アクセルが必要な箇所でブレーキを与える [Hazard575,Hazard577]	UCA1140 ドライバが自動制御にカーブ旋回時にステアリング，ブレーキ，アクセルを誤与える [Hazard575,Hazard577]	UCA1141 ドライバが自動制御にカーブが必要な際にステアリング，ブレーキ，アクセルをすぐに戻してしまう [Hazard575,Hazard577]
		UCA1143 [Hazard575,Hazard577]	UCA1144 ドライバが自動制御にカーブが必要な際に正しくステアリング，ブレーキ，アクセルを与える [Hazard575,Hazard577]	UCA1145 [Hazard575,Hazard577]	UCA1146 [Hazard575,Hazard577]
制御状態：緊急回避 設定 範囲：カーブ		UCA603 ドライバが緊急回避制御にカーブ旋回時にステアリング，ブレーキ，アクセルを与えない [Hazard575,Hazard577]	UCA604 ドライバが緊急回避制御にカーブが必要な際に逆方向にステアリングを与える [Hazard575,Hazard577]	UCA605 ドライバが緊急回避制御にカーブ旋回時にステアリング，ブレーキ，アクセルを誤与える [Hazard575,Hazard577]	UCA606 ドライバが緊急回避制御にカーブが必要な際にステアリング，ブレーキ，アクセルを必要以上に多く与える [Hazard575,Hazard577]
		UCA1148 [Hazard575,Hazard577]	UCA1149 ドライバが緊急回避制御にカーブが必要な際にブレーキを与えない箇所でアクセルを，アクセルが必要な箇所でブレーキを与える [Hazard575,Hazard577]	UCA1150 ドライバが緊急回避制御にカーブ旋回時にステアリング，ブレーキ，アクセルを誤与える [Hazard575,Hazard577]	UCA1151 ドライバが緊急回避制御にカーブが必要な際にステアリング，ブレーキ，アクセルをすぐに戻してしまう [Hazard575,Hazard577]
		UCA1153 [Hazard575,Hazard577]	UCA1154 ドライバが緊急回避制御にカーブが必要な際に正しくカーブを与える [Hazard575,Hazard577]	UCA1155 [Hazard575,Hazard577]	UCA1156 [Hazard575,Hazard577]
制御状態：手動 設定 範囲：道路		UCA609 ドライバが手動制御に道路脇にステアリング，ブレーキ，アクセルをしない [Hazard575,Hazard577]	UCA610 ドライバが手動制御に道路のときにステアリングを与える [Hazard575,Hazard577]	UCA611 ドライバが手動制御に道路のときにステアリングを誤与える [Hazard575,Hazard577]	UCA612 ドライバが手動制御に道路のときにステアリングを必要以上に多く与える [Hazard575,Hazard577]
		UCA1168 [Hazard575,Hazard577]	UCA1169 ドライバが手動制御に道路のときにブレーキ，アクセルを与える(障害物がある場合CIバイパーになるが，これは障害物がある場合のコンテキストにおいて分析する) [Hazard575,Hazard577]	UCA1170 ドライバが手動制御に道路のときにステアリングを誤与える [Hazard575,Hazard577]	UCA1171 ドライバが手動制御に道路のときにステアリングをすぐに戻してしまう [Hazard575,Hazard577]
		UCA615 [Hazard575,Hazard577]	UCA616 [Hazard575,Hazard577]	UCA617 ドライバが手動制御に道路のときにブレーキ，アクセルを誤与える，あるいは，誤与える(障害物がある場合CIバイパーになるが，これは障害物がある場合のコンテキストにおいて分析する) [Hazard575,Hazard577]	UCA618 ドライバが手動制御に道路のときにブレーキ，アクセルを必要以上に多く与える(障害物がある場合CIバイパーになるが，これは障害物がある場合のコンテキストにおいて分析する) [Hazard575,Hazard577]

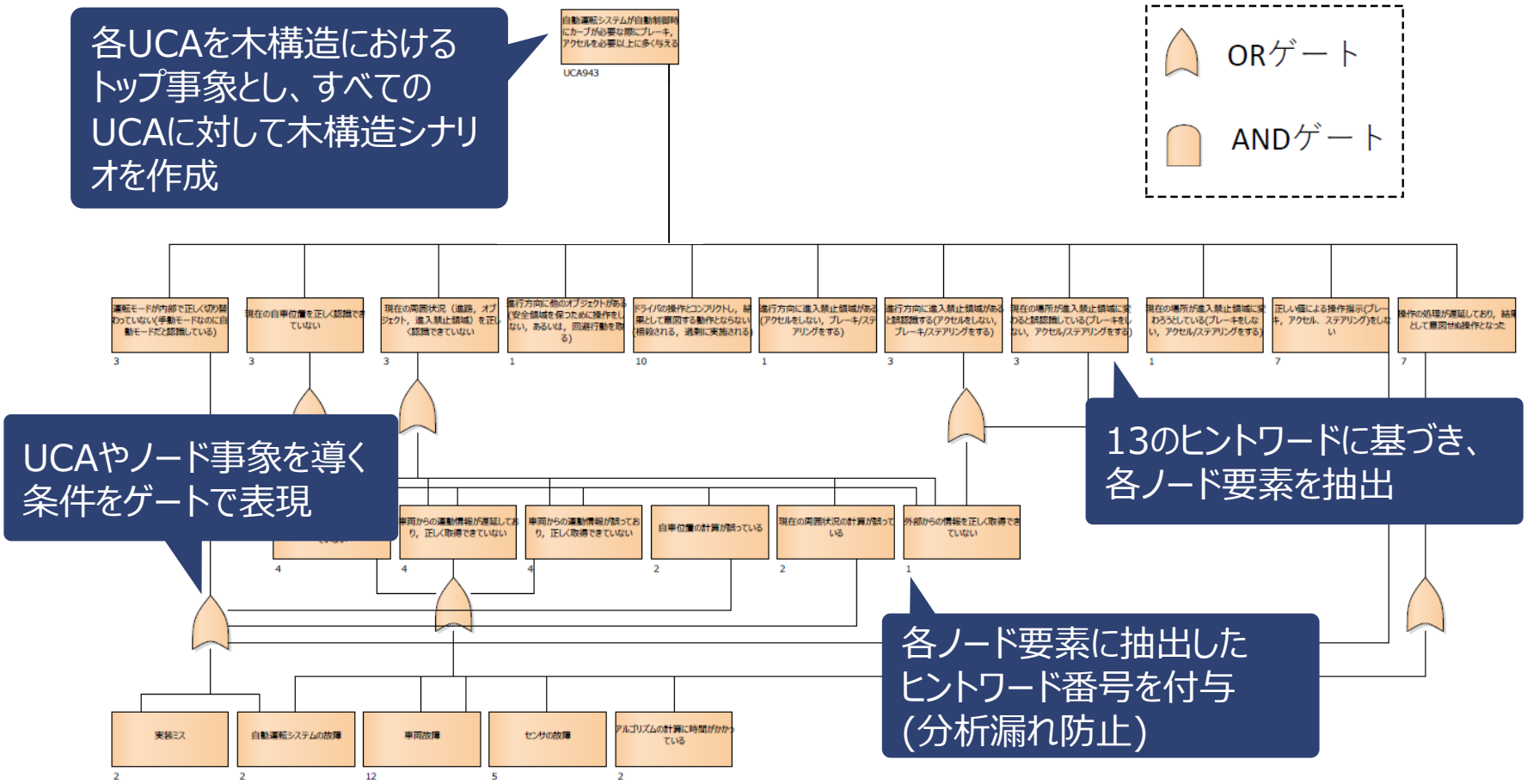
4-4. 評価

HITACHI
Inspire the Next

STAMP/STPA step2における木構造表現化

UCAテーブルに基づく木構造表現(一部抜粋)

各UCAを木構造における
トップ事象とし、すべての
UCAに対して木構造シナリ
オを作成



UCAやノード事象を導く
条件をゲートで表現

13のヒントワードに基づき、
各ノード要素を抽出

各ノード要素に抽出した
ヒントワード番号を付与
(分析漏れ防止)

4-5. 評価

HITACHI
Inspire the Next

- 損失シナリオの木構造表現化評価
  - 自動運転に対するUCAテーブルから損失シナリオの木構造表現化を実施
    - Step1で抽出したUCAをトップノードに配置
    - 13のヒントワードに基づいて、ノードを配置
      (各ノードには適用したヒントワード番号を付与)
    - UCAを導く条件をAND/ORゲートで表現

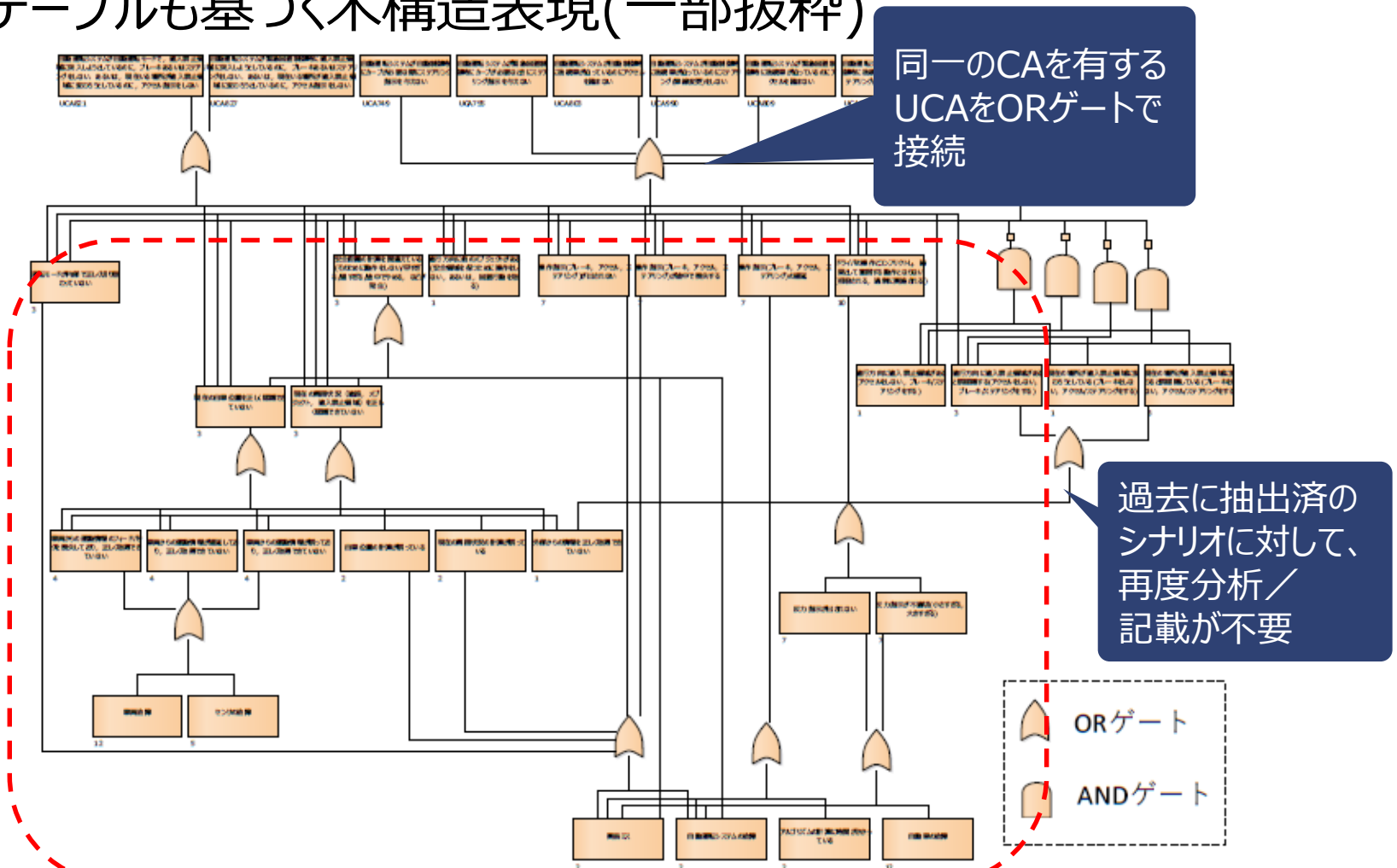
- Step1の各ガイドワードのUCAから抽出されるすべてのシナリオを木構造で表現できることが確認できた.
- ヒントワード情報をノードに付与することにより、分析漏れ箇所が明確になることを確認した.

4-6. 評価

HITACHI
Inspire the Next

同一システム内の異なるUCAの分析過程での再利用

UCAテーブルも基づく木構造表現(一部抜粋)



4-7. 評価

HITACHI
Inspire the Next

- 木構造表現における再利用性評価
  - 損失シナリオの木構造表現化で作成したUCAにおいて、同一のコントロールアクションを持つUCAに、作成済の木構造表現を適用
    - UCA(ツリーの最上位ノード)をORゲートでつなぐことにより、作成済シナリオの再利用を表現
    - ORゲートでつないだUCAは、分析済のUCAが持たないCAのみ分析

- 分析済のシナリオについては、改めてシナリオを分析／記述する必要がなくなり、分析時間を短縮できた.

HITACHI
Inspire the Next

目次

1. 背景
2. 課題
3. 提案手法
4. 評価
5. まとめ

5-1. まとめ

HITACHI
Inspire the Next

結論

- 課題
  - 分析済損失シナリオを再利用することが困難
  - 分析結果(損失シナリオ)の網羅性把握が困難
- 提案手法
  - 損失シナリオ(Step2)の木構造表現化
- 提案手法を自動運転システムにて試行し、課題に対する効果を評価
  - シナリオを木構造で表現できることを確認
  - ノードへのヒントワード付与により、分析漏れ(網羅性)把握が容易になることを確認
  - 同一CAを持つUCAへ分析済シナリオ適用より、分析時間の短縮を確認

今後の取り組み

- 似たSTAMPモデルを持つ他システムでの分析に既存分析結果再利用を試行
  - 分析時間など、損失シナリオの木構造表現化による効果を評価予定

HITACHI

Inspire the Next