

# 2017年度演習コースⅢ 成果発表

## 「セーフティ&セキュリティ開発のための 技術統合提案と事例作成」

|        |   |         |                      |
|--------|---|---------|----------------------|
| 主査     | : | 金子 朋子   | 情報セキュリティ大学院大学        |
| 副主査    | : | 高橋 雄志   | トレドシステム              |
| アドバイザー | : | 勅使河原 可海 | 東京電機大学               |
| メンバ    | : | 荒井 文昭   | キヤノンイメージングシステムズ      |
|        |   | 大森 淳夫   | パイオニア                |
|        |   | 神田 圭    | 日立ソリューションズ           |
|        |   | 邱 章傑    | パナソニック               |
|        |   | 久連石 圭   | 東芝                   |
|        |   | 久木元 豊   | テックスエンジニアリングソリューションズ |
|        |   | 柴引 涼    | メタテクノ                |
|        |   | 太郎田 裕介  | 東京海上日動システムズ          |
|        |   | 中嶋 良秀   | ノーリツ                 |
|        |   | 西村 伸吾   | 富士ゼロックス              |
|        |   | 細谷 雅樹   | 東光高岳                 |
|        |   | 松本 江里加  | ダイキン工業               |

# 演習Ⅲ セーフティ&セキュリティ開発 実績

| 回  | 日時          | 講演テーマ                                         | 講演者               | 演習             |
|----|-------------|-----------------------------------------------|-------------------|----------------|
| 1  | 5/12        | セーフティ・セキュリティ開発のポイント                           | 金子朋子              | なし             |
| 2  | 6/9         | IoT時代のリスク評価・リスクコミュニケーション                      | 東京電機大学<br>佐々木良一教授 | アシュアランス<br>ケース |
| 3  | 7/6,7<br>合宿 | セキュリティ標準とセキュリティ設計<br>ネットワークの信頼性とセキュリティアーキテクチャ | 高橋 雄志<br>勅使河原 可海  | セキュリティ設<br>計演習 |
| 4  | 8/3         | 第1回臨時会 論文化検討 脅威分析研究会での講演聴講                    |                   |                |
| 5  | 9/14,15     | ソフトウェア品質シンポジウム（第2回臨時会 論文作成チーム分け）              |                   |                |
| 6  | 10/13       | STAMP/STPA, STPA-Sec<br>セーフティ・セキュリティリスク手法     | 金子朋子              | 事例作成検討         |
| 7  | 11/17       | トラストと安心・安全について                                | 津田塾大学<br>村山優子教授   | 事例作成を通<br>じた演習 |
| 8  | 12/15       | セキュリティ要求の保証概論と機能要件                            | 金子朋子              | 事例作成を通<br>じた演習 |
| 9  | 1/12        | GSNの開発検証業務への応用事例                              | JAXA梅田浩貴氏         | 論文作成           |
| 10 | 2/1         | 第3回臨時会 論文作成 成果発表会準備                           |                   |                |
| 11 | 2/23        | 成果発表会                                         |                   |                |

# 2017年度演習コースⅢ 成果発表

## 「セーフティ&セキュリティ開発のための 技術統合提案と事例作成」

|        |   |         |                      |
|--------|---|---------|----------------------|
| 主査     | : | 金子 朋子   | 情報セキュリティ大学院大学        |
| 副主査    | : | 高橋 雄志   | トレドシステム              |
| アドバイザー | : | 勅使河原 可海 | 東京電機大学               |
| メンバ    | : | 荒井 文昭   | キヤノンイメージングシステムズ      |
|        |   | 大森 淳夫   | パイオニア                |
|        |   | 神田 圭    | 日立ソリューションズ           |
|        |   | 邱 章傑    | パナソニック               |
|        |   | 久連石 圭   | 東芝                   |
|        |   | 久木元 豊   | テックスエンジニアリングソリューションズ |
|        |   | 柴引 涼    | メタテクノ                |
|        |   | 太郎田 裕介  | 東京海上日動システムズ          |
|        |   | 中嶋 良秀   | ノーリツ                 |
|        |   | 西村 伸吾   | 富士ゼロックス              |
|        |   | 細谷 雅樹   | 東光高岳                 |
|        |   | 松本 江里加  | ダイキン工業               |

# 目次

1. はじめに
2. 開発プロセス説明
3. 開発プロセス適用事例紹介
  1. 対象システム
  2. ハザード抽出プロセス
  3. ハザード分析・対策立案プロセス
  4. 妥当性確認プロセス
4. 得られた知見, まとめ
5. 最後に

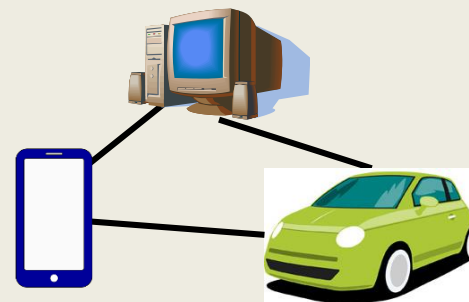
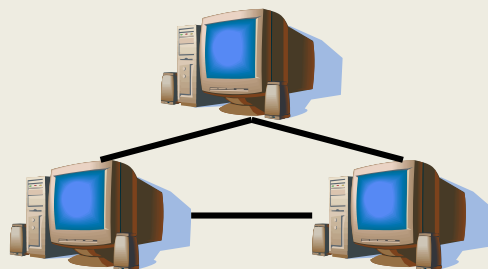
# 目次

1. はじめに
2. 開発プロセス説明
3. 開発プロセス適用事例紹介
  1. 対象システム
  2. ハザード抽出プロセス
  3. ハザード分析・対策立案プロセス
  4. 妥当性確認プロセス
4. 得られた知見, まとめ
5. 最後に

# 時代の流れ

## 1. はじめに

### ● 時代の流れ



セーフティ  
の  
時代

セキュリティ  
の  
時代

セーフティ  
&  
セキュリティ  
の  
時代

機器は独立で  
ネットワークのない  
時代

ネットワークが繋がり  
他の機器に影響が  
有る時代

IoT時代の到来により  
あらゆる機器が  
影響を及ぼし合う時代

# 質問

## 1. はじめに

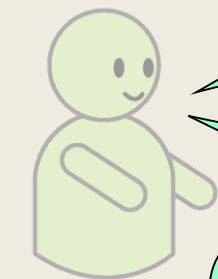
### ● 皆さんの会社では，こんなやり取りありませんか？

#### ＜セーフティ系担当者の場合＞

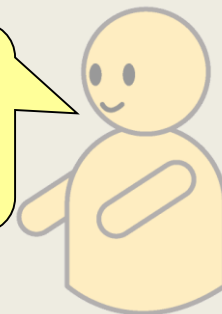
N氏：スマホと連動できるように，派生開発で，セキュリティ要件を追加してほしいよ！

Y氏：セキュリティなんて，専門外です．  
専門部隊がやればいいじゃないですか？

N氏：最近，IoT系の依頼が多くて，  
当分対応してもらえないんだよ．  
元々，セキュリティを専門にしている  
人員が少ないからねえ・・・．



上司 N



セーフティ系  
担当者 Y

# 質問

## 1. はじめに

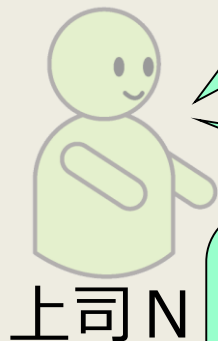
### ● 皆さんの会社では，こんなやり取りありませんか？

#### ＜セキュリティ系担当者の場合＞

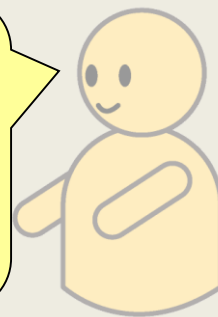
N氏：スマホを使って，  
新たなサービスを提供してほしい。

Y氏：じゃあ，必要そうな制御信号を  
送れるように作りますね。  
セキュリティ面について，ご心配なく。

N氏：この制御信号送ったらダメだよ～！  
万が一があった時，この制御信号によって，  
ユーザーに被害を与えるかもしれないよ！



上司N



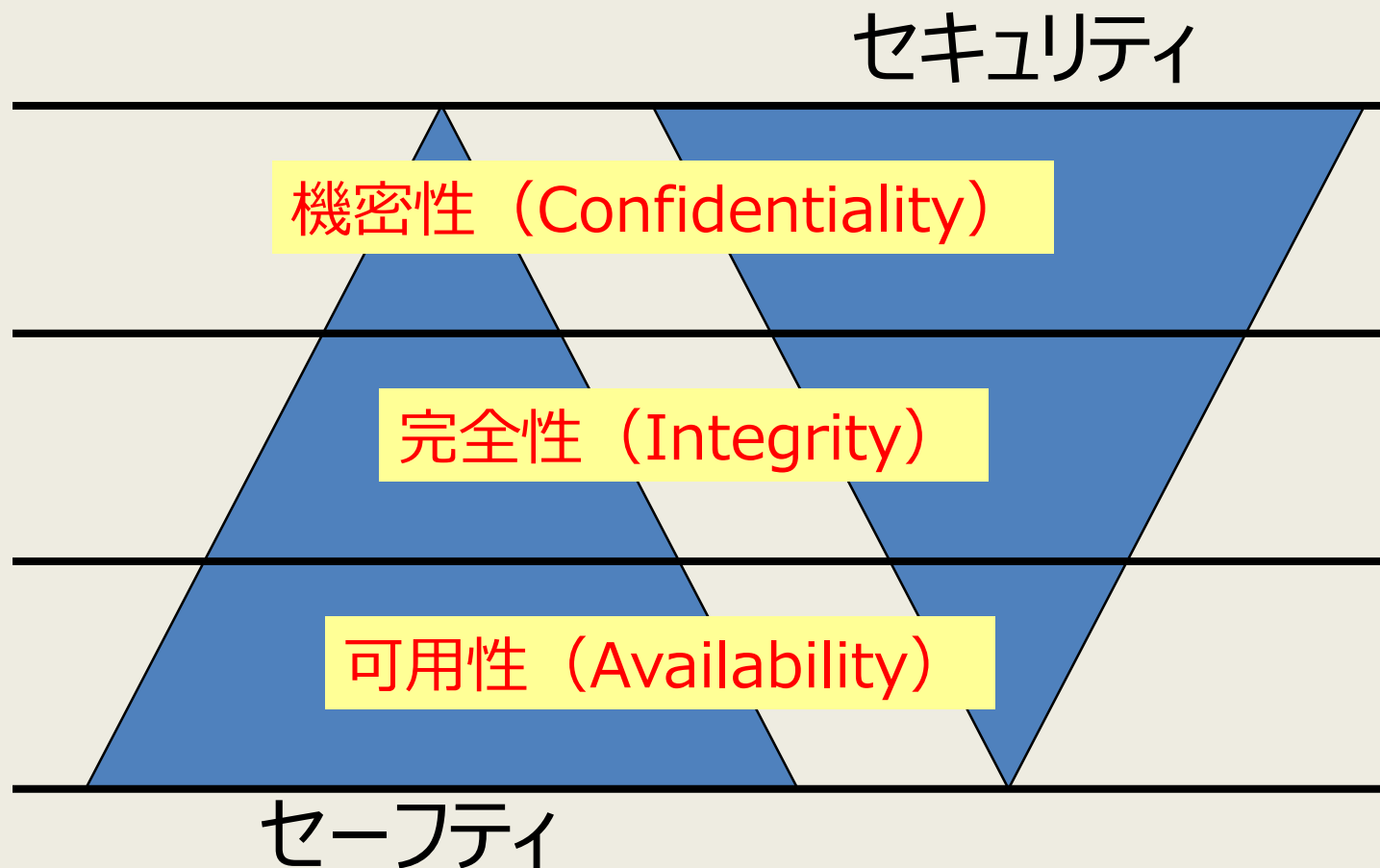
セキュリティ系  
担当者Y



# 視点の違い

## 1. はじめに

### ● セーフティとセキュリティの視点は違う



# 本日お伝えしたいこと

## 1. はじめに

IoT時代において、

1. セーフティに関する開発方法論だけなら、  
情報の機密性を損なう可能性が上がる。
2. セキュリティに関する開発方法論だけなら、  
利便性や機能性を損なう可能性が上がる。
3. セーフティとセキュリティを、まとめて分析したら、  
情報量が多くなりすぎて、整理や説明に困る。

# 本日お伝えしたいこと

## 1. はじめに

IoT時代において、

1. セーフティに関する開発方法論だけなら、  
情報の機密性を損なう可能性が上がる。
2. セキュリティに関する開発方法論だけなら、  
利便性や機能性を損なう可能性が上がる。
3. セーフティとセキュリティを、まとめて分析したら、  
情報量が多くなりすぎて、整理や説明に困る。

セーフティとセキュリティ、  
それぞれバランスの取れた開発方法論ってどうするの？

# 目次

1. はじめに
2. 開発プロセス説明
3. 開発プロセス適用事例紹介
  1. 対象システム
  2. ハザード抽出プロセス
  3. ハザード分析・対策立案プロセス
  4. 妥当性確認プロセス
4. 得られた知見, まとめ
5. 最後に

## (参考) 関連用語

### 2. 開発プロセスの説明

## <セーフティ系> (1 / 3)

### FTA

- Fault Tree Analysis
- 発生が好ましくない事象について、発生経路、発生原因及び発生確率をフォールトの木を用いて解析

### FMEA

- Failure Mode and Effect Analysis
- 不完全な設計や潜在的な欠点を見出すために、構成要素の故障モードとその上位アイテムへの影響を解析

## (参考) 関連用語

### 2. 開発プロセスの説明

## <セーフティ系> (2 / 3)

### STAMP

- **S**ystems-**T**heoretic **A**ccident **M**odel and **P**rocesses
- システム理論に基づく事故モデル

### STPA

- **S**ystem-**T**heoretic **P**rocess **A**nalysis
- STAMPアクシデントモデルを前提とする,  
システムのハザード要因を分析する新しい安全解析手法
- MITのNancy Leveson教授が提唱

## (参考) 関連用語

### 2. 開発プロセスの説明

## <セーフティ系> (3 / 3)

### ASIL分析

- Automotive Safety Integrity Level
- 車載電子システムで起こり得るさまざまなハザードを、回避するために、達成しなければならない安全性レベル.
- 以下, 3つの評価指標により、ハザード要因を評価
  - 過酷度クラス
  - 発生頻度クラス
  - 回避可能性クラス

## (参考) 関連用語

### 2. 開発プロセスの説明

#### <セキュリティ系>

##### - コモンクライテリア

- Common Criteria(CC)

セキュリティ評価における国際標準規格

##### - CC-Case

- ITセキュリティ評価の国際標準であるコモンクライテリアとアシュアランスケースを用い,  
セキュリティ仕様を顧客と合意の上で決定する開発方法論
- 論理モデル：論理的プロセスによって、保証全体像を示す
- 具体モデル：製品ごとの具体的な特性を持った,  
リスクに対する検証をするアシュアランスケース



# 目次

1. はじめに
2. 開発プロセス説明
3. 開発プロセス適用事例紹介
  1. 対象システム
  2. ハザード抽出プロセス
  3. ハザード分析・対策立案プロセス
  4. 妥当性確認プロセス
4. 得られた知見, まとめ
5. 最後に

# 安全なIoTシステムを目指す

## 2. 開発プロセスの説明

### セキュリティ・バイ・デザイン

企画・  
要件定義

設計

実装

検証・評価

保守・運用

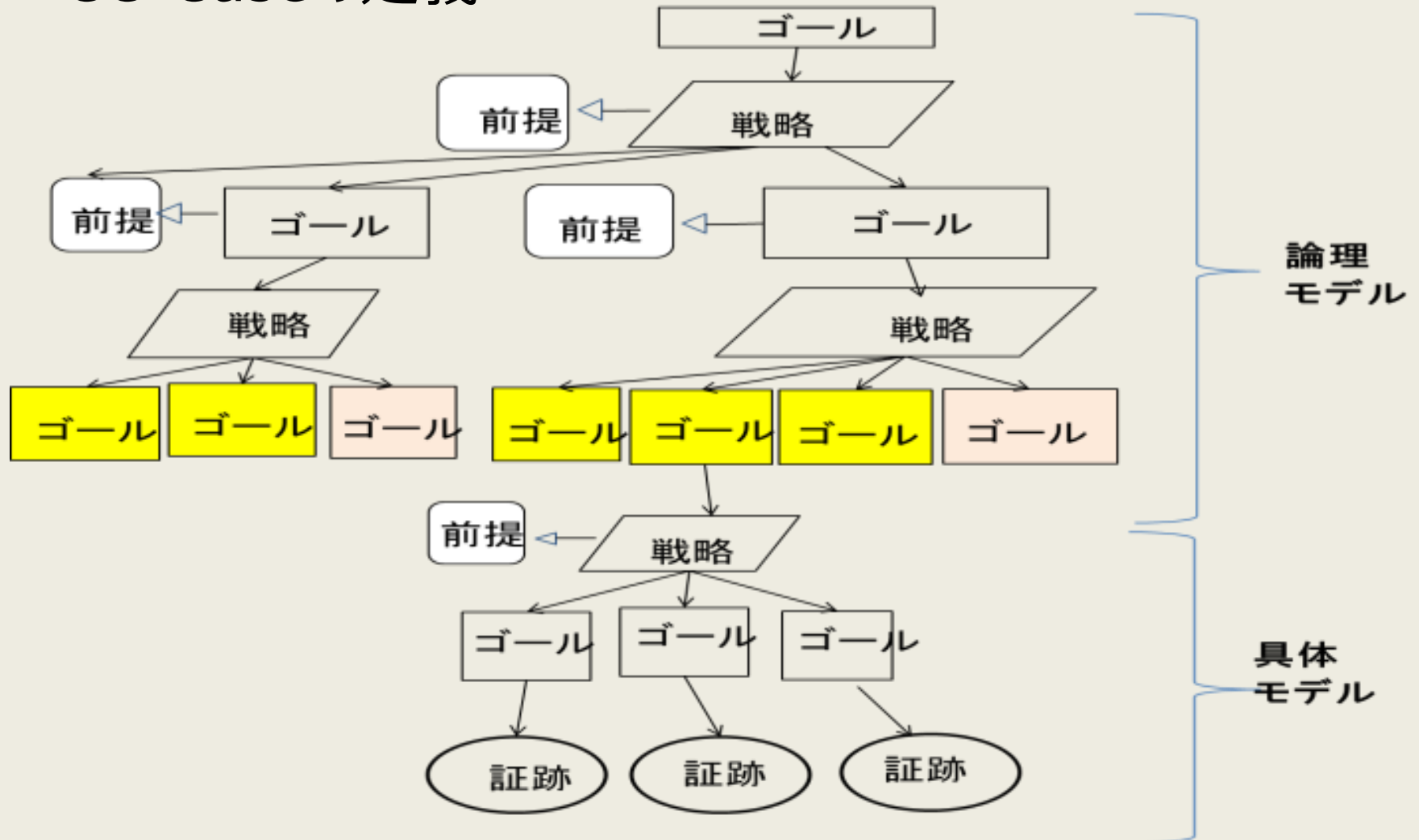
- 企画・要件定義、設計段階という上流工程から情報セキュリティを確保するための方策
- IoT時代において、セキュリティ上の脅威によって、多大な被害を及ぼす可能性が出ているため、早期対応が重要。

CC-Caseをセーフティとセキュリティ、  
それぞれを考慮した開発方法論として適用する

# 論理モデルと具体モデル

## 2. 開発プロセスの説明

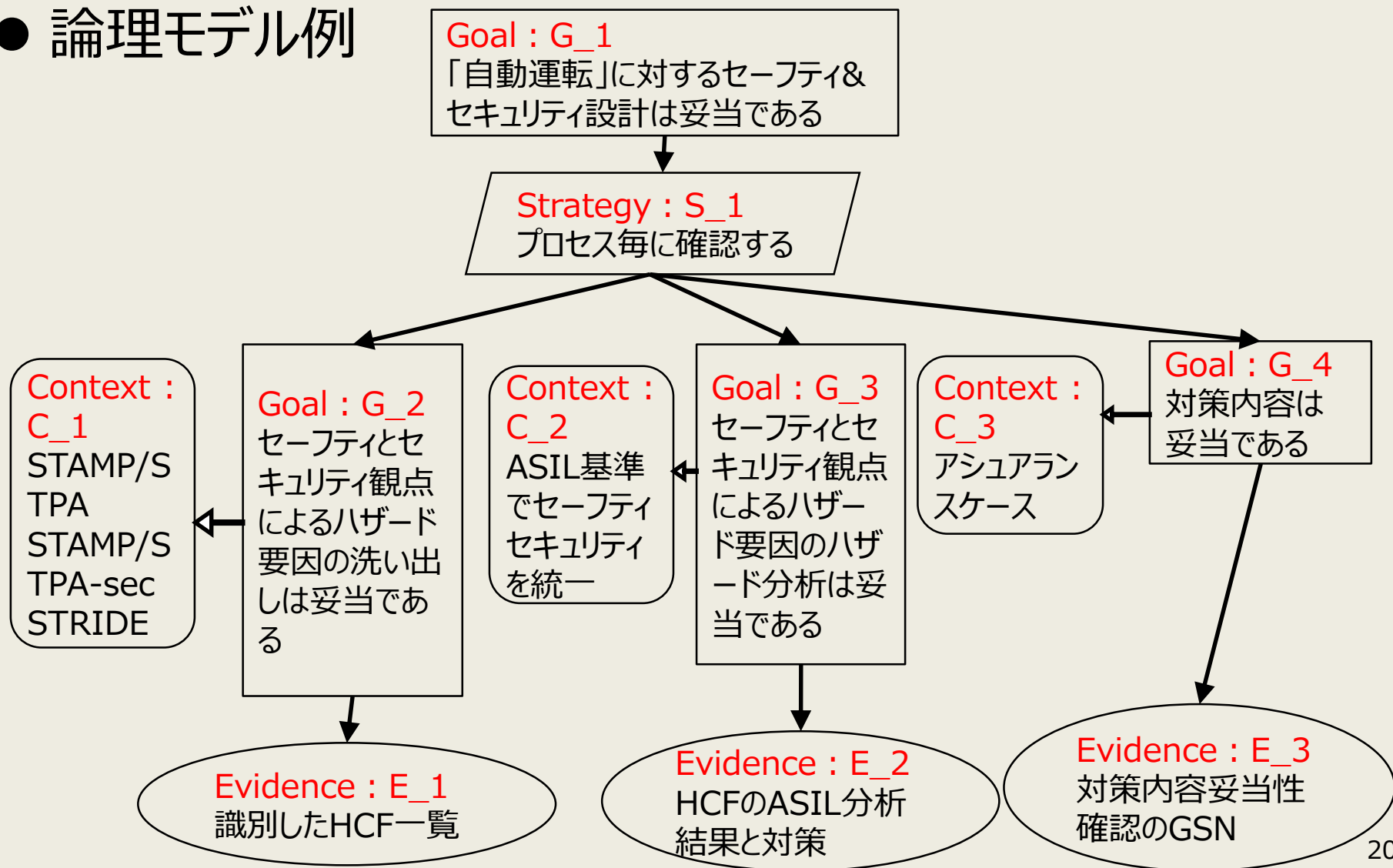
### ● CC-Caseの定義



# 保証全体像

## 2. 開発プロセスの説明

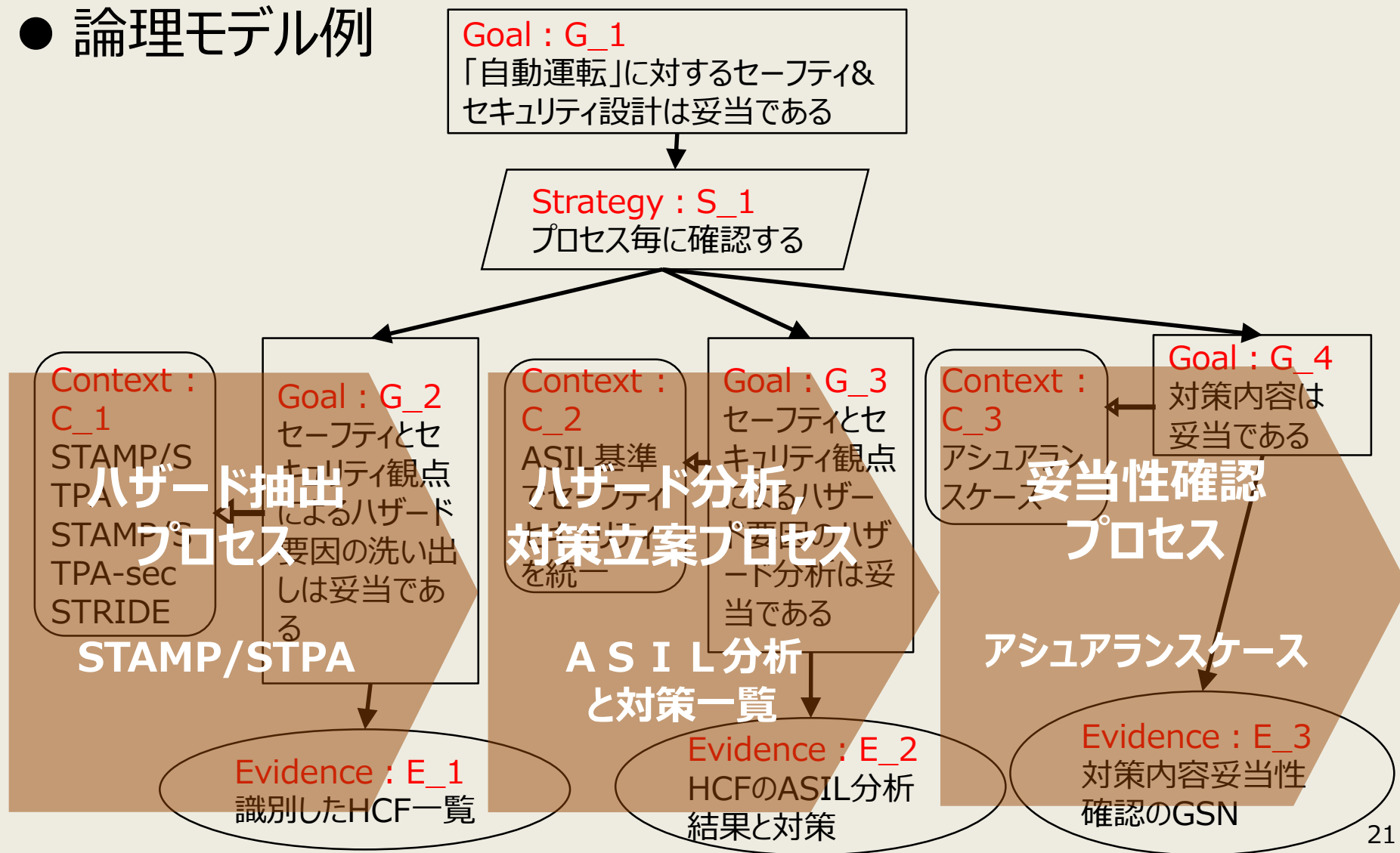
### ● 論理モデル例



# 保証全体像

## 2. 開発プロセスの説明

### ● 論理モデル例



# 目次

1. はじめに
2. 開発プロセス説明
3. 開発プロセス適用事例紹介
  1. 対象システム
  2. ハザード抽出プロセス
  3. ハザード分析・対策立案プロセス
  4. 妥当性確認プロセス
4. 得られた知見, まとめ
5. 最後に

# 目次

1. はじめに
2. 開発プロセス説明
3. 開発プロセス適用事例紹介
  1. 対象システム
  2. ハザード抽出プロセス
  3. ハザード分析・対策立案プロセス
  4. 妥当性確認プロセス
4. 得られた知見, まとめ
5. 最後に

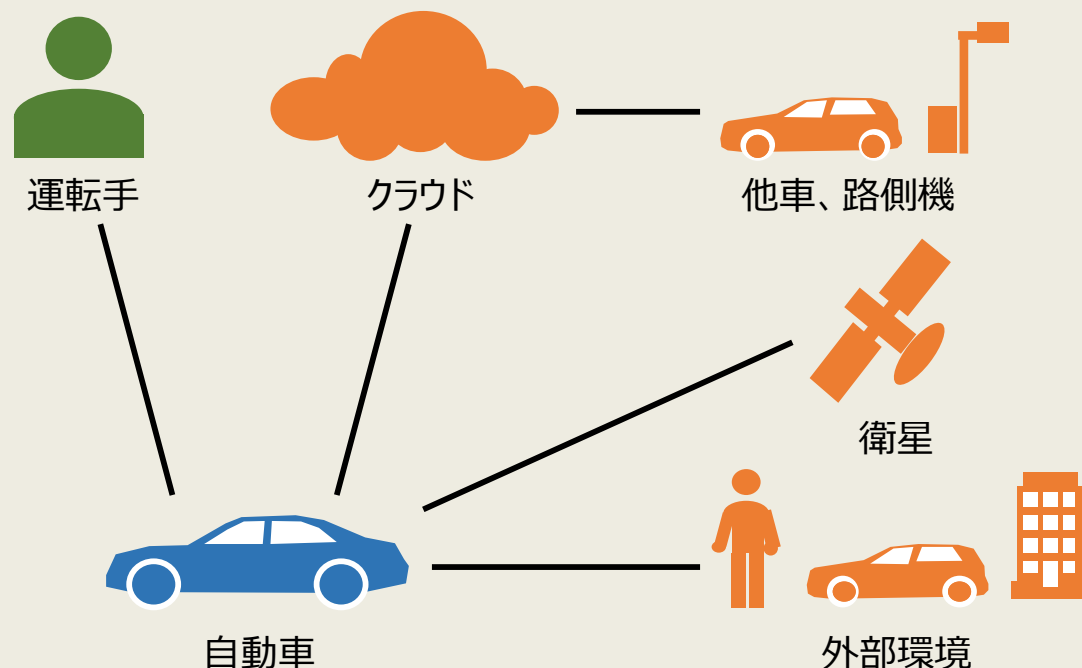
# 対象システム

## 3.1. 対象システム

### 対象システム：

#### ネットワークに接続された レベル3の自動運転自動車

- 通常，自動車は自動運転で走行する
- システムが扱いきれない場合，運転手が運転する





# 目次

1. はじめに
2. 開発プロセス説明
3. 開発プロセス適用事例紹介
  1. 対象システム
  2. ハザード抽出プロセス
  3. ハザード分析・対策立案プロセス
  4. 妥当性確認プロセス
4. 得られた知見, まとめ
5. 最後に

# STAMP/STPA 背景

## 3.2. ハザード抽出 プロセス

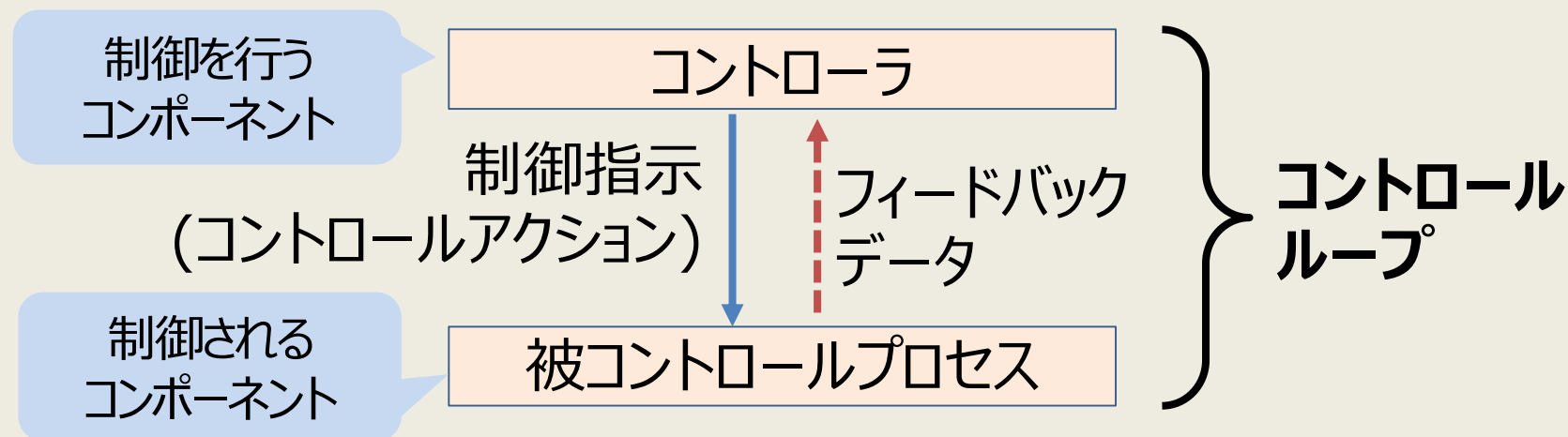
### 背景

|        | 従来                                                                                                                      | 現在                                                                                                                                   |
|--------|-------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| システム   | <ul style="list-style-type: none"><li>- システムは小規模</li><li>- ハードウェア主体</li></ul>                                           | <ul style="list-style-type: none"><li>- システムは大規模/複雑</li><li>- ソフトウェア主体</li><li>- システム間のコミュニケーションミスによる障害が増加</li></ul>                 |
| 安全解析手法 | <ul style="list-style-type: none"><li>- 従来のアクシデントモデル：機器の故障や人間のオペレーションミスにシステムアクシデントの根本原因がある</li><li>- FTA FMEA</li></ul> | <ul style="list-style-type: none"><li>- 新しいアクシデントモデル<br/>STAMP：アクシデントは相互作用が適切に働かないことによって起きる(次頁)</li><li>- STPA：STAMPに基づく手法</li></ul> |

# STAMP/STPA 考え方

## 3.2. ハザード抽出 プロセス

アクシデントは相互作用が適切に働かないことによって起きる

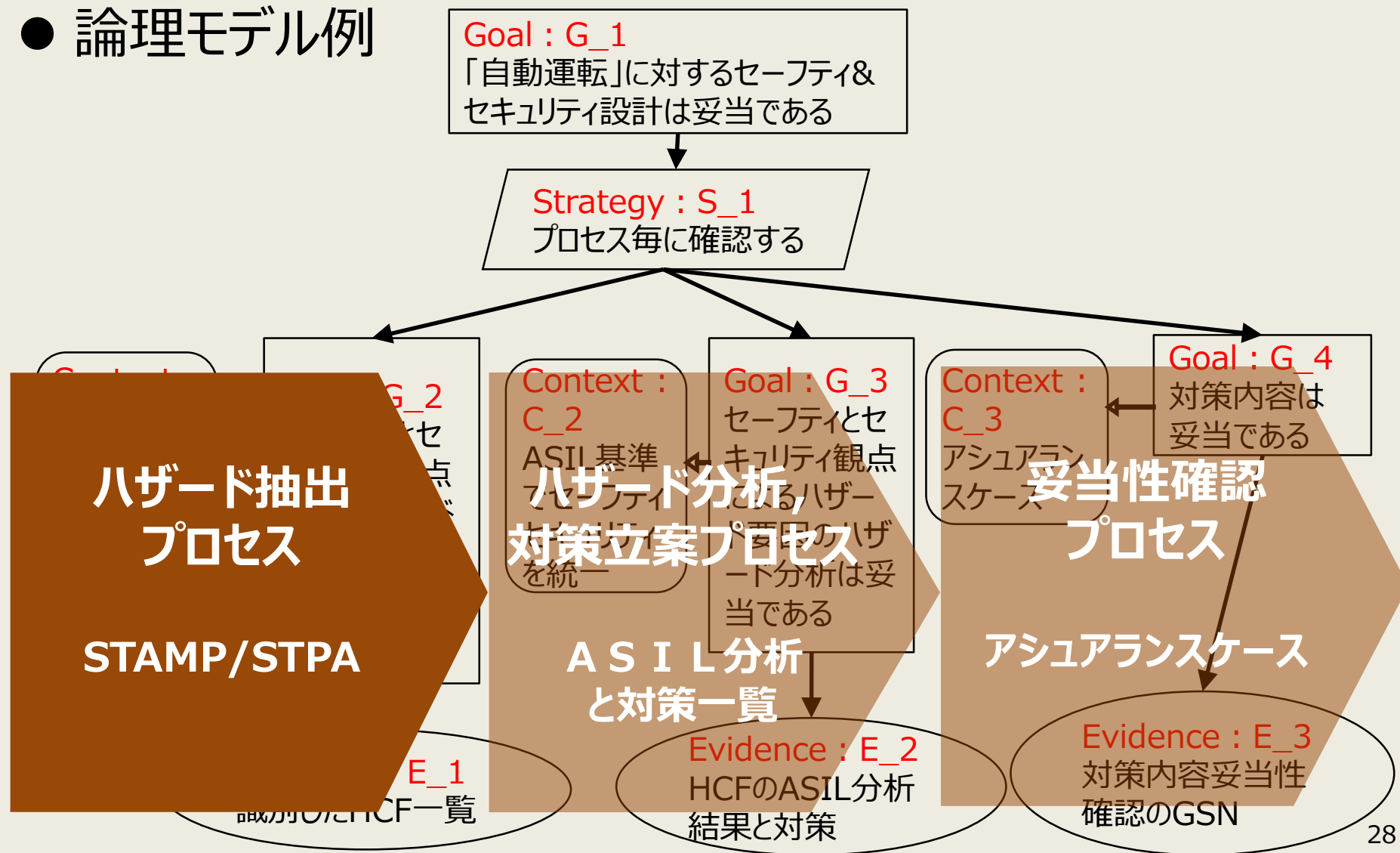


- コントロールループが階層となり、システムが構築される
- 制御指示(コントロールアクション)が適切に与えられないためにアクシデントが起こる

# 保証全体像

## 3.2. ハザード抽出 プロセス

### ● 論理モデル例



# STAMP/STPA 概要手順

## 3.2. ハザード抽出 プロセス

**Step 0 : (準備1)**  
**アクシデント, ハザード, 安全制約の識別**

**Step 0 : (準備2)**  
**コントロールストラクチャーの構築**

**Step 1 :**  
**非安全なコントロールアクション (UCA) の抽出**

**Step 2 :**  
**ハザード要因 (HCF) の特定**

# STAMP/STPA 概要手順

## 3.2. ハザード抽出 プロセス

**Step 0 : (準備1)**  
**アクシデント, ハザード, 安全制約の識別**

**Step 0 : (準備2)**  
**コントロールストラクチャーの構築**

**Step 1 :**  
**非安全なコントロールアクション (UCA) の抽出**

**Step 2 :**  
**ハザード要因 (HCF) の特定**

## Step0 (準備1)

### 3.2. ハザード抽出 プロセス

アクシデント：損失  
(Loss)につながるような  
望ましくない事象  
→分析の目的

ハザード：  
アクシデントに  
つながるシステ  
ムの状態

安全制約：ハザードから  
導かれるシステムを安全  
に保つための要件もしくは  
制約→step1へ入力

## 作成した成果物

| アクシデント<br>(Loss)                                  | ハザード (Hazard)                                       | 安全制約<br>(Safety Constraints)                          |
|---------------------------------------------------|-----------------------------------------------------|-------------------------------------------------------|
| (A1)自動車<br>が外部環境(歩<br>行者/他の車/<br>周辺物)と衝突<br>/接触する | (H1-1) 自動車<br>が、ブレーキを<br>かけても、外部<br>環境の前で停止<br>できない | (SC1-1) 自動車<br>が、外部環境と<br>衝突しないよう<br>にブレーキをかける        |
|                                                   | (H1-2) ブレー<br>キがかからない                               | (SC1-2) 運転手<br>と自動車の両方<br>がブレーキをかけ<br>られない状態に<br>ならない |

人命・財産喪失という重大アクシデントに限定

# STAMP/STPA 概要手順

## 3.2. ハザード抽出 プロセス

Step 0 : (準備1)  
アクシデント, ハザード, 安全制約の識別

Step 0 : (準備2)  
コントロールストラクチャーの構築

Step 1 :  
非安全なコントロールアクション (UCA) の抽出

Step 2 :  
ハザード要因 (HCF) の特定

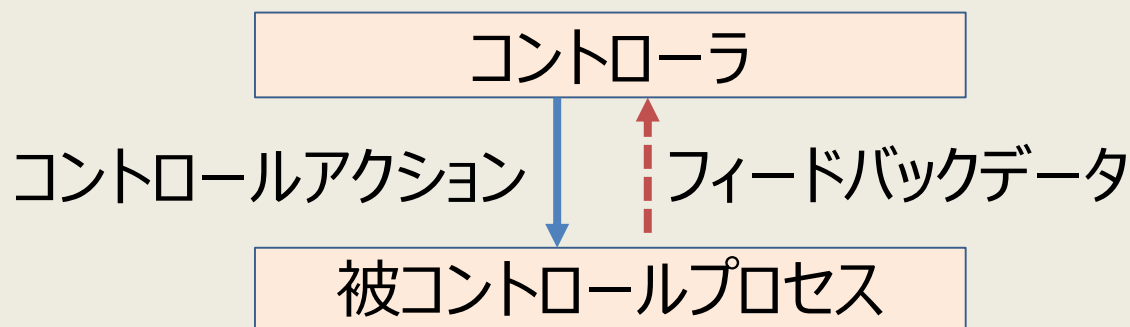


## Step0 (準備2)

### 3.2. ハザード抽出 プロセス

## Step 0 : (準備2) コントロールストラクチャーの構築

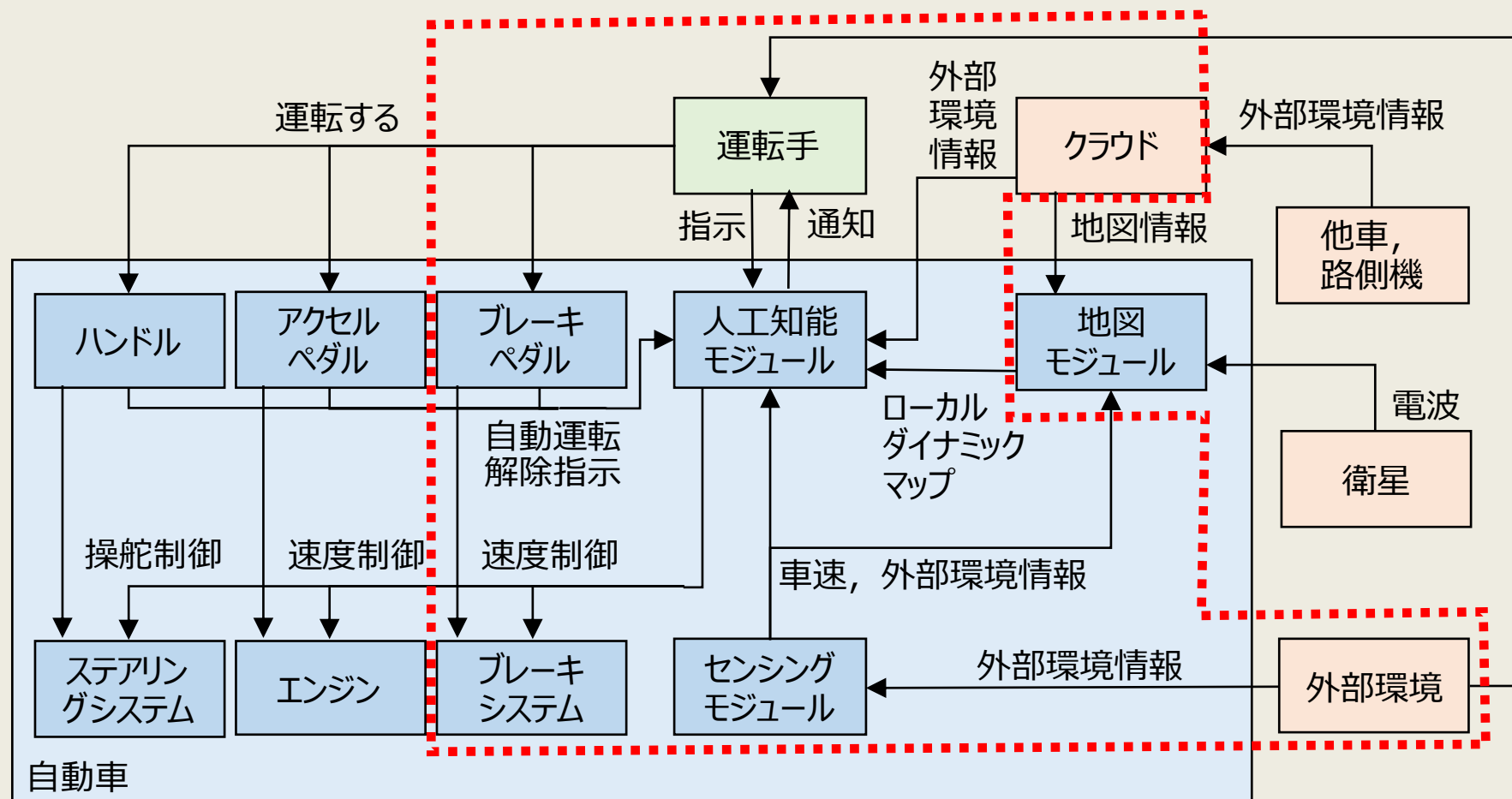
- 目的 : (相互作用が適切に働かないところを見つけるために) コンポーネント間の相互作用を明確化する
- コントロールストラクチャー(制御構造図)で構成要素間の相互作用を表す



# Step0 (準備2)

## 3.2. ハザード抽出 プロセス

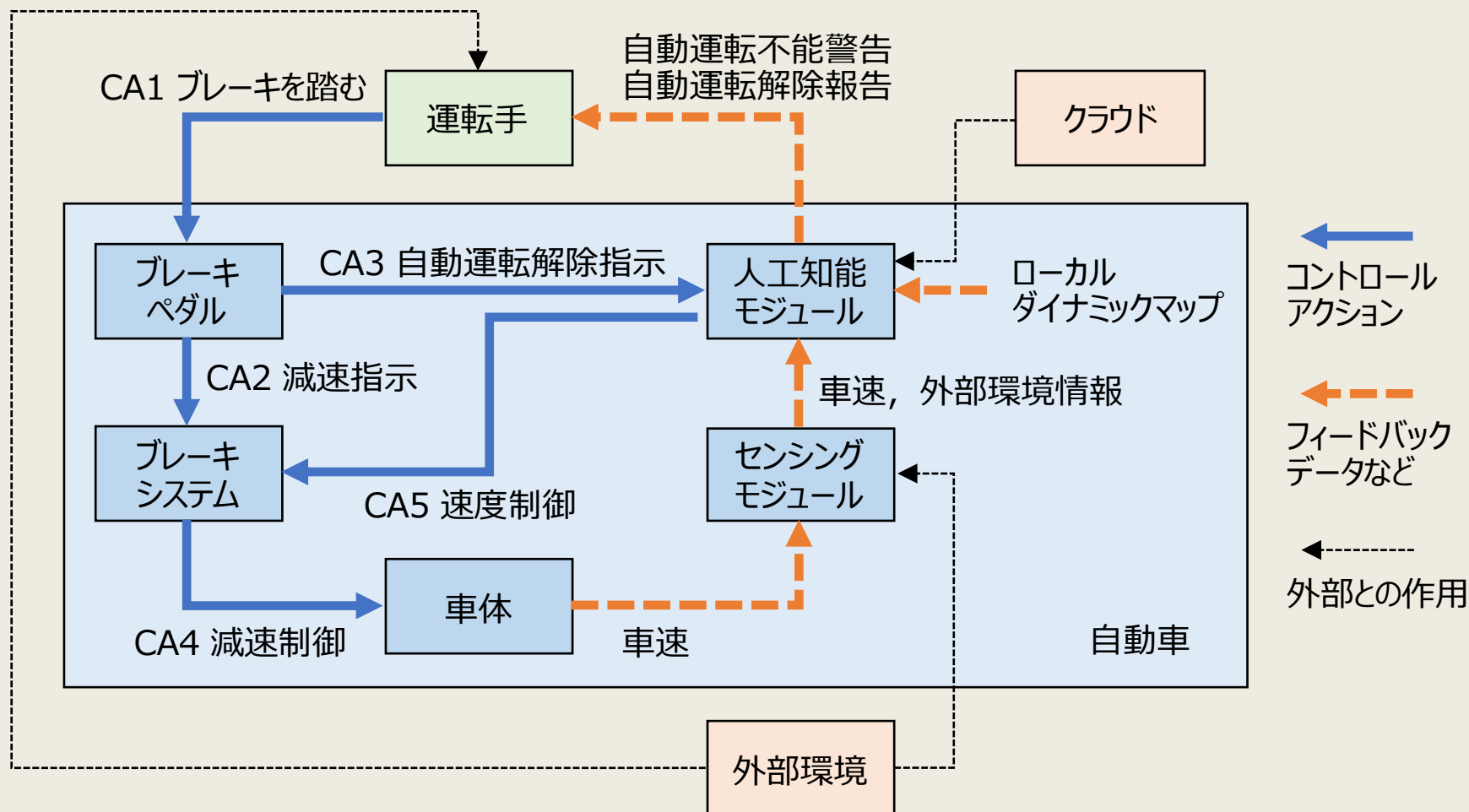
### 規定した自動車のシステムアーキテクチャ



# Step0 (準備2)

## 3.2. ハザード抽出 プロセス

### 作成したコントロールストラクチャー



# STAMP/STPA 概要手順

## 3.2. ハザード抽出 プロセス

Step 0 : (準備1)  
アクシデント, ハザード, 安全制約の識別

Step 0 : (準備2)  
コントロールストラクチャーの構築

Step 1 :  
非安全なコントロールアクション (UCA) の抽出

Step 2 :  
ハザード要因 (HCF) の特定

# Step1 : UCAの抽出

## 3.2. ハザード抽出 プロセス

### Step 1 : 非安全なコントロールアクション (UCA) の抽出

- UCA : **U**nsafe **C**ontrol **A**ction  
非安全なコントロールアクション  
ハザードにつながるコントロールアクション
- 目的 : ハザードにつながり得る, 適切ではないコントロールアクションを識別する
- 手順 : 4個のガイドワードを当てはめて, 安全制約(SC)違反となれば, UCAとする
  - (1) コントロールアクションが与えられない
  - (2) 不適切なコントロールアクションが与えられる
  - (3) コントロールアクションが早過ぎる, 遅過ぎる
  - (4) コントロールアクションの早過ぎる停止, 長過ぎる適用

# Step1 : UCAの抽出

## 3.2. ハザード抽出 プロセス

### 作成した成果物

与えられない  
とハザード

与えられる  
とハザード

早過ぎ、  
遅過ぎ

早過ぎる停止、  
長過ぎる適用

| コントロール<br>アクション            | Not<br>Providing                                                            | Providing<br>causes<br>hazard                                                  | Too early /<br>Too late                                                           | Stop too soon<br>/ Applying too<br>long                                               |
|----------------------------|-----------------------------------------------------------------------------|--------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| CA1<br>運転手が<br>ブレーキ<br>を踏む | (UCA1-N) 運<br>転手がブレーキ<br>を踏まないで危<br>険回避ができず、<br>外部環境と衝突<br>する (SC1-2)<br>違反 | (UCA1-P) 運<br>転手が誤った力<br>加減でブレーキ<br>操作を行うと、<br>減速が弱く外部<br>環境と衝突する<br>(SC1-1)違反 | (UCA1-T) 運<br>転手のブレー<br>キが遅すぎる<br>場合、危険<br>回避ができず、<br>外部環境と衝<br>突する (SC1-<br>1)違反 | (UCA1-S) 運<br>転手がブレーキ<br>を踏む時間が短<br>すぎる場合、危<br>険回避ができず<br>外部環境と衝<br>突する (SC1-<br>1)違反 |
| CA2 減速<br>指示               |                                                                             |                                                                                |                                                                                   |                                                                                       |

ガイドワードを当てはめて、安全制約違反(SC)となれば、UCAとする

# STAMP/STPA 概要手順

## 3.2. ハザード抽出 プロセス

Step 0 : (準備1)  
アクシデント, ハザード, 安全制約の識別

Step 0 : (準備2)  
コントロールストラクチャーの構築

Step 1 :  
非安全なコントロールアクション (UCA) の抽出

Step 2 :  
ハザード要因 (HCF) の特定

## Step2 : ハザード要因の特定

### 3.2. ハザード抽出 プロセス

## Step 2 : ハザード要因（HCF）の特定

- HCF : **H**azard **C**ausal **F**actor  
ハザード要因. ハザードを引き起こす原因
- 目的 : 抽出したUCA について, どのような原因によってハザードと成り得るのか (安全制約違反になるか) を特定する
- 手順 : ヒントワードを当てはめて, ハザードになるかどうかを考える.  
ハザードになる場合, どうなったらハザードになって, アクシデントにつながるかを考えて, ハザード要因を特定する



## ヒントワード①

### 3.2. ハザード抽出 プロセス

## STPAのヒントワード

- (1) コントロール入力や外部情報の誤りや喪失
- (2) 不適切なコントロールアルゴリズム
- (3) 不整合, 不完全, または不正確なプロセスモデル. 不適切な操作.
- (4) コンポーネントの不具合. 経年による変化.
- (5) 不適切なフィードバック, あるいはフィードバックの喪失. フィードバックの遅れ
- (6) 不正確な情報の供給, または情報の欠如. 測定の不正確性. フィードバックの遅れ
- (7) 操作の遅れ
- (8) 不適切または無効なコントロールアクション, コントロールアクションの喪失
- (9) コントロールアクションの衝突. プロセス入力の喪失または誤り
- (10) 未確認, または範囲外の障害
- (11) システムにハザードを引き起こすプロセス出力

## ヒントワード②

### 3.2. ハザード抽出 プロセス

## STPA-Sec

- STPAにセキュリティの要素を組み込んだ安全解析手法
- セキュリティ上の脅威抽出に必要な分析の視点が追加

### 青字部分がSTPA-Secで追加されたヒントワード

- (5) **悪い形状**・不適切なフィードバック, あるいはフィードバックの喪失. フィードバックの遅れ
- (6) **部分的な情報**・不正確な情報の供給, または情報の欠如. 測定の不正確性. フィードバックの遅れ
- (7) 操作の遅れ, **部分的・悪い形状のオペレーション**
- (8) **悪い形状**・不適切または無効なコントロールアクション, コントロールアクションの喪失

# ヒントワード③

## 3.2. ハザード抽出 プロセス

### STRIDE : マイクロソフト社が定義する脅威モデル をヒントワードとして使用

|   |                           |        |                                               |
|---|---------------------------|--------|-----------------------------------------------|
| S | Spoofing<br>Identity      | なりすまし  | コンピュータに対し, 他のユーザを装うこと                         |
| T | Tampering                 | 改ざん    | データを意図的に操作すること                                |
| R | Repudiation               | 否認     | ユーザがあるアクションを行ったことを否認し, 相手はこのアクションを証明する方法がないこと |
| I | Information<br>Disclosure | 情報の暴露  | アクセス権限を持たない個人に情報が公開されていること                    |
| D | Denial of<br>Service      | サービス不能 | 攻撃により正規へのユーザへのサービスが中断される                      |
| E | Elevation of<br>Privilege | 権限の昇格  | 権限のないユーザがアクセス権限を得ること                          |

## Step2: ハザード要因の特定

### 3.2. ハザード抽出 プロセス

## 作成した成果物

# STRIDE

[illegible]

## Step2：ハザード要因の特定

### 3.2. ハザード抽出 プロセス

#### 作成した成果物

| UCAx                                                 | (1)コントロール入力や外部情報の誤りや喪失     | (2) | (3)不整合, 不完全, または不正確なプロセスモデル, 不適切な操作 | (5) | (6)部分的な情報・不正確な情報の供給, または情報の欠如, 測定の不正確性, フィードバックの遅れ |
|------------------------------------------------------|----------------------------|-----|-------------------------------------|-----|----------------------------------------------------|
| UCA1-N<br>運転手がブレーキを踏まないと危険回避ができず, 外部環境と衝突する(SC1-2)違反 | ・悪天候など外部環境が悪く, 運転手が危険察知しない | -   | ・運転手が危険を察知したが自動運転を過信して, ブレーキを踏まない   | -   | ・人工知能モジュールで異常を検知したが内部判定ロジックの誤りで自動運転不能警告が報知されない     |

## Step2 : ハザード要因の特定

### 3.2. ハザード抽出 プロセス

#### 作成した成果物

| UCAx                                                                    | (S)<br>なりす<br>まし | (T)<br>Tampering<br>改ざん                                              | (R)<br>否認 | (I)<br>情報の<br>暴露 | (D)<br>Denial of<br>Service<br>サービス不能                |
|-------------------------------------------------------------------------|------------------|----------------------------------------------------------------------|-----------|------------------|------------------------------------------------------|
| UCA1-N<br>運転手がブレー<br>キを踏まない<br>と危険回避がで<br>きず、外部環<br>境と衝突する<br>(SC1-2)違反 | -                | ・クラウドから<br>の情報を改ざ<br>んし、人工知<br>能モジュールに<br>自動運転継続<br>可能であると<br>誤認識させる | -         | -                | ・人工知能モ<br>ジュールに高<br>負荷を与え<br>自動運転不<br>能警告を報<br>知できない |

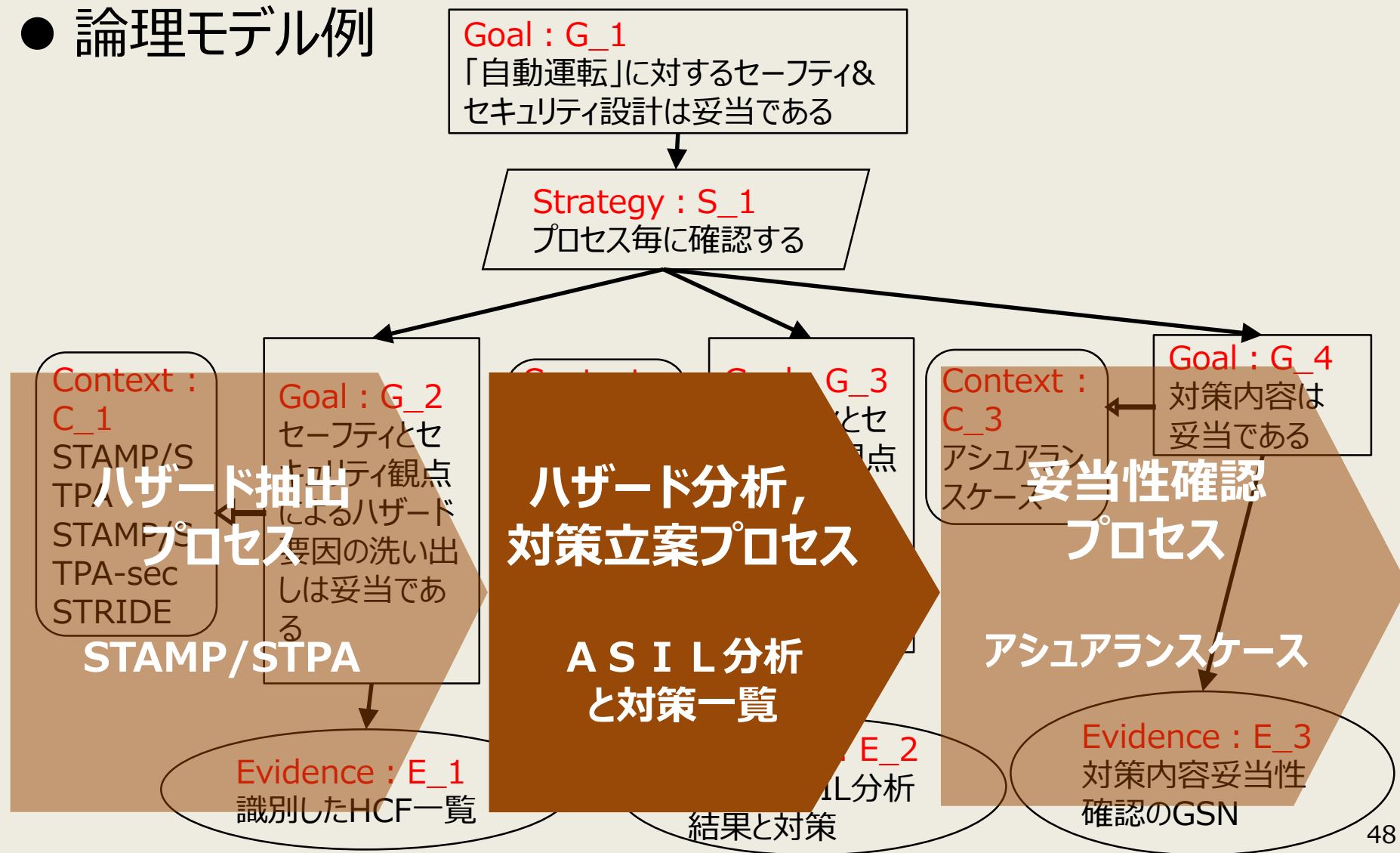
# 目次

1. はじめに
2. 開発プロセス説明
3. 開発プロセス適用事例紹介
  1. 対象システム
  2. ハザード抽出プロセス
  3. ハザード分析・対策立案プロセス
  4. 妥当性確認プロセス
4. 得られた知見, まとめ
5. 最後に

# 保証全体像

## 3.3. ハザード分析 対策立案プロセス

### ● 論理モデル例





### 3.3. ハザード分析 対策立案プロセス

# STRIDE

[illegible]

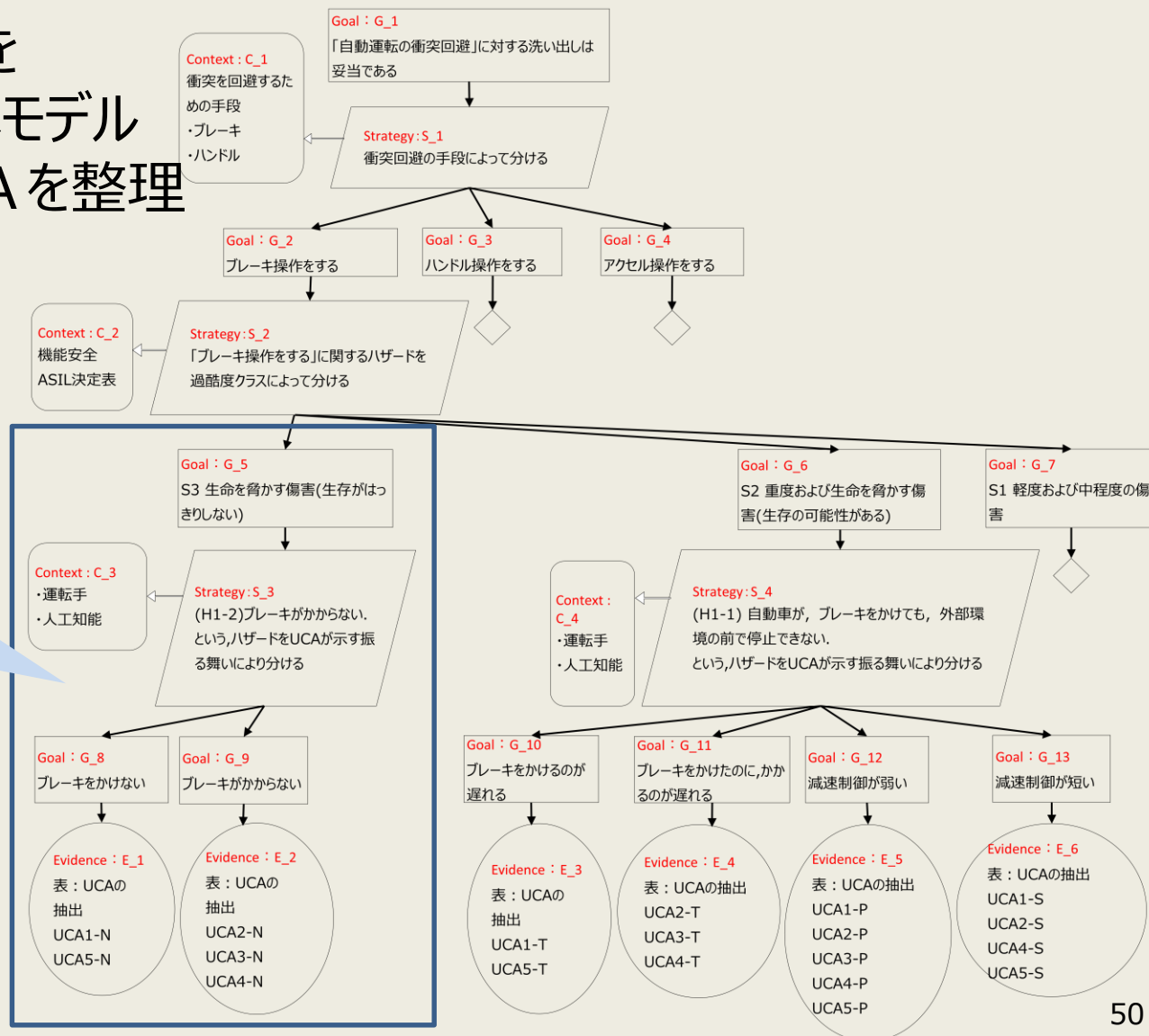
# STPA-Sec

いきなり分析を始めても  
いいのですが...

# UCAを整理 全体像

## 3.3. ハザード分析 対策立案プロセス

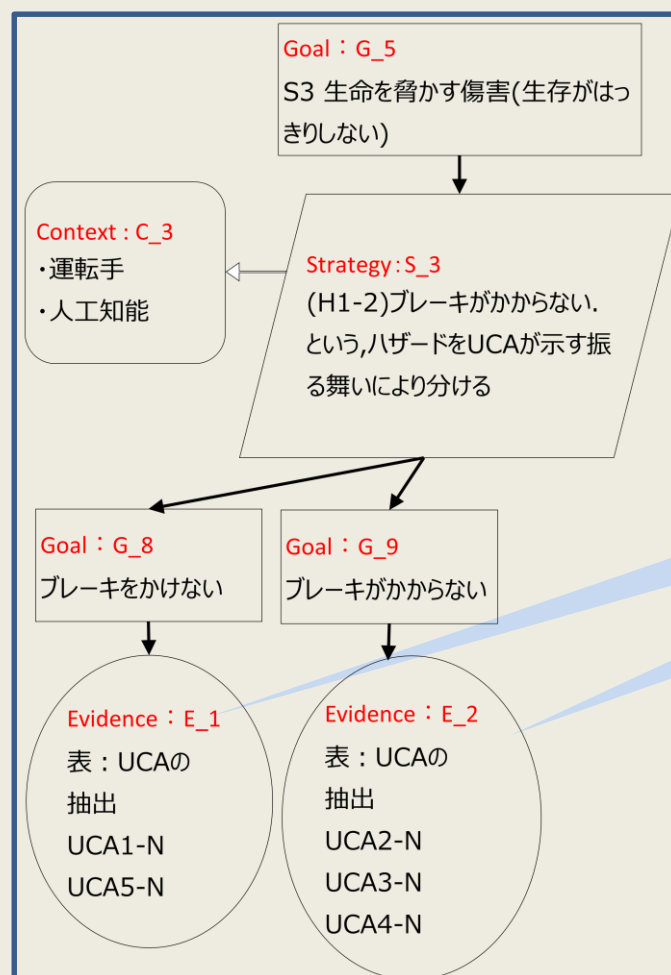
- 抽出したハザードを  
CC-Caseの具体モデル  
に基づき, UCAを整理  
した全体像



# UCAを整理 具体例

## 3.3. ハザード分析 対策立案プロセス

- A S I L 分析における評価指標のうち，深刻度が高い，UCAを整理して，対策立案を検討する優先度を決定.



UCAを整理！

# ASIL 分析結果と対策

## 3.3. ハザード分析 対策立案プロセス

- U C A 毎に整理した A S I L 分析を実施
- 分析結果により，優先順位の高いものについて，優先的に対策内容を検討
- 優先順位が低いハザード要因について，残存リスクを確認

| アクシデント                        | 対象           | 該当するUCA | HCF                                   | 評価指標   |         |          |         | 対策内容                            | 残存リスク |
|-------------------------------|--------------|---------|---------------------------------------|--------|---------|----------|---------|---------------------------------|-------|
|                               |              |         |                                       | 過酷度クラス | 発生頻度クラス | 回避可能性クラス | ASIL決定値 |                                 |       |
| 自動車が外部環境(歩行者/他の車/周辺物)と衝突/接触する | 運転手—ブレーキペダル間 | UCA1-N  | 悪天候など外部環境が悪く，運転手が危険察知しない              | S3     | E2      | C2       | ASIL_A  | 運転手の注意レベルを監視する                  | -     |
|                               |              |         | 運転手が危険を察知したが自動運転を過信して，ブレーキを踏まない       | S3     | E4      | C2       | ASIL_C  | 運転手の注意レベルを監視する<br>定期的に音声による注意喚起 | -     |
|                               |              |         | ブレーキペダルの遊びと認知する値が大きすぎて，ブレーキを踏んだと認識しない | S3     | E2      | C2       | ASIL_A  | ユーザビリティ評価を実施し，適切な遊び量に調整する       | -     |

UCAごとに，  
HCFを整理

ASIL\_A～Dを  
優先して分析。  
優先度：A<D

対策が不十分な  
内容について，  
残存リスクを別途管理

# ASIL 分析結果と対策例

## 3.3. ハザード分析 対策立案プロセス

### - 具体的な対策内容を立案

| 該当する<br>UCA | HCF                             | 評価指標        | 対策内容                            |
|-------------|---------------------------------|-------------|---------------------------------|
|             |                                 | ASIL<br>決定値 |                                 |
| UCA1-N      | 運転手が危険を察知したが自動運転を過信して、ブレーキを踏まない | ASIL_C      | 運転手の注意レベルを監視する<br>定期的に音声による注意喚起 |
|             | 人工知能モジュールに高負荷を与え自動運転不能警告を報知できない | ASIL_A      | DoS対策を実施する                      |

対策が十分か、  
社内合意を取る

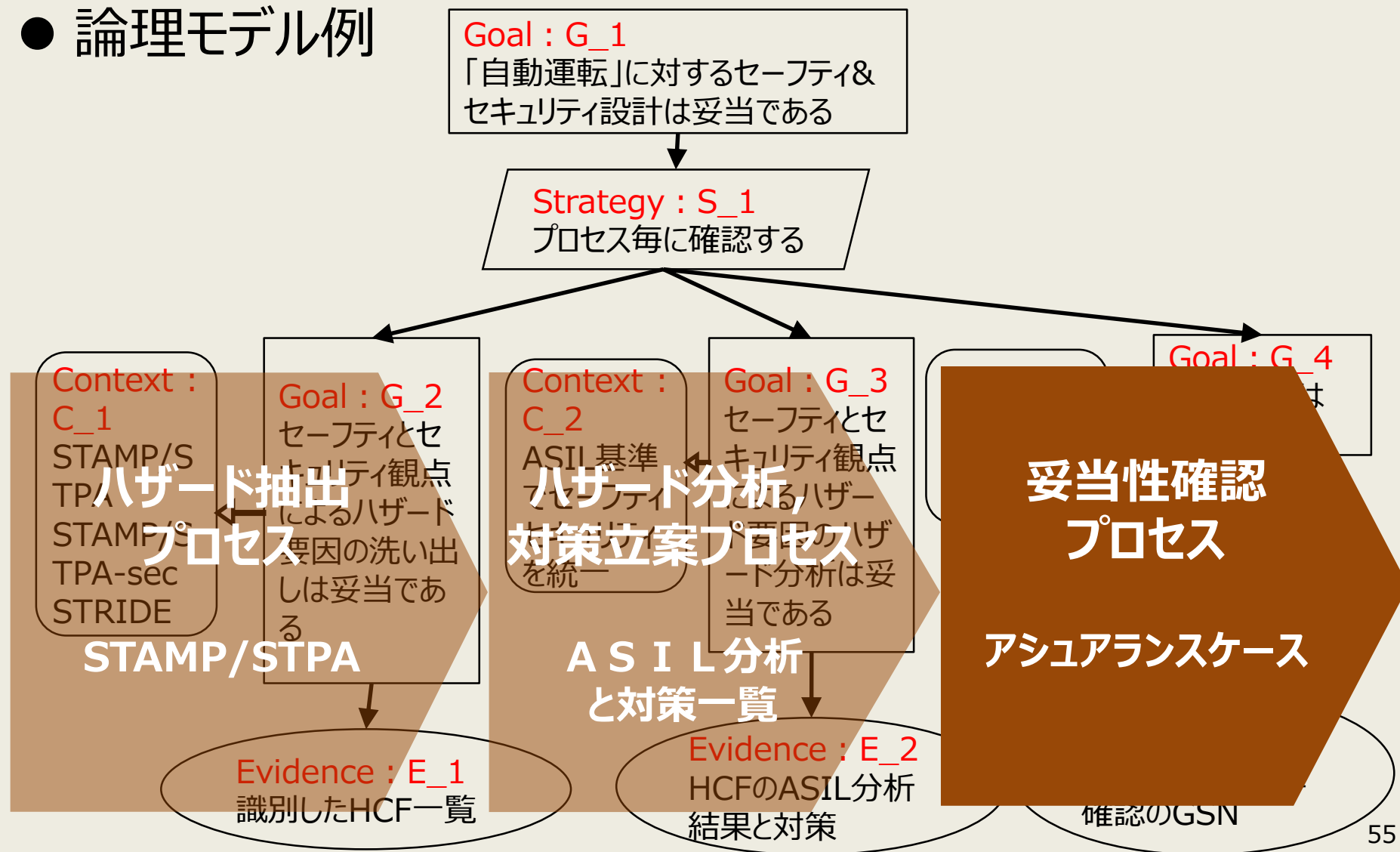
# 目次

1. はじめに
2. 開発プロセス説明
3. 開発プロセス適用事例紹介
  1. 対象システム
  2. ハザード抽出プロセス
  3. ハザード分析・対策立案プロセス
  4. 妥当性確認プロセス
4. 得られた知見, まとめ
5. 最後に

# 保証全体像

## 3.4. 妥当性確認 プロセス

### ● 論理モデル例



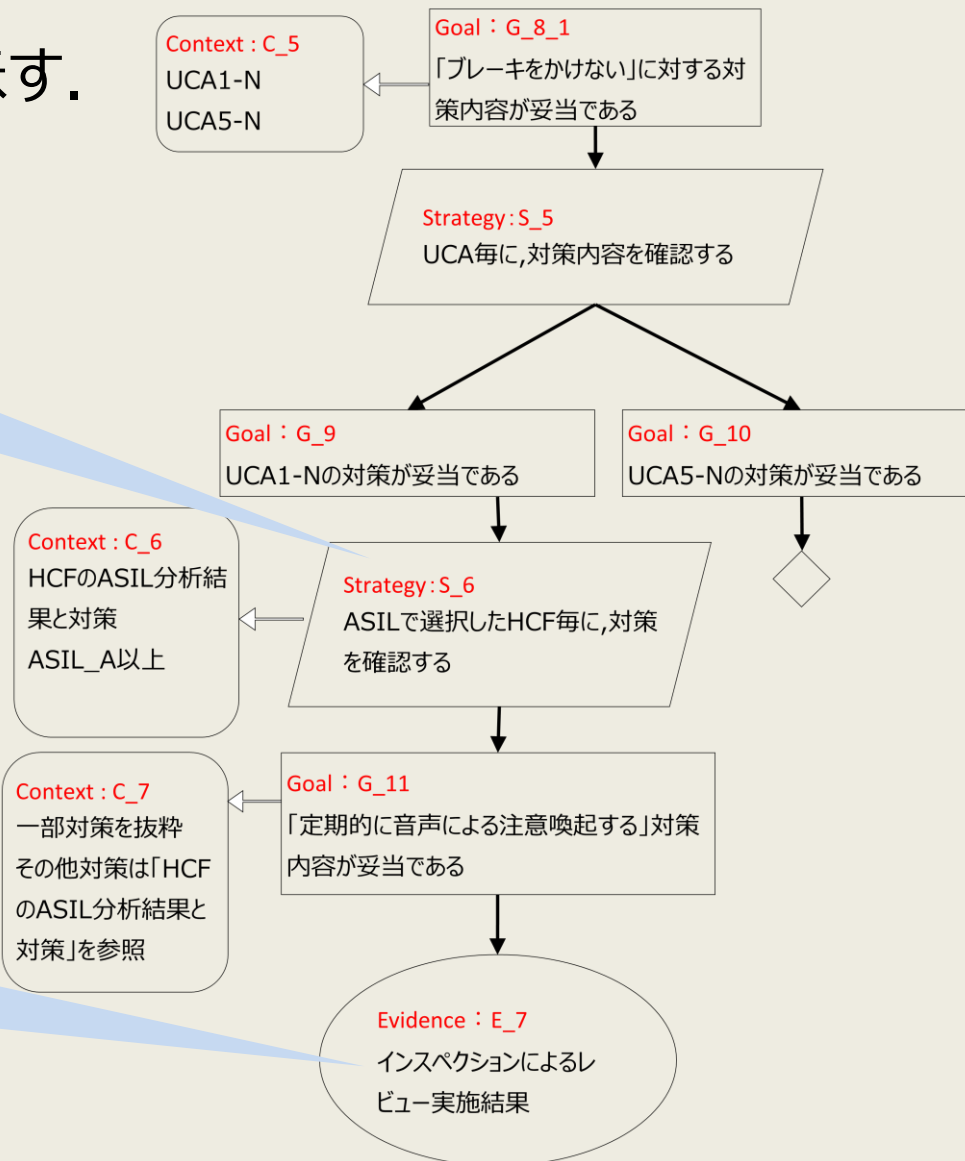
# 対策内容の妥当性を確認

## 3.4. 妥当性確認 プロセス

- 対策内容が妥当かを示す.

ASIL\_A~Dについて,  
対策内容が妥当か確認

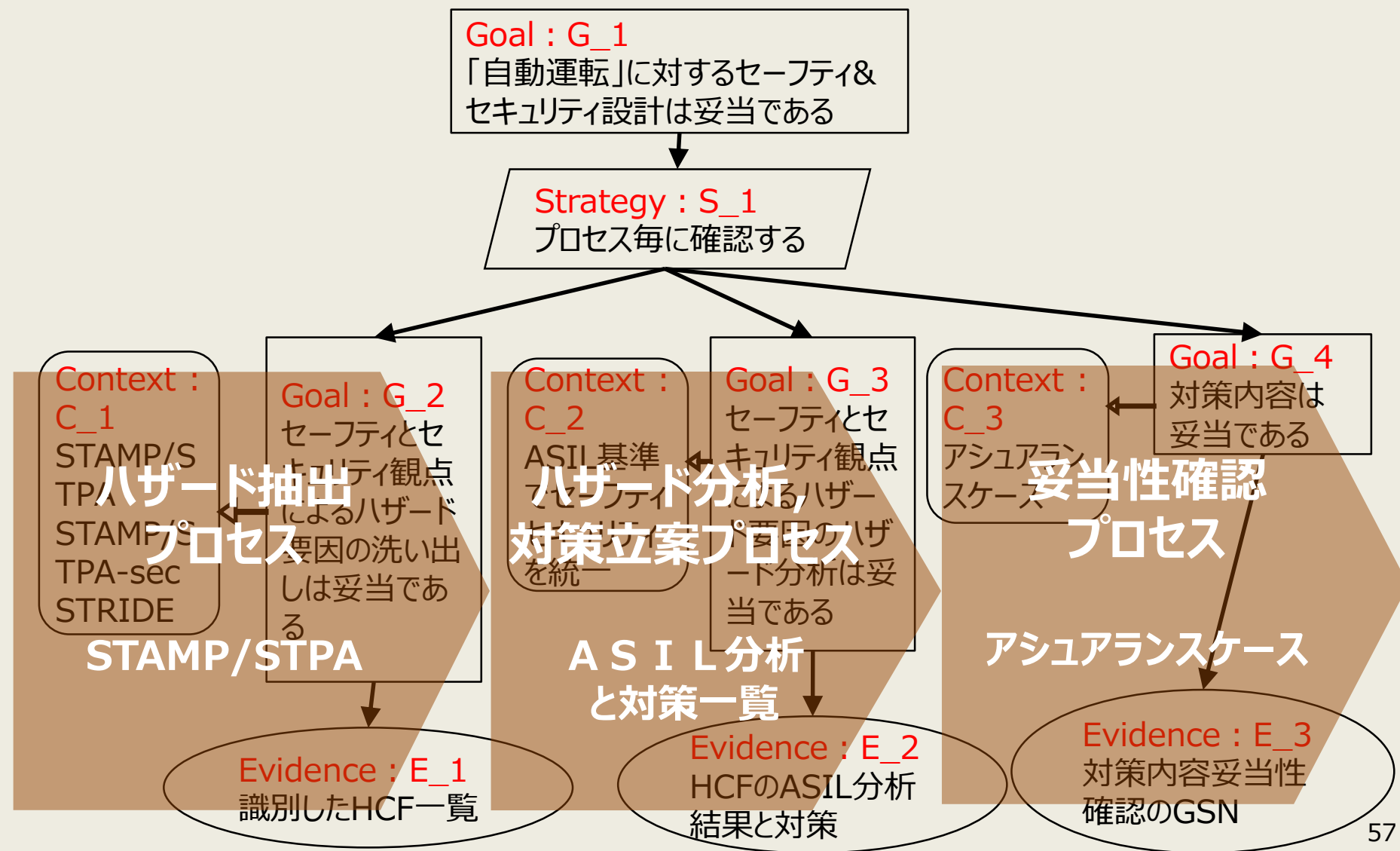
インスペクション議事録等,  
実施した証跡を確認





# 保証全体像

## 3.4. 妥当性確認 プロセス



# 目次

1. はじめに
2. 開発プロセス説明
3. 開発プロセス適用事例紹介
  1. 対象システム
  2. ハザード抽出プロセス
  3. ハザード分析・対策立案プロセス
  4. 妥当性確認プロセス
4. 得られた知見, まとめ
5. 最後に

# 得られた知見

## 4. 得られた知見, まとめ

### プロセス毎に，知見をまとめる

- ハザード抽出プロセス
  - STAMP/STPAは，セーフティの手法であるが，STAMP/STPA-SecやSTRIDEをヒントワードとして適用することにより，セキュリティに関する脅威を洗い出せた。  
特にSTRIDEをヒントワードとして用いて拡張することは，有効であった。
  - ハザード，UCA，HCFを複数人で分析することを考慮すると，各用語に該当する具体例を事前に定義することが必要である。  
実際，複数人で分析を始めると，各用語に対する粒度が異なり，整合性が取れなかった。
- ハザード整理，対策立案プロセス
  - ハザード抽出プロセスにより得た結果を，深刻度が高いハザードをUCA毎に，整理することで，対策を立案する優先順位が明確になった。
- 妥当性確認プロセス
  - 開発者が，対策の妥当性をGSNを用いて検証することで，第三者に対して説明しやすくなった。

## まとめ

### 4. 得られた知見, まとめ

1. IoT時代に必要なセーフティとセキュリティを  
バランスよく対応できるか、開発方法論を試行した。
2. 自動運転に対して、知見のないメンバーが、  
**STAMP/STPAを拡張して適用**することにより、  
セーフティとセキュリティ、それぞれに関するハザードを抽出できた。  
効率よく進めるための  
改善策は知見参照
3. CC-Caseで提唱している論理モデルを使って、**プロセスを定義**し、  
具体モデルを使って、**妥当性を確認**するという開発方法論は、  
**思考を整理**できる点や**説明性**において有益である。

セーフティとセキュリティ、  
それぞれバランスの取れた開発方法論いかがですか？

# 目次

1. はじめに
2. 開発プロセス説明
3. 開発プロセス適用事例紹介
  1. 対象システム
  2. ハザード抽出プロセス
  3. ハザード分析・対策立案プロセス
  4. 妥当性確認プロセス
4. 得られた知見, まとめ
5. 最後に

## 謝辞

### 5. 最後に

**ご指導を頂きました**

**金子主査，高橋副主査，勅使河原アドバイザー**

**ならびに特別講義の講師の方々に御礼申し上げます。**

**また，有意義な機会を与えて頂きました**

**日本科学技術連盟の皆様，**

**およびコース参加を許可して頂きました会社と上司の方々へ  
感謝申し上げます。**

**ご清聴ありがとうございました**

**演習コースⅢ 参加者一同**