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	：	髙橋　雄志	トレドシステム
アドバイザ	：	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 佐々木良一教授	アシュアランスケース
3	7/6,7 合宿	セキュリティ標準とセキュリティ設計 ネットワークの信頼性とセキュリティアーキテクチャ	髙橋　雄志 勅使河原　可海	セキュリティ設計演習
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 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 村山優子教授	事例作成を通じた演習
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」

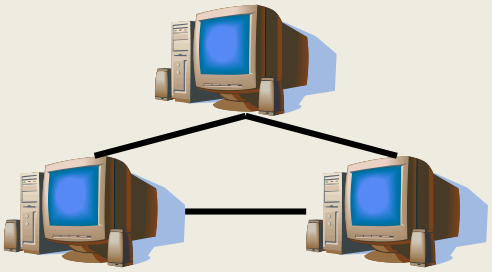
主査	：	金子　朋子	情報セキュリティ大学院大学
副主査	：	髙橋　雄志	トレドシステム
アドバイザ	：	勅使河原　可海	東京電機大学
メンバ	：	荒井　文昭	キヤノンイメージングシステムズ
		大森　淳夫	パイオニア
		神田　圭	日立ソリューションズ
		邱　章傑	パナソニック
		久連石　圭	東芝
		久木元　豊	テックスエンジソリューションズ
		柴引　涼	メタテクノ
		太郎田　裕介	東京海上日動システムズ
		中嶋　良秀	ノーリツ
		西村　伸吾	富士ゼロックス
		細谷　雅樹	東光高岳
		松本　江里加	ダイキン工業

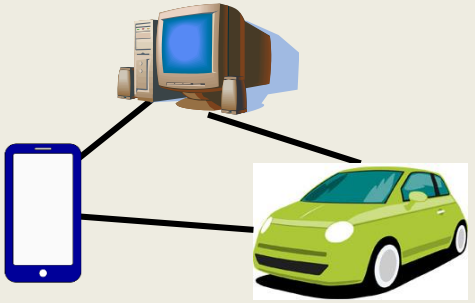
目次

目次

時代の流れ

● 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

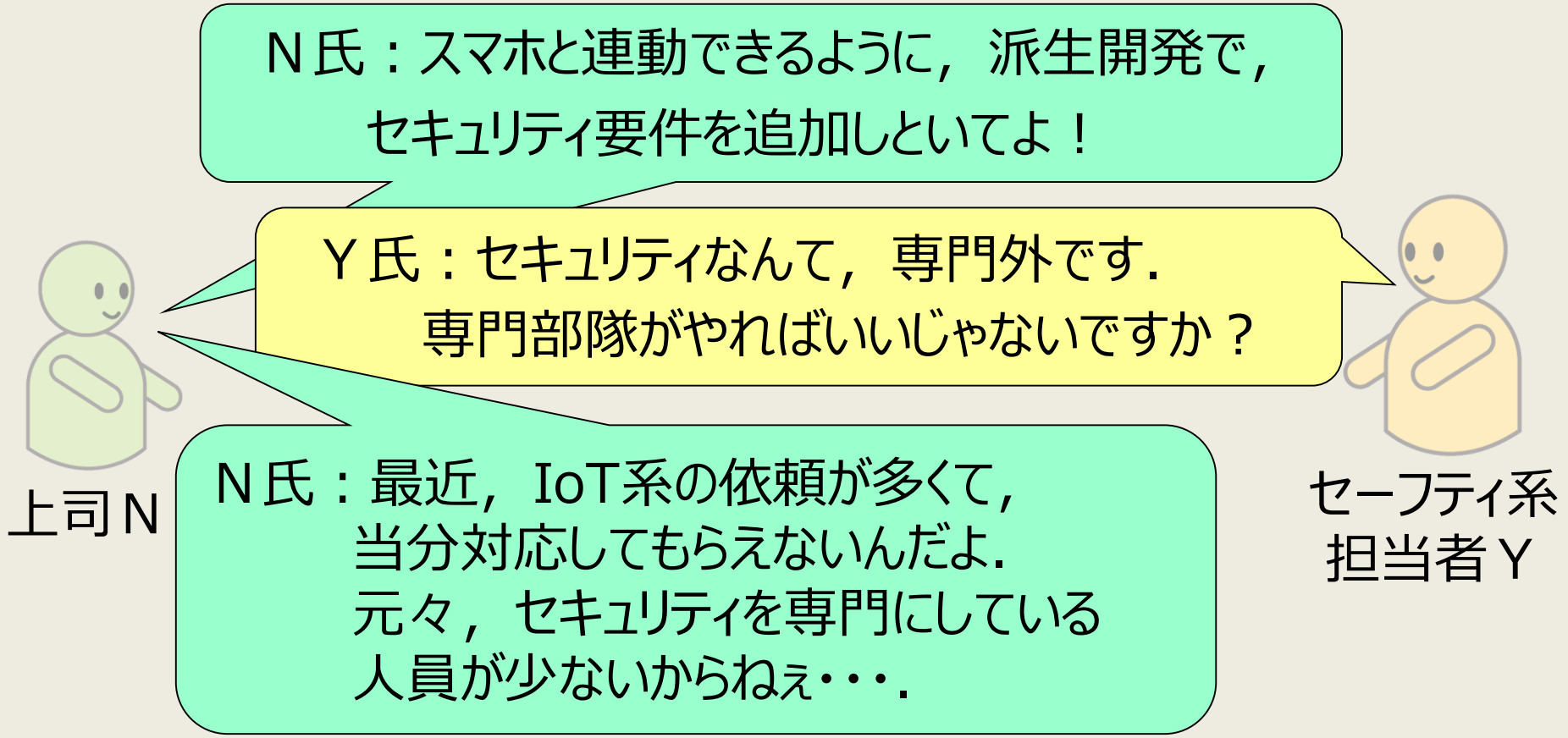
ネットワークが繋がり
他の機器に影響が
有る時代

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

● **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＞



質問

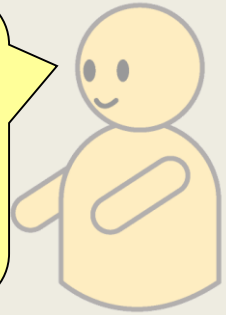
- **皆さんの会社では，こんなやり取りありませんか？**

＜セキュリティ系担当者の場合＞

上司Ｎ

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．

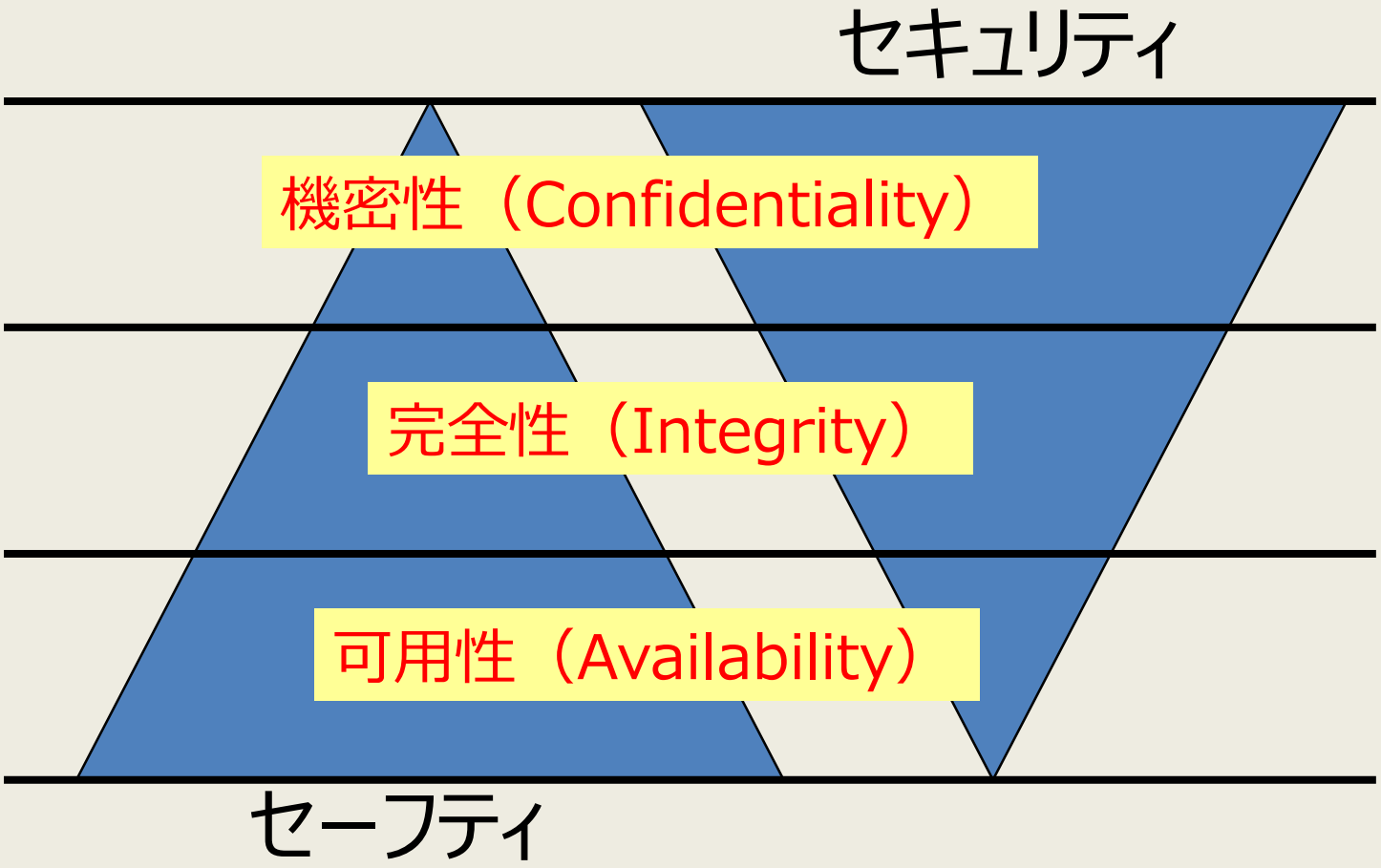


セキュリティ系
担当者Ｙ

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！

視点の違い

- 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

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

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

（参考）関連用語

＜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

<セーフティ系>（２／３）

STAMP

- Systems-Theoretic Accident Model and Processes
- システム理論に基づく事故モデル

STPA

- System–Theoretic Process Analysis
- 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

＜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

＜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

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

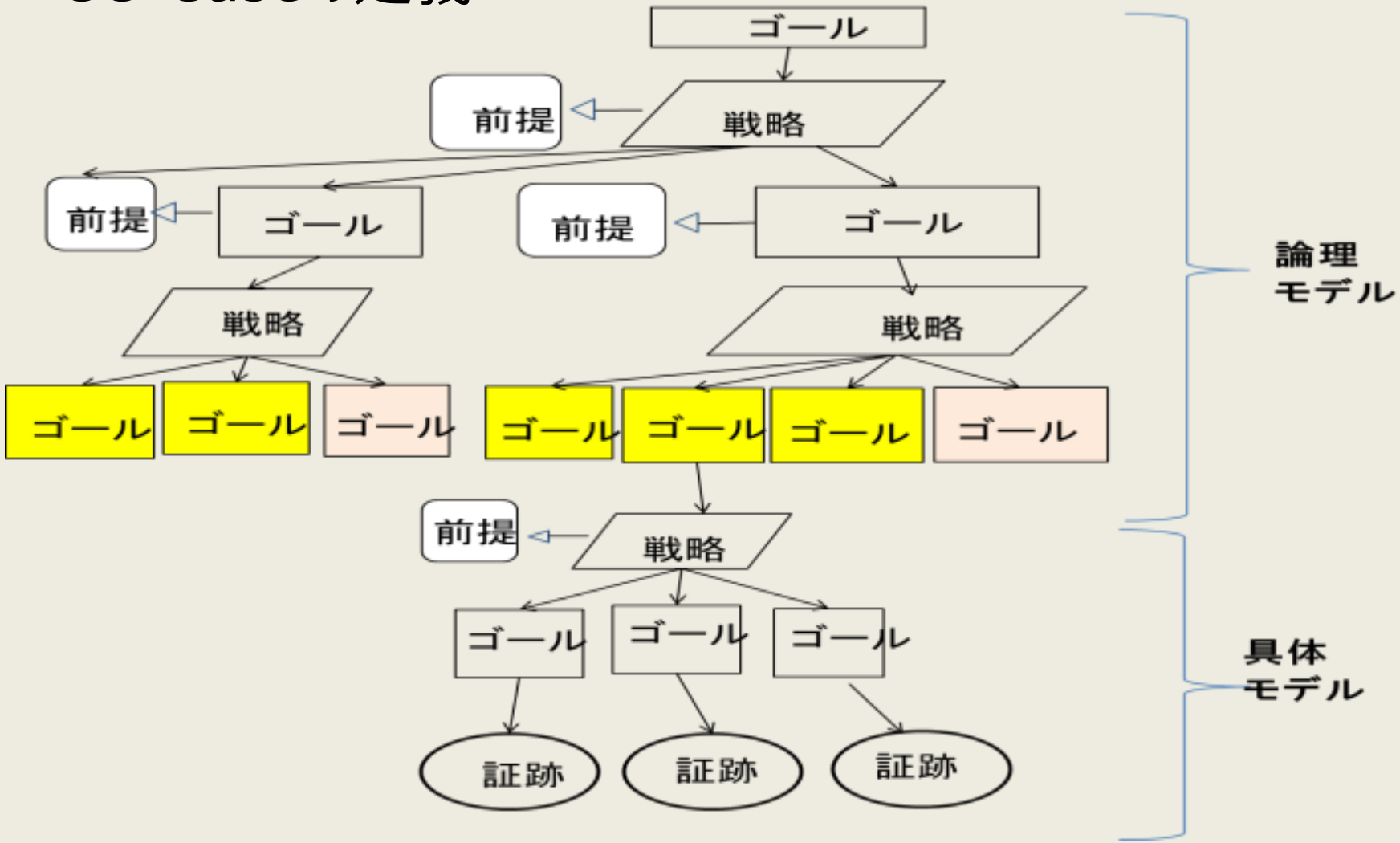
企画・要件定義 → 設計 → 実装 → 検証・評価 → 保守・運用

- 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

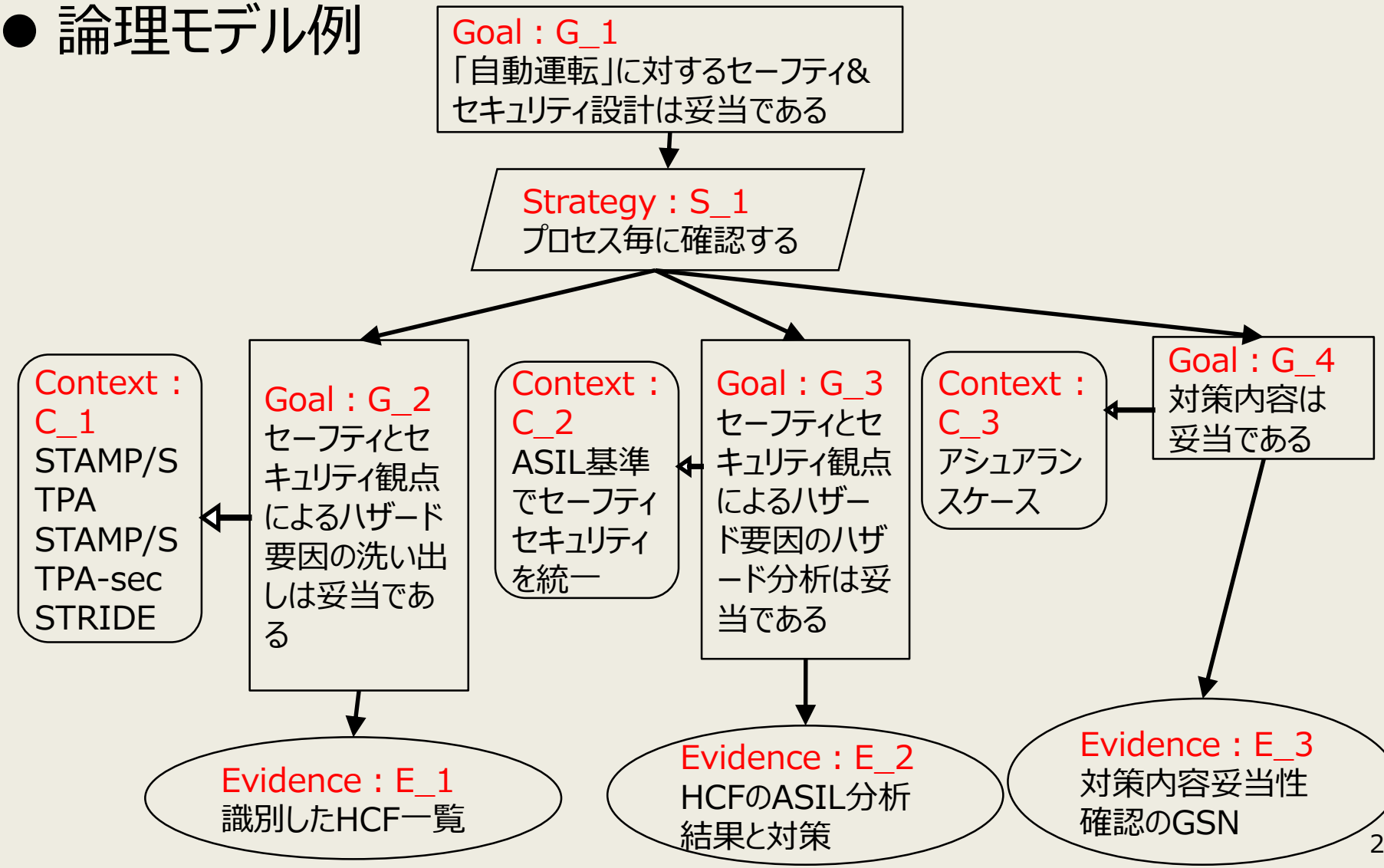
論理モデルと具体モデル

- CC-Caseの定義



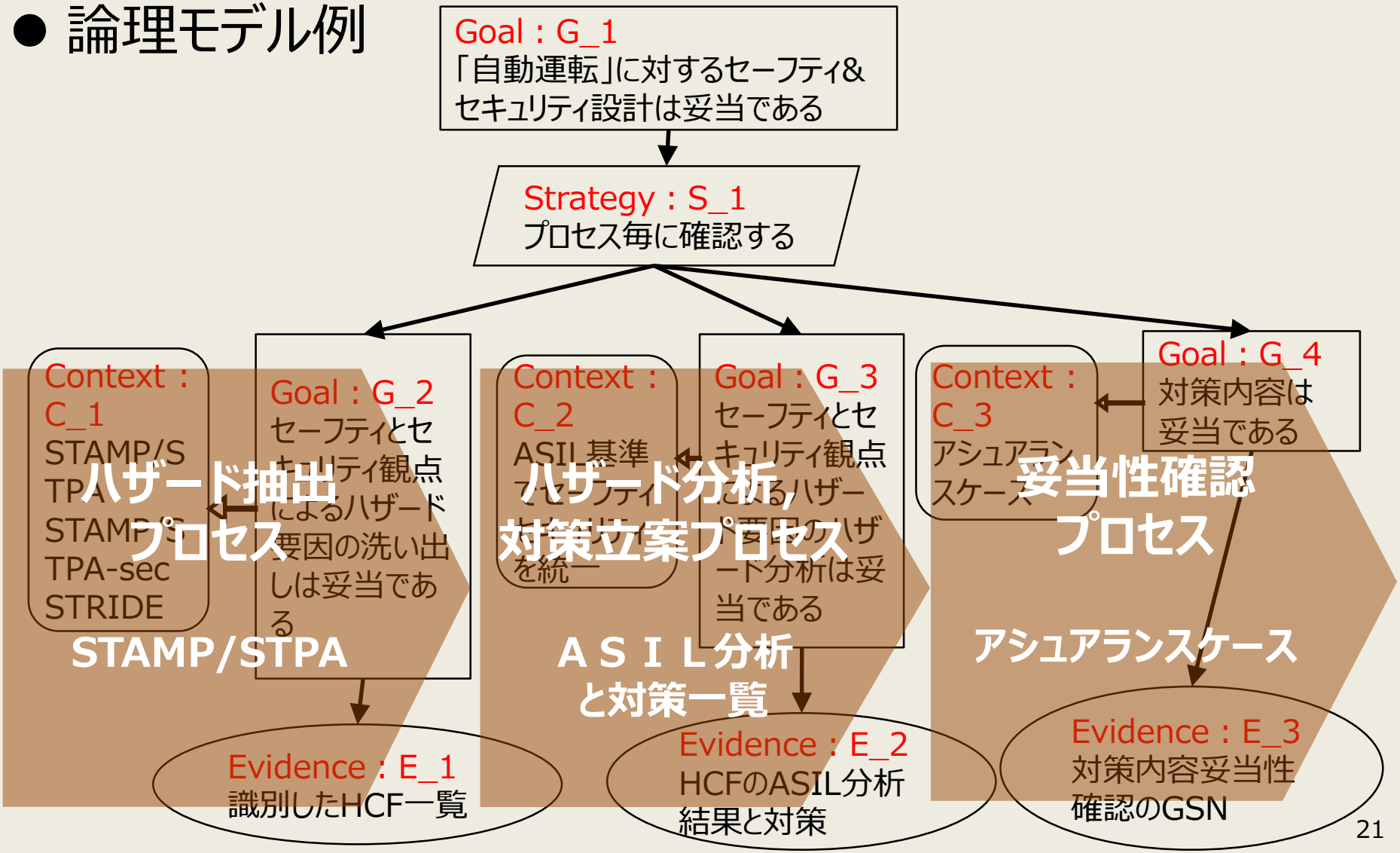
保証全体像

● 論理モデル例



保証全体像

● 論理モデル例



目次

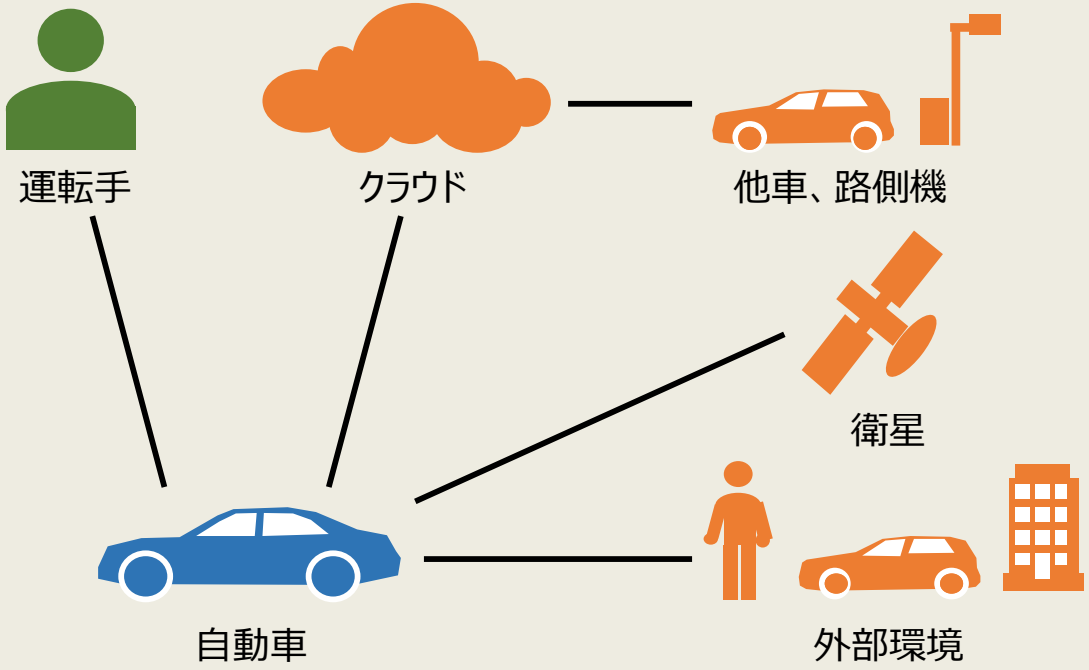
目次

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

STAMP/STPA 背景

3.2. ハザード抽出プロセス

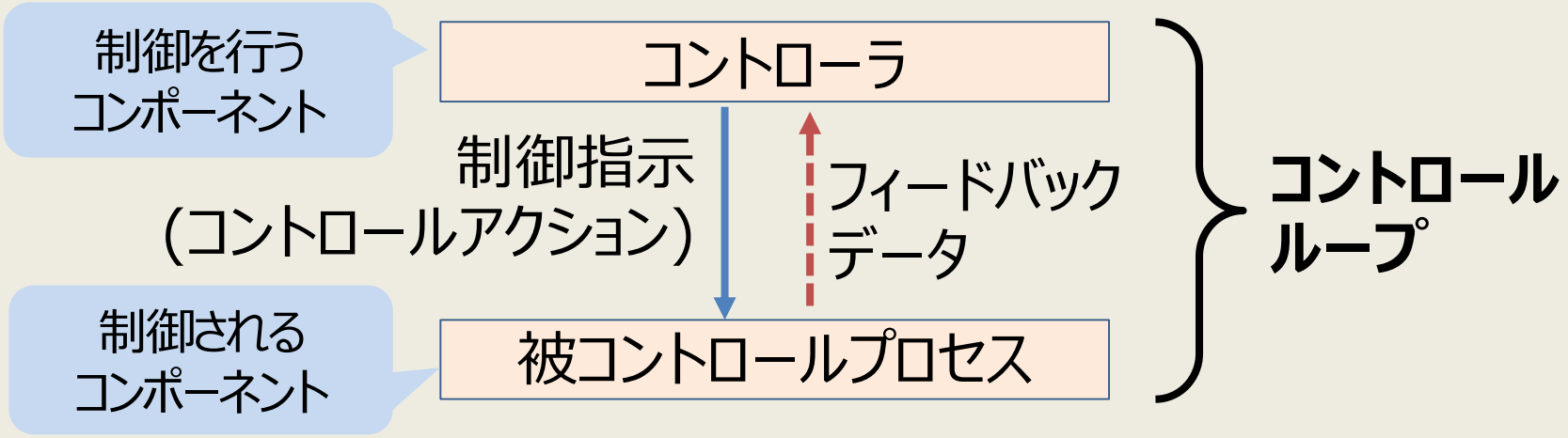
背景

	従来	現在
システム	- システムは小規模 - ハードウェア主体	- システムは大規模/複雑 - ソフトウェア主体 - **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**
安全解析手法	- 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 - FTA FMEA	- 新しいアクシデントモデル 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)** - STPA：STAMPに基づく手法

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

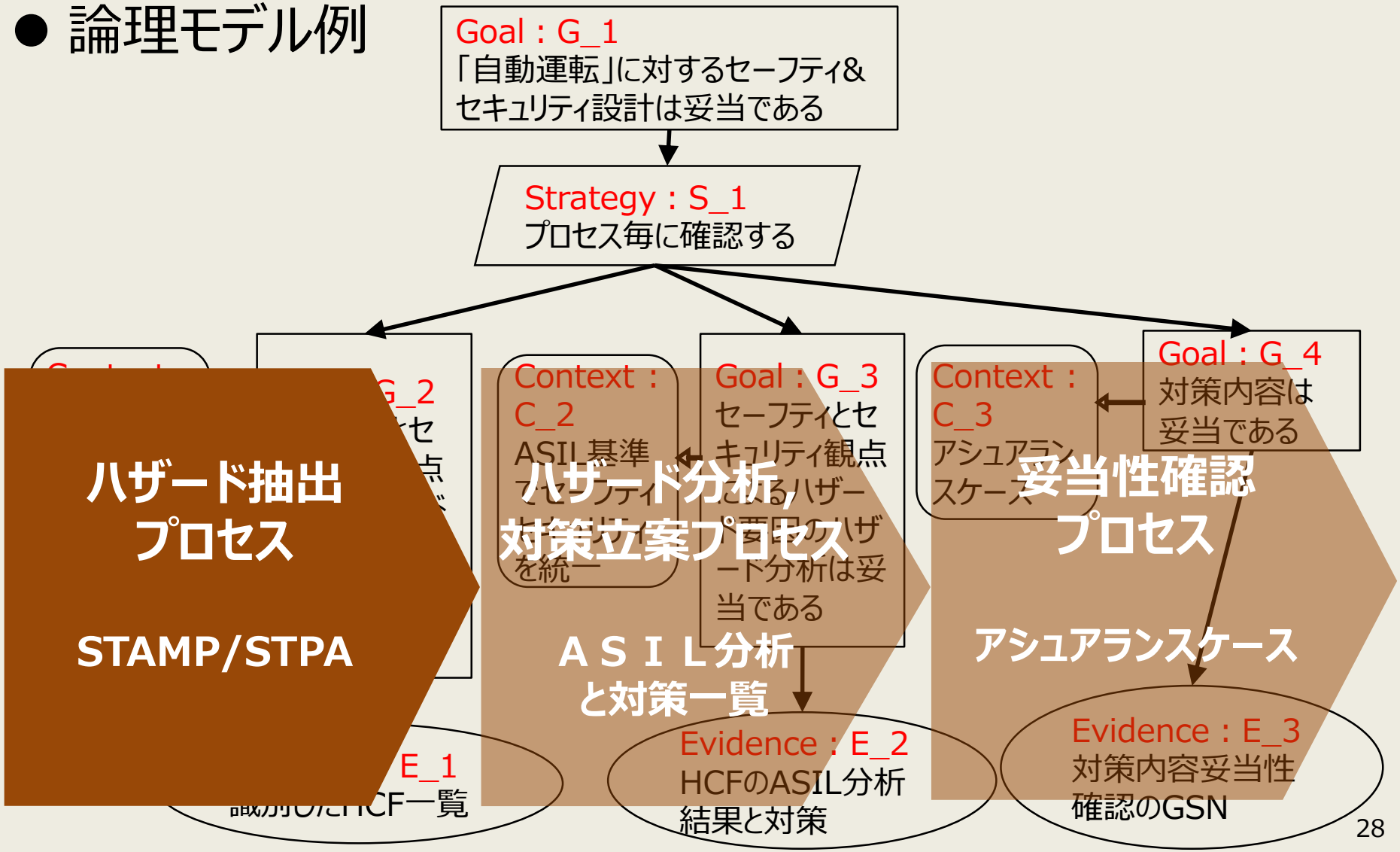


- コントロールループが階層となり、システムが構築される
- **制御指示(コントロールアクション)が適切に与えられないためにアクシデントが起こる**

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(Loss)	ハザード（Hazard）	安全制約(Safety Constraints)
(A1)自動車が外部環境(歩行者/他の車/周辺物)と衝突/接触する	(H1-1) 自動車が，ブレーキをかけても，外部環境の前で停止できない	(SC1-1) 自動車が，外部環境と衝突しないようにブレーキをかける
	(H1-2)ブレーキがかからない	(SC1-2)運転手と自動車の両方がブレーキをかけられない状態にならない

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

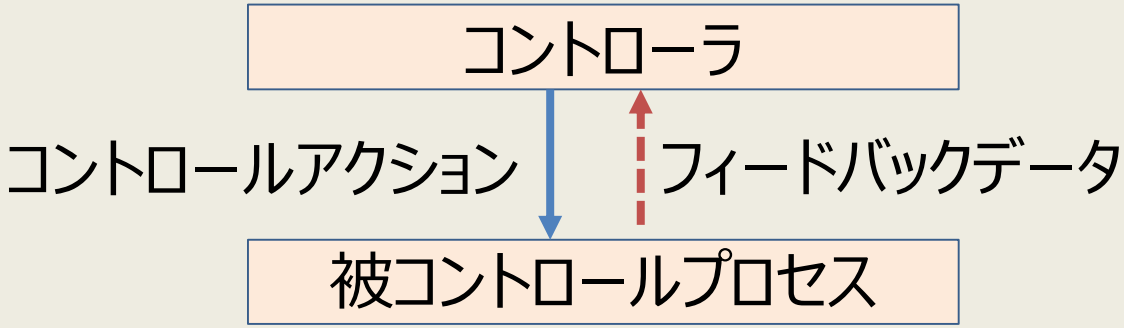
Step 1：
非安全なコントロールアクション（UCA）の抽出

Step 2：
ハザード要因（HCF）の特定

Step0（準備2）

Step 0：（準備2）コントロールストラクチャーの構築

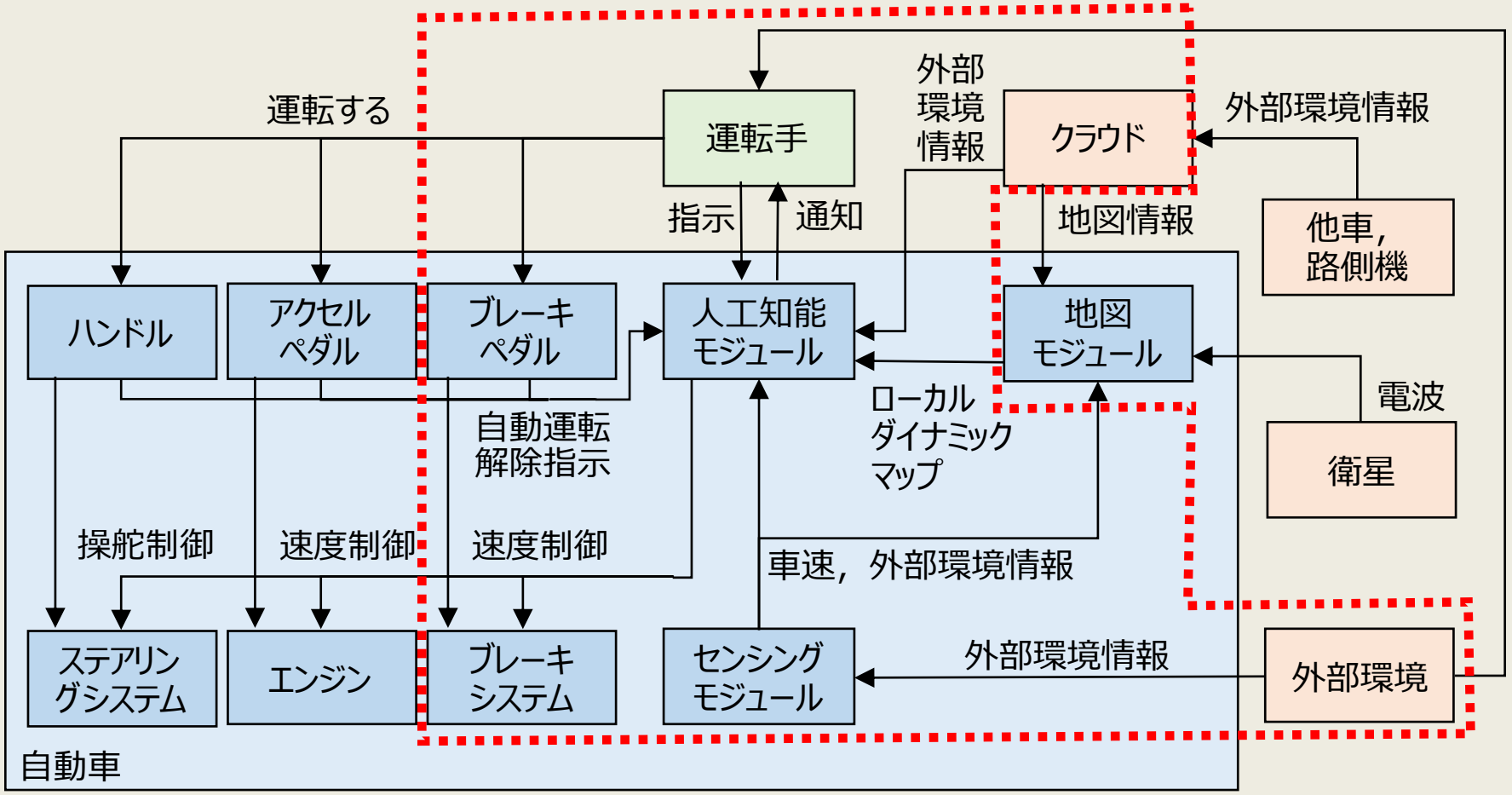
- 目的：(相互作用が適切に働かないところを見つけるために) コンポーネント間の相互作用を明確化する
- コントロールストラクチャー(制御構造図)で構成要素間の相互作用を表す



Step0（準備2）

3.2. ハザード抽出プロセス

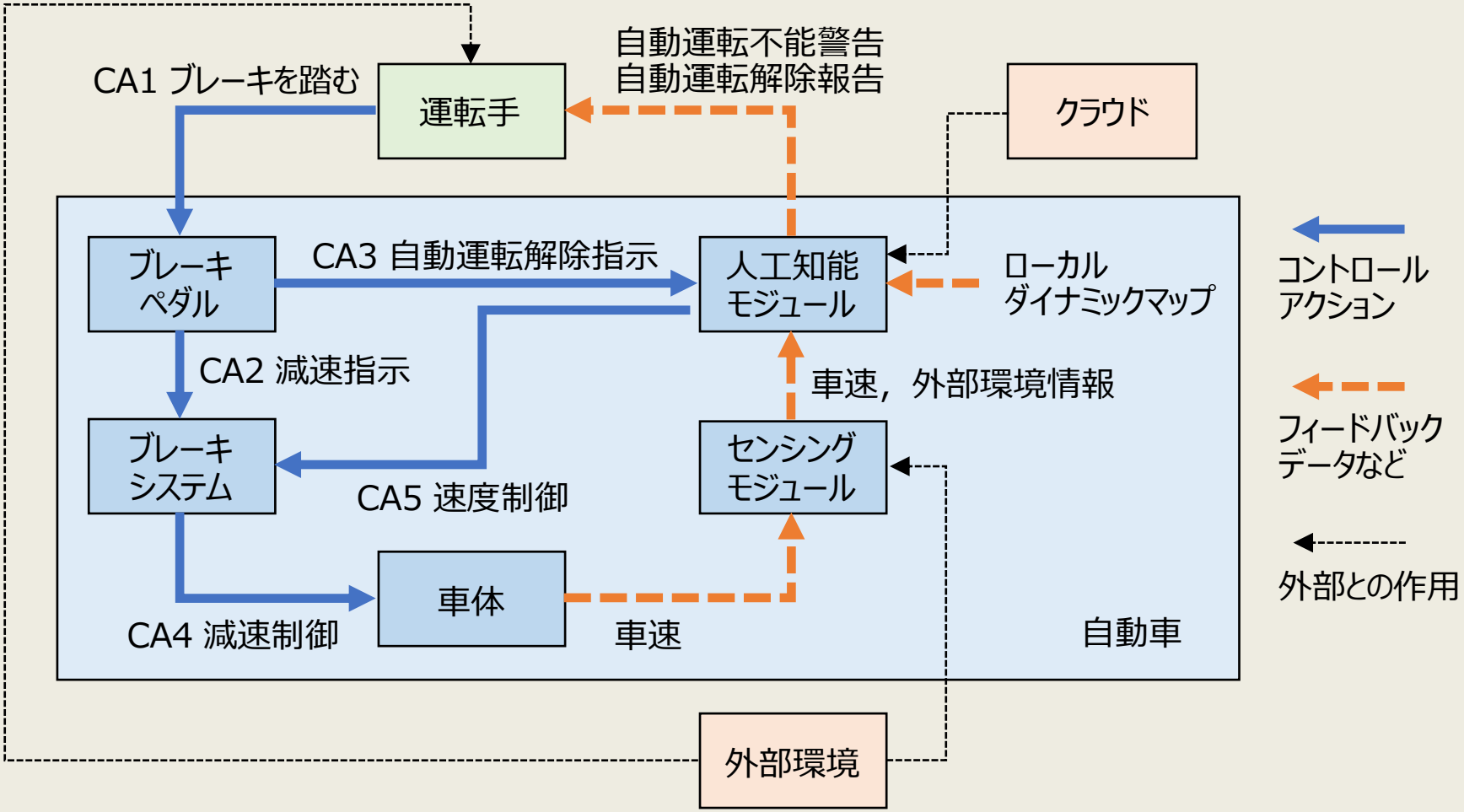
規定した自動車のシステムアーキテクチャ



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

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

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

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

Step 2：ハザード要因（HCF）の特定

- HCF：Hazard Causal Factor
  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

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

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 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 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 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 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

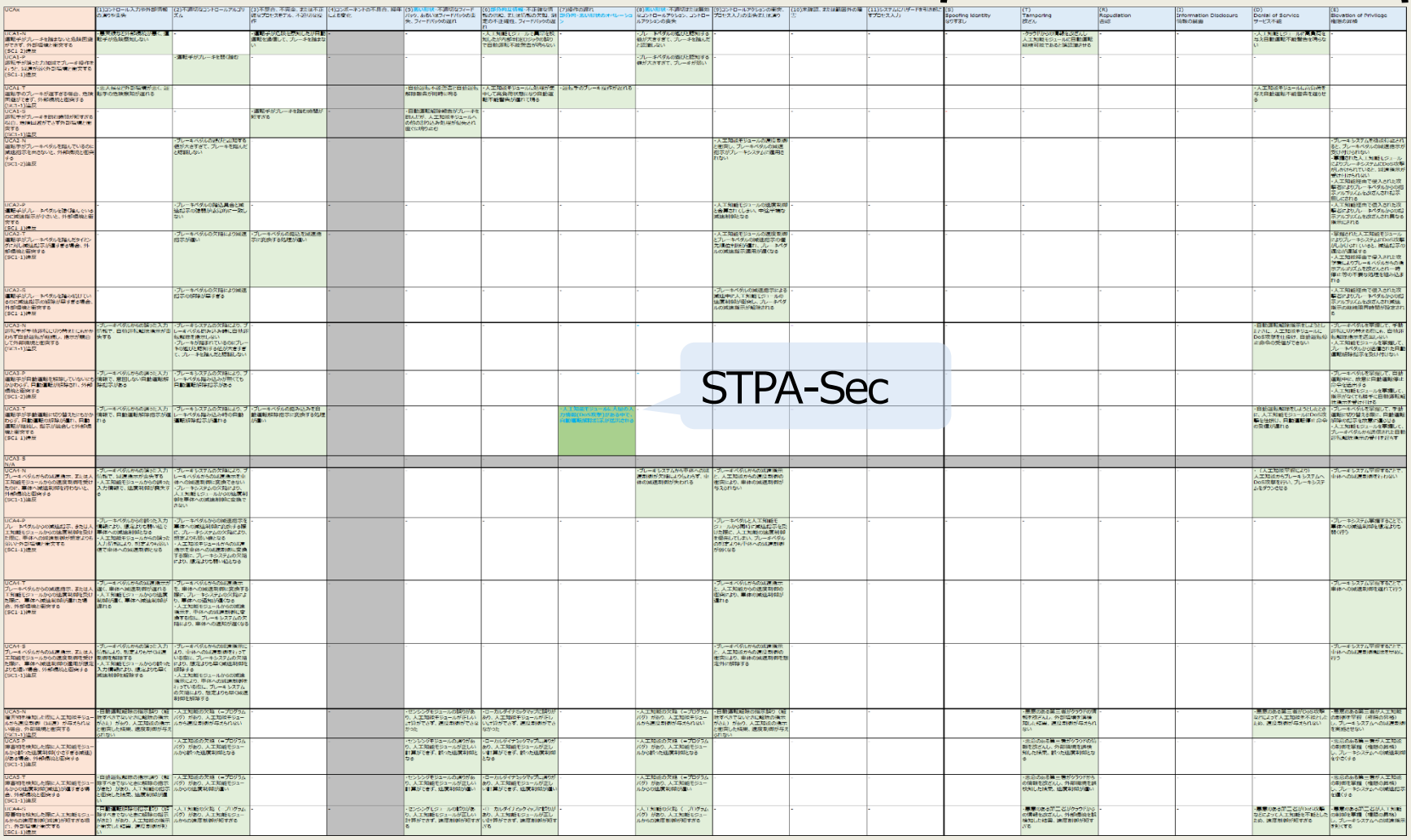
Step2：ハザード要因の特定

3.2. ハザード抽出プロセス

作成した成果物

STRIDE

STPA-Sec



UCAx	(1)コントロール入力が外部原因のあり得る条件	(2)不適切なコントロールアルゴリズム	(3)不意合、不適合、または不正確なプロセスモデル、入力の変化	(4)コンポーネントの不具合、故障による影響	(5)[黒い影響]：不適切なフィードバック、あるいはフィードバックの欠如、フィードバックの遅れ	(6)[青い外部環境情報]：不正確な情報、外部の状態、または他の関与者、誤った情報、誤った状態、誤った仮定の不正確性、フィードバックの遅れ	(7)[緑の制御]：[青い外部環境情報]の誤った処理、誤った制御アクション	(8)[黒い影響]：不適切または異常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発信、プロセス入力の生成または維持	(10)実施団、または範囲外の機能	(11)システムユーザーを示す外部プロセス入力	(S) Spoofing Identity なりすまし	(T) Tamporting 改ざん	(R) Repudiation 否認	(I) Information Disclosure 情報の漏洩	(D) Denial of Service サービス不能	(E) Elevation of Privilege 権限の昇格
UCA1-N 運転中かブレーキを踏まないと危険回避ができず、外部環境が衝突する (SC1-2)連回	・運転者などが高速走行中に、運転中かブレーキを踏まない	-	・運転者などが高速走行中に、ブレーキを踏まない			・人工知能ビジョン：前方車両などを検知したが、判断根拠（センシング誤り）で自動運転不能発生が考えない		・ブレーキやアクセルの操作を認識しない					・クラウドからの情報を元にした人工知能モジュールが自動運転継続可能であると誤認識する			・人工知能ビジョン：前方車両などを自動運転不能警告を考えない	
UCA1-P 運転中かブレーキを踏んだ加速でブレーキ操作をやめる、加速や外部環境に衝突する (SC1-1)連回		・運転手がブレーキを踏み続ける						・ブレーキやアクセルの操作を認識しない									
UCA1-T 運転手のブレーキが遅すぎる場合、危険回避ができず、外部環境と衝突する (UC1-1)連回	・前方車両が急に減速、前方車両の急激な減速を認識しない				・自動運転モジュールが前方車両の減速を認識しない	・人工知能モジュール：前方車両を検知し、前方車両の減速を認識して自動運転不能警告が遅れて出る	・自動ブレーキのブレーキ操作が遅れる								・人工知能モジュールから自動運転不能警告を遅らせる	
UCA1-S 運転中かブレーキを踏む速度が遅すぎるなど、衝突回避ができず外部環境と衝突する (SC1-1)連回		-	・運転手がブレーキを踏む時間が短すぎる		・自動運転継続判断：自動運転モジュールが、人工知能モジュールへのカメラからの入力を誤った値（センサ値）で判断する												
UCA2-N 運転手がブレーキペダルを踏んでいるのに減速指示がでないなど、外部環境と衝突する (SC1-1)連回		・ブレーキペダルの実行と指示を続けすぎて、ブレーキを踏んだと認識しない							・人工知能モジュールの運転指令を実現し、ブレーキペダルの減速指示がブレーキシステムへ適用されない								・ブレーキシステムを経由にはされず、ブレーキペダルの減速指示が受け取りができない ・車両のかた人工知能ビジョン（センシングシステム）のECUが壊れ、故障状態になっている ・人工知能処理で使えないと攻撃者のどちらブレーキペダルからの信号とブレーキペダルを読み込まれる
UCA2-P 運転手がブレーキペダルを踏み込んでいるのに減速指示が小さい、外部環境と衝突する (SC1-1)連回		・ブレーキペダルの踏込量量と減速指示の強度が合いがとれていない							・人工知能モジュールの減速指令値を実現し、ブレーキペダルの減速制御となる								・人工知能処理で使えないと攻撃者のどちらブレーキペダルからの信号とブレーキペダルを読み込まれる
UCA2-T 運転手がブレーキペダルを踏んでインターバル減速などに工夫して考え事後、外部環境と衝突する (SC1-1)連回		・ブレーキペダルの欠陥により減速指示が遅い	・ブレーキペダルの踏込を減速指示に変換する処理が遅い						・人工知能モジュールの運転指令とブレーキペダルの減速指示の値が異なり、ブレーキペダルの減速指示が適用されない								・攻撃者が人工知能モジュールとがブレーキシステムがECUの攻撃に入れていると、車両とのやり取りが遅延する ・人工知能処理で使えないと攻撃者のどちらブレーキペダルからの信号とブレーキペダルを読み込まれる ・車両のかた人工知能ビジョン（センシングシステム）のECUが壊れ、故障状態になっている ・人工知能処理で使えないと攻撃者のどちらブレーキペダルからの信号とブレーキペダルを読み込まれる
UCA2-N 運転手がブレーキペダルを踏んでいるのに減速指示の解除が出ず事故機会と衝突する (SC1-1)連回		・ブレーキペダルの欠陥により減速指示の解除が出ない							・ブレーキペダルの減速指示による減速中の人工知能ビジョンの減速解除指令値と、ブレーキペダルの減速指示が解除される								・人工知能処理で使えないと攻撃者のどちらブレーキペダルからの信号とブレーキペダルを読み込まれる
UCA3-N 運転手がブレーキペダルを踏んでいるのに、ハンドルやその他の操作が不適切なため、自動運転機能停止が発生する (UC1-1)連回	・ブレーキペダルからの誤った入力	・ブレーキシステムの欠陥により、ブレーキペダルからの減速指示が、人工知能モジュールからの操作入力と異なる														・自動運転継続指示が遅れたりなどにより、人工知能モジュールにDoS攻撃を受けるなど、自動運転継続指示の受信ができない	・ブレーキペダルを攻撃して、ブレーキペダルの停止のため、自動運転継続指示を受けるため ・人工知能モジュールを攻撃して、ブレーキペダルの減速指示を受けて自動運転継続指示を受け取れない
UCA3-P 運転手が自動運転を解除していないにもかかわらず、自動運転解除操作が、外部環境と衝突する (SC1-2)連回	・ブレーキペダルからの誤った入力	・ブレーキシステムの欠陥により、ブレーキペダル踏み込みが取れても自動運転解除指示が出る															・ブレーキペダルを攻撃して、自動運転中に、故意に自動運転停止を受け取る ・人工知能モジュールを攻撃して、偽の停止などを出す ・人工知能モジュールを攻撃して、偽の停止などを出す、自動運転解除を受け取れない
UCA3-T 運転手が手動運転に切り替えたにもかかわらず、自動運転解除操作が遅れ、自動運転が継続し、外部環境と衝突する (SC1-1)連回	・ブレーキペダルからの誤った入力	・ブレーキシステムの欠陥により、ブレーキペダル踏み込みを自動運転解除指示に変換する処理が遅い	・ブレーキペダルの踏み込みを自動運転解除指示に変換する処理が遅い			・人工知能ビジョン：前方車両などの検知により、自動運転解除指示が出力されるが、外部環境の解除判断が遅れる											・自動運転継続指示はうけとるが、人工知能モジュールがDoS攻撃を受けるなど、自動運転解除の指示を出せない。自動運転が継続してしまう ・人工知能モジュールを攻撃して、偽の停止などを出す、自動運転解除を受け取れない
UCA3-S N/A																	
UCA4-N ブレーキペダルからの減速指示、または人工知能モジュールからの減速指令時を受けたなど、車両への減速制御を行わないと、外部環境と衝突する (SC1-1)連回	・ブレーキペダルからの誤った入力	・ブレーキシステムの欠陥により、ブレーキペダルからの減速指示や人工知能モジュールからの操作入力と異なる、減速制御が異なる						・ブレーキシステムから受けた減速制御が異なる	・ブレーキペダルからの減速指示や、人工知能からの減速指令の衝突により、車両の減速制御が与えられない				・人工知能処理遅れの人工知能モジュールからブレーキシステムへDoS攻撃を受けない、ブレーキシステムをブロックをせる			・ブレーキシステムを攻撃するなどで、車両への減速制御を遮断されない
UCA4-P ブレーキペダルからの減速指示、または人工知能モジュールからの減速指令時を受けたなど、車両への減速制御をしなければならないタイミングで減速しない (SC1-1)連回	・ブレーキペダルからの誤った入力	・ブレーキペダルからの減速指示を車両への減速制御に変換できない、ブレーキシステムの欠陥などの問題がある ・人工知能モジュールからの減速指令や車両への減速制御を、ブレーキシステムが受け取れない							・ブレーキペダルと人工知能モジュールからの減速指令を同時に受けた場合、人工知能の減速制御を優先してしまい、ブレーキペダルの減速制御が弱くなる								・ブレーキシステム単体でまとめて車両への減速制御を優先よりも弱く行う
UCA4-T ブレーキペダルからの減速指示、または人工知能モジュールからの減速指令時を受けたなど、車両への減速制御が遅れて、車両と衝突する (SC1-1)連回	・ブレーキペダルからの誤った入力	・ブレーキペダルからの減速指示を、車両への減速制御に変換する際や、ブレーキシステムの欠陥などの問題で、車両への減速制御が遅くなる ・人工知能モジュールからの減速指令や、ブレーキシステムの欠陥などの問題で、車両への減速制御が遅くなる							・ブレーキペダルからの減速指示と、人工知能からの減速指令の衝突により、車両の減速制御が遅れる								・ブレーキシステム単体でまとめて車両への減速制御を遅れて行う
UCA4-S ブレーキペダルからの減速指示、または人工知能モジュールからの減速指令時を受けたなど、車両への減速制御が遅れて、車両と衝突する (SC1-1)連回	・ブレーキペダルからの誤った入力	・ブレーキペダルからの減速指示や、車両への減速制御に変換する際や、ブレーキシステムの欠陥などの問題で、車両への減速制御が遅くなる ・人工知能モジュールからの減速指令や、ブレーキシステムの欠陥などの問題で、車両への減速制御が遅くなる							・ブレーキペダルからの減速指示と、人工知能からの減速指令の衝突により、車両の減速制御が遅れる								・ブレーキシステム単体でまとめて車両への減速制御を遅れて行う
UCA5-N 車両が停車時、人が乗っている状態で、人工知能モジュールから停車（加速）するなどの場合、外部環境と衝突する (SC1-1)連回	・自動運転継続判断：人工知能モジュールが、前方車両などがいなくなったと誤認識（センシング誤り）から、人工知能モジュールから停車（加速）するなどの場合、外部環境と衝突する	・人工知能の欠陥（プログラムバグ）により、人工知能モジュールから誤った加速制御が出る			・センシングモジュールの誤りがあり、人工知能モジュールが正しい判断ができず、誤った加速制御が出る	・ローカルダイナミックマップ上の誤りがあり、人工知能モジュールが正しい判断ができず、誤った加速制御が出る	・人工知能の欠陥（プログラムバグ）により、人工知能モジュールから誤った加速制御が出る	・自動運転継続判断：人工知能モジュールが、前方車両などがいなくなったと誤認識（センシング誤り）から、人工知能モジュールから停車（加速）するなどの場合、外部環境と衝突する				・車両のある第三者がDoS攻撃などにより、人工知能モジュールが正しい判断ができず、誤った加速制御が出る		・車両のある第三者が人工知能の誤停車判断（検知の誤検知）、システムへの攻撃を受けるなど
UCA5-P 車両停車時も人が乗っている状態で、人工知能モジュールから誤った加速制御（さらする制御）が出る場合、外部環境と衝突する (SC1-1)連回		・人工知能の欠陥（プログラムバグ）により、人工知能モジュールから誤った加速制御が出る			・センシングモジュールの誤りがあり、人工知能モジュールが正しい判断ができず、誤った加速制御が出る	・ローカルダイナミックマップ上の誤りがあり、人工知能モジュールが正しい判断ができず、誤った加速制御が出る	・人工知能の欠陥（プログラムバグ）により、人工知能モジュールから誤った加速制御が出る				・乗っている第三者がクラウドからの情報を元にした、外部環境を誤検知した結果、誤った加速制御が出る			・乗っている第三者がクラウドからの情報を元にした、外部環境を誤検知した結果、誤った加速制御が出る	・乗っている第三者がDoS攻撃などにより、人工知能モジュールが正しい判断ができず、誤った加速制御が出る	・乗っている第三者が人工知能の誤停車判断（検知の誤検知）、システムへの攻撃を受けるなど
UCA5-S N/A																	
UCA6-N 前方車両や障害物など、人工知能モジュールから停車しない場合（加速）、外部環境と衝突する (SC1-1)連回	・自動運転継続判断：人工知能モジュールが、前方車両などがいなくなったと誤認識（センシング誤り）から、人工知能モジュールから停車しない場合（加速）、外部環境と衝突する	・人工知能の欠陥（プログラムバグ）により、人工知能モジュールから誤った加速制御が出る			・センシングモジュールの誤りがあり、人工知能モジュールが正しい判断ができず、誤った加速制御が出る	・ローカルダイナミックマップ上の誤りがあり、人工知能モジュールが正しい判断ができず、誤った加速制御が出る	・人工知能の欠陥（プログラムバグ）により、人工知能モジュールから誤った加速制御が出る	・自動運転継続判断：人工知能モジュールが、前方車両などがいなくなったと誤認識（センシング誤り）から、人工知能モジュールから停車しない場合（加速）、外部環境と衝突する				・乗っている第三者がクラウドからの情報を元にした、外部環境を誤検知した結果、誤った加速制御が出る			・乗っている第三者がDoS攻撃などにより、人工知能モジュールから停車しない場合（加速）、外部環境と衝突する	・乗っている第三者が人工知能の誤停車判断（検知の誤検知）、システムへの攻撃を受けるなど
UCA6-P 前方車両や障害物など、人工知能モジュールから停車しない場合（加速）が出ずに、外部環境と衝突する (SC1-1)連回	・自動運転継続判断：人工知能モジュールが、前方車両などがいなくなったと誤認識（センシング誤り）から、人工知能モジュールから停車しない場合（加速）、外部環境と衝突する	・人工知能の欠陥（プログラムバグ）により、人工知能モジュールから誤った加速制御が出る			・センシングモジュールの誤りがあり、人工知能モジュールが正しい判断ができず、誤った加速制御が出る	・ローカルダイナミックマップ上の誤りがあり、人工知能モジュールが正しい判断ができず、誤った加速制御が出る	・人工知能の欠陥（プログラムバグ）により、人工知能モジュールから誤った加速制御が出る				・乗っている第三者がクラウドからの情報を元にした、外部環境を誤検知した結果、誤った加速制御が出る			・乗っている第三者がDoS攻撃などにより、人工知能モジュールから停車しない場合（加速）、外部環境と衝突する	・乗っている第三者が人工知能の誤停車判断（検知の誤検知）、システムへの攻撃を受けるなど

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 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

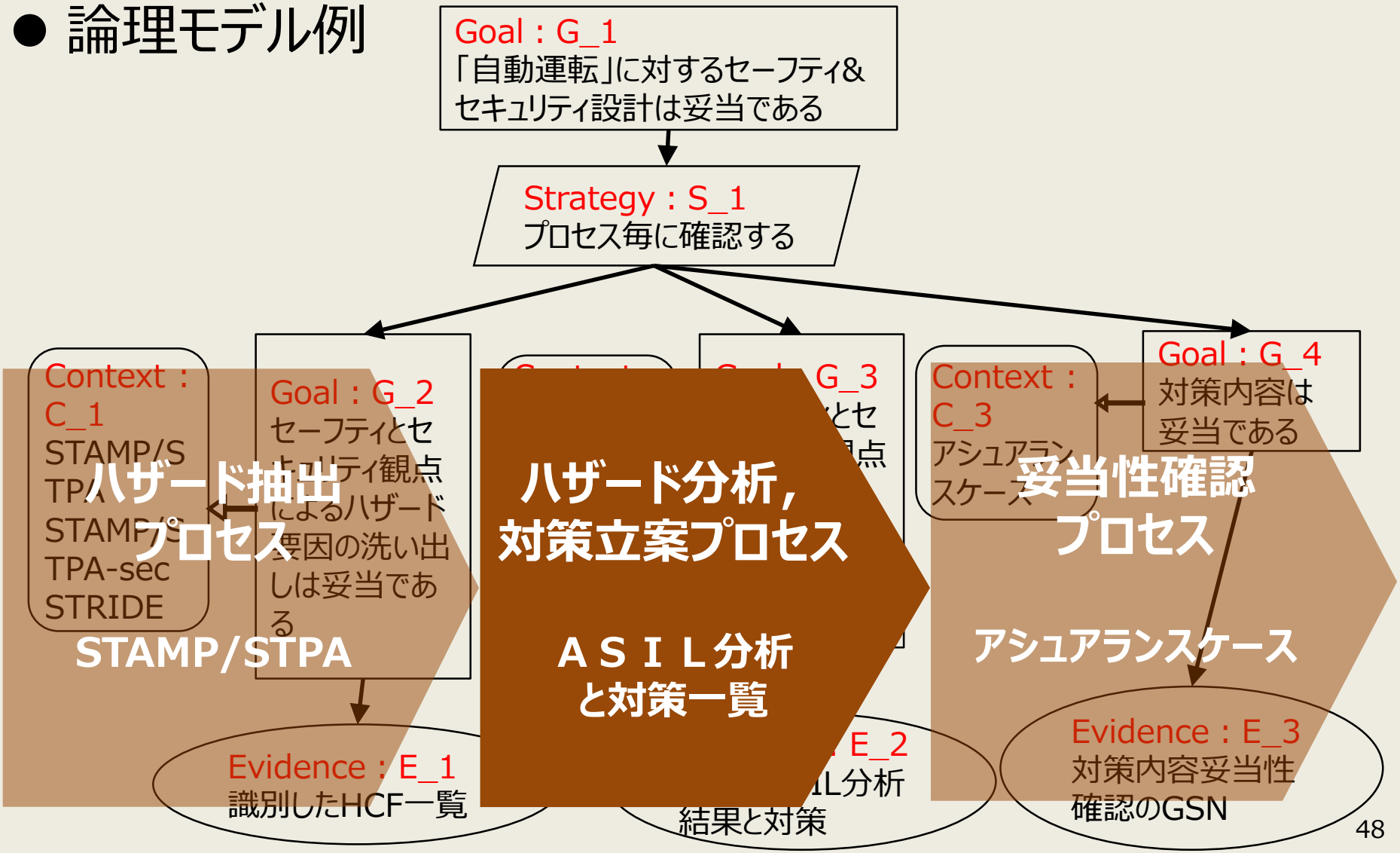
UCAx	(S) なりすまし	(T) Tampering 改ざん	(R) 否認	(I) 情報の暴露	(D) Denial of Service サービス不能
UCA1-N 運転手がブレーキを踏まないと危険回避ができず，外部環境と衝突する(SC1-2)違反	-	・クラウドからの情報を改ざんし，人工知能モジュールに自動運転継続可能であると誤認識させる	-	-	・人工知能モジュールに高負荷を与え自動運転不能警告を報知できない

目次

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



ハザード要因抽出完了…

3.3. ハザード分析
対策立案プロセス

作成した成果物

STRIDE

STPA-Sec

いきなり分析を始めても
いいのですが・・・

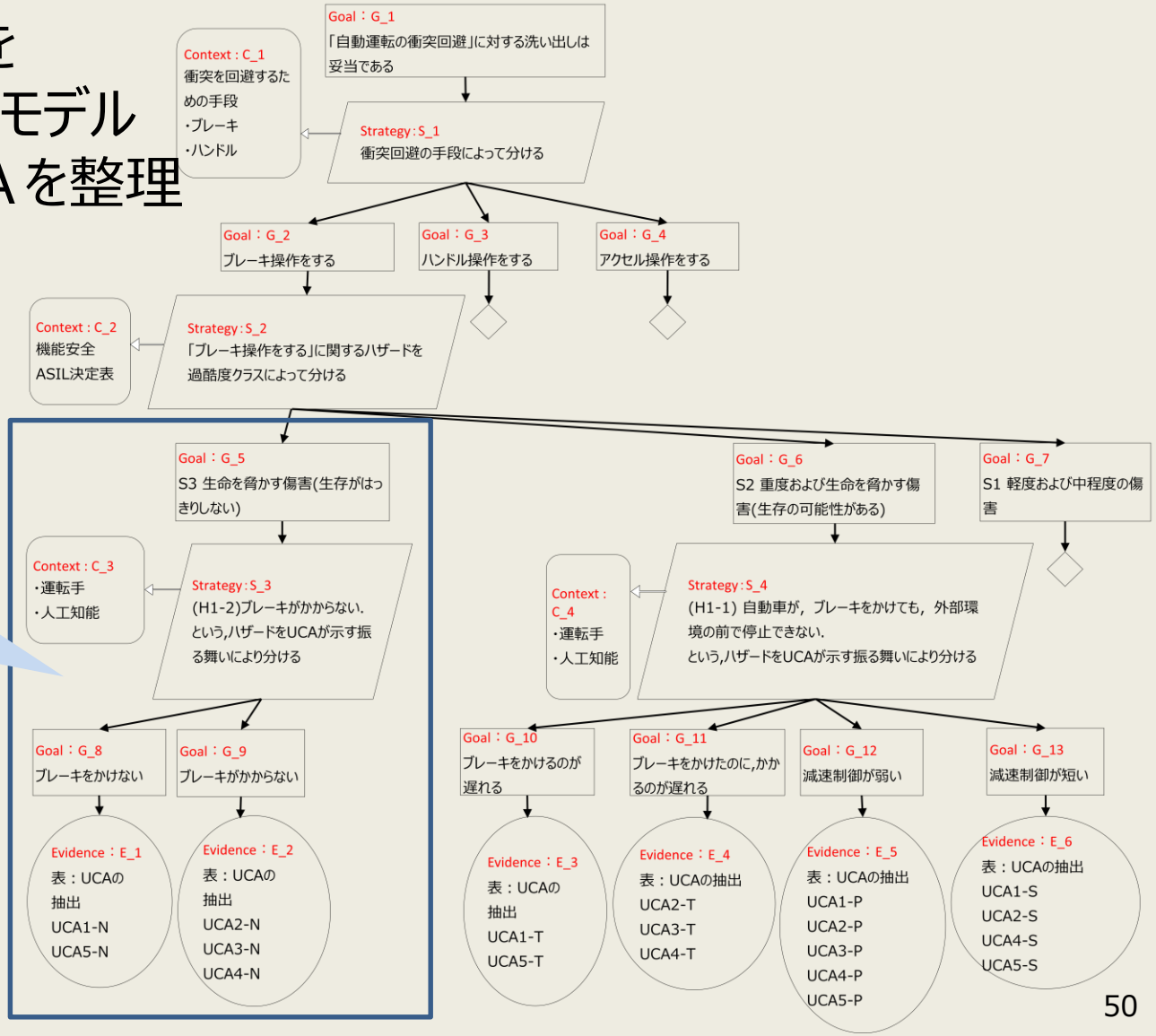
UCAx	(1)コントロール入力が外部原因のあり得る条件	(2)不適切なコントロールアルゴリズム	(3)不整合・不適切なプロセスモデル（人的エラーなど）	(4)コントロールの不良合、故障による影響	(5)[悪い影響] 不適切なフィードバック、あるいはフィードバックの欠如、フィードバックの遅れ	(6)[潜在的な誘因] 不注意な使用者の行為、または他の外部、関連の不注意性、フィードバックの遅れ	(7)[潜在的な誘因] 潜在的 - 悪い影響	(8)[悪い影響] 不適切または偶然なコントロールアクション、コントロールアクションの喪失	(9)コントロールアクションの発生、プロセス入力の生み出しあり	(10)実施間、または範囲外の場合	(11)システムレベルを考慮したプロセス入力	(S) Spoofing Identity なりすまし	(T) Tamporting 改ざん	(R) Repudiation 否認	(I) Information Disclosure 情報の漏洩	(D) Denial of Service サービス不能	(E) Elevation of Privilege 権限の昇格
UCA1-N 運転手がブレーキを踏まないと危険回避ができず、外部環境が衝突する (SC1-1)連関	・運転者などにより意図的に、運転者の急病などの発生により、ブレーキを踏まない		・運転手が正しく認識できないと、ブレーキを踏まない		・人工知能ビジョン装置の誤った認識（人などの障害物を認識しない）により、ブレーキを踏まない			・ブレーキペダルの踏込を認知する機能が欠落する					・クラウドからの情報を正しく入手しない			・人工知能ビジョン装置などの人工知能モジュールは自動運転制御時間にあるため、誤認識がある	
UCA1-P 運転手が誤ってブレーキを踏んでしまうなど、結果的に外部環境に衝突する (SC1-1)連関		・運転手がブレーキを踏み続ける						・ブレーキペダルの踏込を認知する機能が欠落する									
UCA1-T 運転手のブレーキが遅延する場合、危険回避ができず、外部環境と衝突する (SC1-1)連関	・自動運転制御装置に、故障等の危険検知が遅れる				・自動運転制御装置が、ブレーキを踏む指令を出すタイミングが遅い	・人工知能モジュールに故障が発生して異常発生時に適切な自動運転制御指令が遅れて出る	・誤ったブレーキ操作が加えられる									・人工知能モジュールにおいて異常な自動運転制御指令を出せない	
UCA1-S 誤ってブレーキを踏む機会が多くなり、衝突回避ができず外部に衝突する (SC1-1)連関			・運転手がブレーキを踏む時間が短すぎる		・自動運転制御装置がブレーキを踏んだが、人工知能モジュールへのあたりがない為に急な減速を伴う制御値（ブレーキ）の値になる												
UCA2-N 運転手がブレーキペダルを踏んでいるため減速指示を出さないと、外部環境と衝突する (SC1-2)連関		・ブレーキペダルの操作による減速指示ができず、ブレーキを踏んだと認識しない							・人工知能モジュールの異常な影響を受け、ブレーキペダルの減速指示がブレーキシステムへ適切に伝わらない								・ブレーキシステムを経由にはされず、ブレーキペダルの減速指示が受け取りやすい ・車両のかた人（知識ビジョンのインターネットなどのBOS情報）が入力されていない、誤認識が発生する ・人工知能経由で侵入された攻撃者がより、ブレーキペダルからの独立したプログラムなどされた制御を実行される
UCA2-P 運転手がブレーキペダルを踏み込んでいるため減速指示が小さい、外部環境と衝突する (SC1-1)連関		・ブレーキペダルの踏込量などを踏んだ量の情報が正しく伝わらない							・人工知能モジュールの減速指示値を誤って、中心や異常な減速制御をとる								・人工知能経由で侵入された攻撃者により、ブレーキペダルからの独立したプログラムなどされた制御を実行される
UCA2-T 運転手がブレーキペダルを踏んだタイミングが、外部環境と衝突する場合、外部環境と衝突する (SC1-1)連関		・ブレーキペダルの反応が遅い	・ブレーキペダルの踏込を減速指示に変換する処理が遅い						・人工知能モジュールの減速指示の値をブレーキペダルの減速指示の値と比較して、ブレーキペダルの減速指示を適用する								・冗長構成された人工知能モジュールとブレーキシステムがCheck処理（入力しているか、異常な応答が返ってきていないか）を行う ・人工知能経由で侵入された攻撃者により、ブレーキペダルからの独立したプログラムなどされた制御を実行される
UCA2-N 運転手がブレーキペダルを踏んでいるため減速指示の解除が出ず衝突する (SC1-1)連関		・ブレーキペダルの反応により減速指示の解除ができる							・ブレーキペダルの減速指示による減速中の人工知能モジュールの減速制御指令に、ブレーキペダルの減速指示が解除される								・人工知能経由で侵入された攻撃者により、ブレーキペダルからの独立したプログラムなどされた制御を実行される
UCA3-N 誤ってブレーキペダルを踏んだりの時または、ふかみが大きな状態になり始めた、後方が異常として外部環境と衝突する (SC1-1)連関	・ブレーキペダルからの誤った入力 ・ブレーキペダルの踏込量が大きすぎる	・ブレーキシステムの欠陥により、ブレーキペダルからの踏込量を、自動運転制御指示に変換できない ・ブレーキシステムの欠陥により、ブレーキペダルの踏込量を、自動運転制御指示に変換できない														・自動運転制御指示を受信して、車両が停止しかつ、人工知能モジュールを受信して、ブレーキペダルの踏量が大きいため、自動運転制御指示を受け付けない	・ブレーキペダルを受信して、自動運転中に、故意に自動運転停止させられる ・人工知能モジュールを受信して、偽の入力によって外部環境と自動運転制御ができない
UCA3-P 運転手が自動運転を解除していないため、自動運転制御が続き、外部環境と衝突する (SC1-2)連関	・ブレーキペダルからの誤った入力	・ブレーキシステムの欠陥により、ブレーキペダルの踏込みを自動運転制御指示に変換する処理が遅い															・ブレーキペダルを受信して、自動運転中に、故意に自動運転停止させられる ・人工知能モジュールを受信して、偽の入力によって外部環境と自動運転制御ができない
UCA3-T 運転手が手動運転に切り替えたにもかかわらず、自動運転制御解除が遅れ、自動運転制御解除指示が出ない (SC1-1)連関	・ブレーキペダルからの誤った入力 ・ブレーキペダルの踏込量が大きすぎる	・ブレーキシステムの欠陥により、ブレーキペダルの踏込みを自動運転制御指示に変換する処理が遅い	・ブレーキペダルの踏込みを自動運転制御指示に変換する処理が遅い			・人工知能モジュールに、不適切な外乱情報（Dos攻撃）があるなど、外部環境制御指示が出力される										・自動運転制御装置により、ブレーキペダルの踏込量を受信して、自動運転制御の停止を指示する ・人工知能モジュールを受信して、ブレーキペダルからの踏込量が大きいため、自動運転制御指示を受け付けない	・ブレーキペダルを受信して、手動運転中に切り替えた場合、自動運転制御の停止を指示する ・人工知能モジュールを受信して、ブレーキペダルからの踏込量が大きいため、自動運転制御指示を受け付けない
UCA3-S N/A																	
UCA4-N ブレーキペダルからの誤った入力、または人工知能モジュールからの異常な制御指示を受け取ったが、車体への減速制御が行われないと、外部環境と衝突する (SC1-1)連関	・ブレーキペダルからの誤った入力 ・人工知能モジュールからの誤った入力 ・人工知能モジュールからの誤った入力情報で、車体への減速制御が行われない	・ブレーキシステムの欠陥により、ブレーキペダルからの踏込量を、車体への減速制御に変換できない ・ブレーキシステムの欠陥により、人工知能ビジョンからの減速制御指示を、車体への減速制御に変換できない						・ブレーキシステムから車体への減速制御が行われない	・ブレーキペダルからの異常指示 ・人工知能モジュールからの異常な指示の複合により、車体への減速制御が行われない							・人工知能を評価したの人工知能モジュールからの異常指示により、ブレーキシステムをダウンさせる	・ブレーキシステム単体でも車体への減速制御が行われない
UCA4-P ブレーキペダルからの誤った入力、または人工知能モジュールからの異常な制御指示を受け取ったが、車体への減速制御が行われないため、車体への減速制御が想定よりも小さく、外部環境と衝突する (SC1-1)連関	・ブレーキペダルからの誤った入力 ・人工知能モジュールからの異常な制御指示	・ブレーキペダルからの踏込量を、車体への減速制御に変換できる範囲よりも小さい値で変換する ・人工知能モジュールからの減速制御指示を、車体への減速制御に変換できない							・ブレーキペダルと人工知能モジュールからの減速制御指示を合成する際に、人工知能の減速制御を採用しているが、ブレーキペダルからの減速制御が無くなる								・ブレーキシステム単体でも車体への減速制御が行われないため、車体への減速制御を優先よりも弱く行う
UCA4-T ブレーキペダルからの減速指示、または人工知能ビジョンからの減速制御指示は適切、車体への減速制御が遅れ、外部環境と衝突する (SC1-1)連関	・ブレーキペダルからの減速指示が遅い、車体への減速制御に遅れる ・人工知能ビジョンからの減速制御が遅い	・ブレーキペダルからの減速指示を、車体への減速制御に変換するタイミングが遅れる ・人工知能モジュールからの減速制御を、車体への減速制御に変換するタイミングが遅れる ・人工知能モジュールからの減速指示が、ブレーキシステムの不具合により、車体への減速制御が遅れる							・ブレーキペダルからの減速指示と、人工知能からの減速指示の合成により、車体の減速制御が遅れる								・ブレーキシステム単体でも車体への減速制御が行われない
UCA4-S ブレーキペダルからの誤った入力、または人工知能モジュールからの減速制御指示が遅れ、車体への減速制御が遅れ、外部環境と衝突する (SC1-1)連関	・ブレーキペダルからの誤った入力 ・人工知能モジュールからの減速制御指示が遅い	・ブレーキペダルからの減速指示を、車体への減速制御に変換するタイミングが遅れる ・人工知能モジュールからの減速制御を、車体への減速制御に変換するタイミングが遅れる ・人工知能モジュールからの減速指示が、ブレーキシステムの不具合により、車体への減速制御が遅れる							・ブレーキペダルからの減速指示と、人工知能からの減速指示の合成により、車体の減速制御が遅れる								・ブレーキシステム単体でも車体への減速制御が行われない
UCA5-N 車体が停車状態、または人工知能モジュールから停止指示（以降）がない状態から、外部環境と衝突する (SC1-1)連関	・自動運転制御装置が誤り（転倒やすべてないなど）制御の異常により、ブレーキペダルの異常（以降）がない状態から、外部環境と衝突する (SC1-1)連関	・人工知能の欠陥（＝プログラムバグ）があり、人工知能モジュールから停止指示が出ていない			・センシングシステムの誤りがあり、人工知能モジュールが正しい判断ができず、停止指示が出なかった	・ローカルダイナミックマップ上の誤りがあり、人工知能モジュールが正しい判断ができず、停止指示が出なかった		・人工知能の欠陥（＝プログラムバグ）があり、人工知能モジュールから停止指示が出ない	・自動運転制御装置が誤り（転倒やすべてないなど）制御の異常により、ブレーキペダルの異常（以降）がない状態から、外部環境と衝突する (SC1-1)連関		・悪意のある第三者がクラウドの情報を改ざんし、外部環境を異常情報に変換し、人工知能モジュールに入力、停止指示が出ない		・悪意のある第三者がDos攻撃などにより、人工知能モジュールに入力、停止指示が出ない	・悪意のある第三者の人工知能の脆弱性を悪用などにより、人工知能モジュールに入力、停止指示が出ない
UCA5-P 車体が停車状態、または人工知能モジュールから停止指示（以降）がない状態異常状態（さまざまな制御）の場合、外部環境と衝突する (SC1-1)連関		・人工知能の欠陥（＝プログラムバグ）があり、人工知能モジュールから誤った減速制御となる			・センシングシステムの誤りがあり、人工知能モジュールが誤った減速制御となる	・ローカルダイナミックマップ上の誤りがあり、人工知能モジュールが誤った減速制御となる		・人工知能の欠陥（＝プログラムバグ）があり、人工知能モジュールから誤った減速制御となる		・悪意のある第三者がクラウドの情報を改ざんし、外部環境を異常情報に変換し、人工知能モジュールに入力、誤った減速制御となる		・悪意のある第三者がDos攻撃などにより、人工知能モジュールに入力、誤った減速制御となる	・悪意のある第三者の人工知能の脆弱性を悪用などにより、人工知能モジュールに入力、誤った減速制御となる
UCA5-S 車体が停車状態、または人工知能モジュールから誤った減速制御（さまざまな制御）の場合、外部環境と衝突する (SC1-1)連関	・自動運転制御装置の異常により（転倒やすべてないなど）制御の異常により、ブレーキペダルの異常（以降）がない、人工知能の指示（さまざまな）がない、人工知能の指示（正常）、もしくは、誤った制御が出力される	・人工知能の欠陥（＝プログラムバグ）があり、人工知能モジュールから誤った減速制御となる			・センシングシステムの誤りがあり、人工知能モジュールが正しい判断ができず、誤った減速制御となる	・ローカルダイナミックマップ上の誤りがあり、人工知能モジュールが正しい判断ができず、誤った減速制御となる		・人工知能の欠陥（＝プログラムバグ）があり、人工知能モジュールから誤った減速制御となる						
UCA6-N 車両が停車状態、または人工知能モジュールからの後退指示（以降）がない状態から、外部環境と衝突する (SC1-1)連関	・自動運転制御装置の異常により（転倒やすべてないなど）制御の異常により、ブレーキペダルの異常（以降）がない、人工知能の指示（さまざまな）がない、人工知能の指示（正常）、もしくは、誤った制御が出力される	・人工知能の欠陥（＝プログラムバグ）があり、人工知能モジュールからの後退指示が出ない			・センシングシステムの誤りがあり、人工知能モジュールが正しい判断ができず、後退指示が出ない	・ローカルダイナミックマップ上の誤りがあり、人工知能モジュールが正しい判断ができず、後退指示が出ない		・人工知能の欠陥（＝プログラムバグ）があり、人工知能モジュールから後退指示が出ない		・悪意のある第三者がクラウドからの情報を改ざんし、外部環境を異常情報に変換し、人工知能モジュールに入力、後退指示が出ない		・悪意のある第三者がDos攻撃などにより、人工知能モジュールに入力、後退指示が出ない	・悪意のある第三者の人工知能の脆弱性を悪用などにより、人工知能モジュールに入力、後退指示が出ない

ＵＣＡを整理　全体像

3.3. ハザード分析
対策立案プロセス

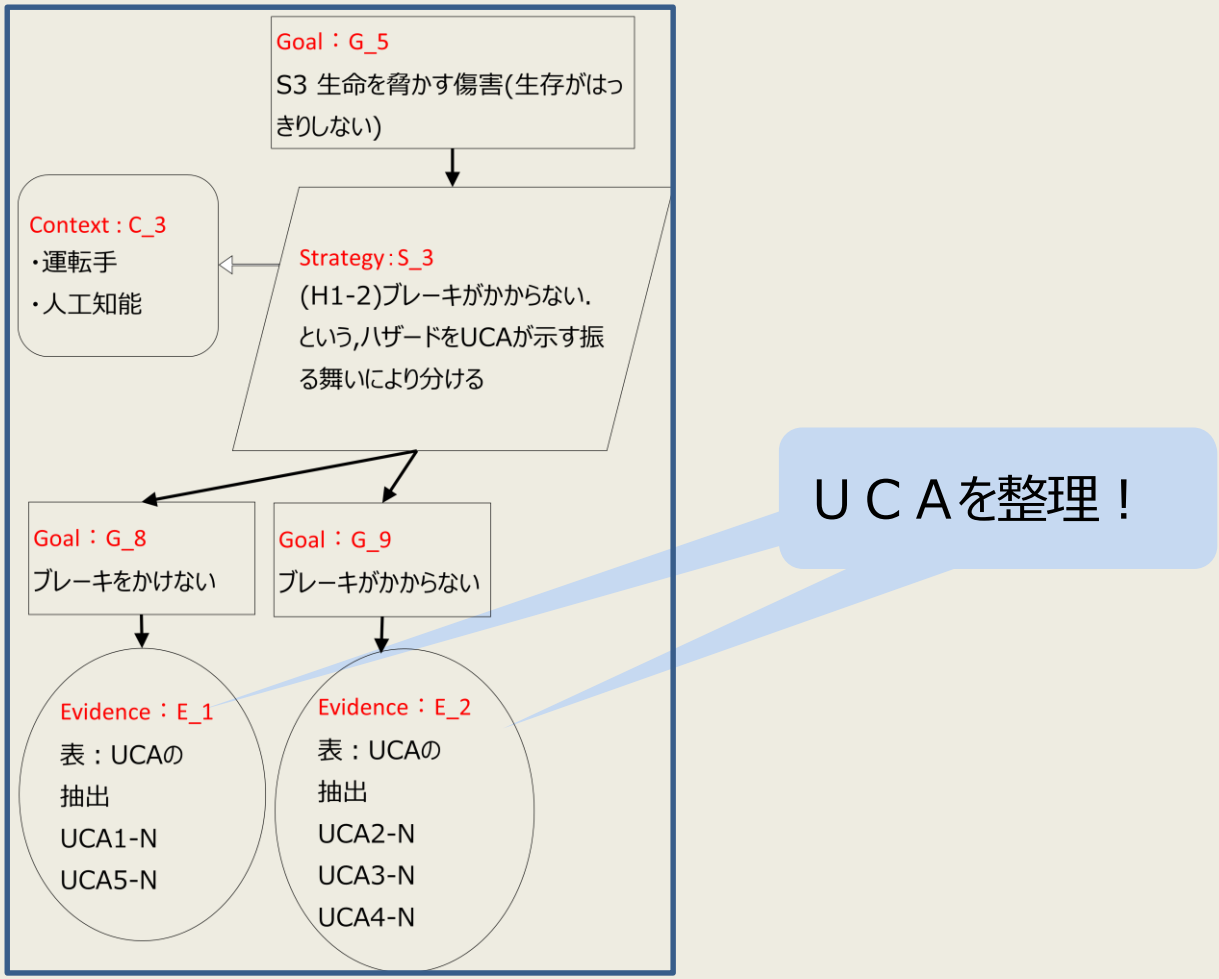
- 抽出したハザードを CC-Caseの具体モデルに基づき，ＵＣＡを整理した全体像

「生命を脅かす障害」部分を拡大！



ＵＣＡを整理　具体例

- ＡＳＩＬ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.



ＡＳＩＬ分析結果と対策

3.3. ハザード分析
対策立案プロセス

- ＵＣＡ毎に整理したＡＳＩＬ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 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UCA	HCF	評価指標 ＡＳＩＬ決定値	対策内容
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 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

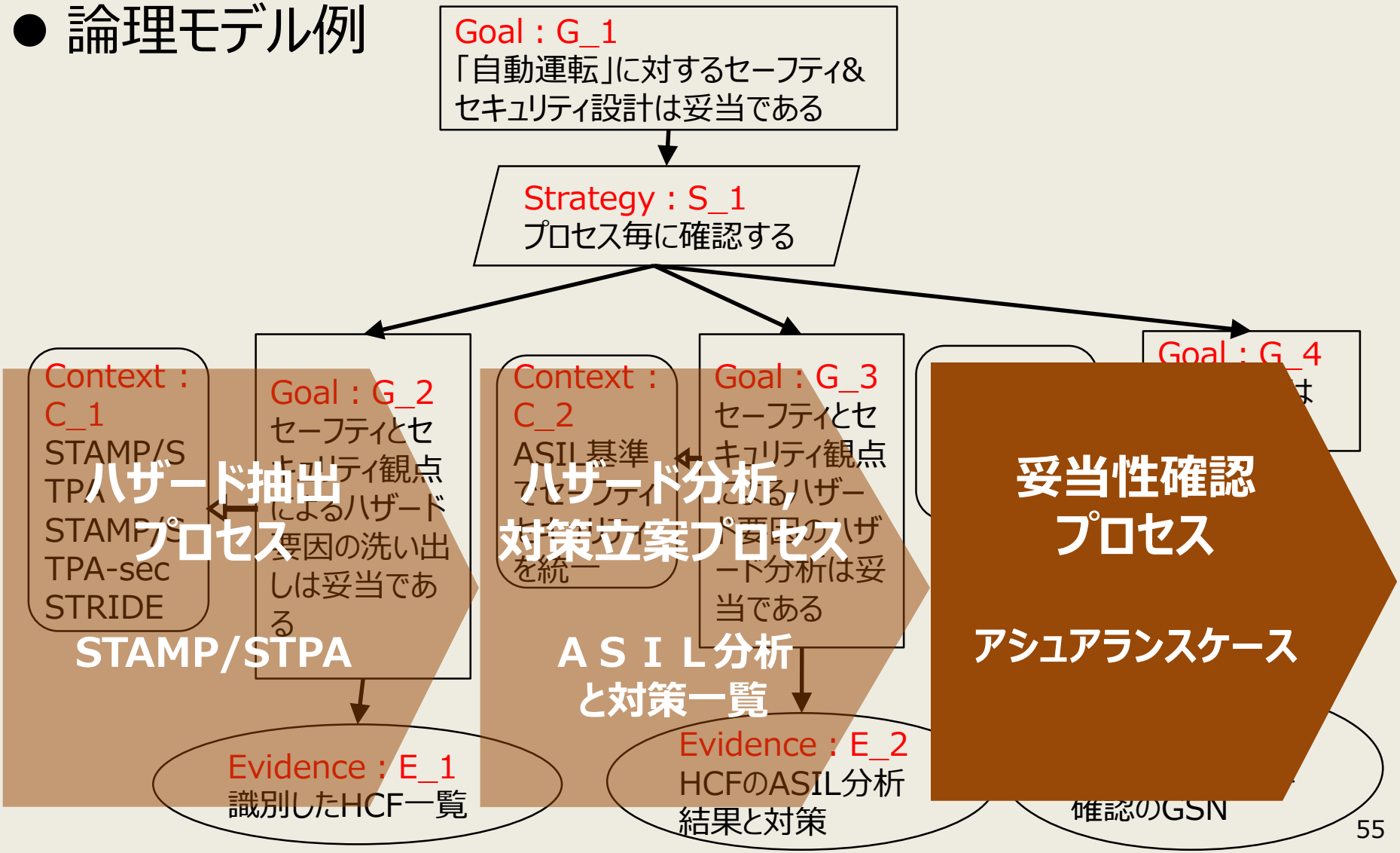
対策が十分か，
社内合意を取る

目次

保証全体像

3.4. 妥当性確認プロセス

- 論理モデル例



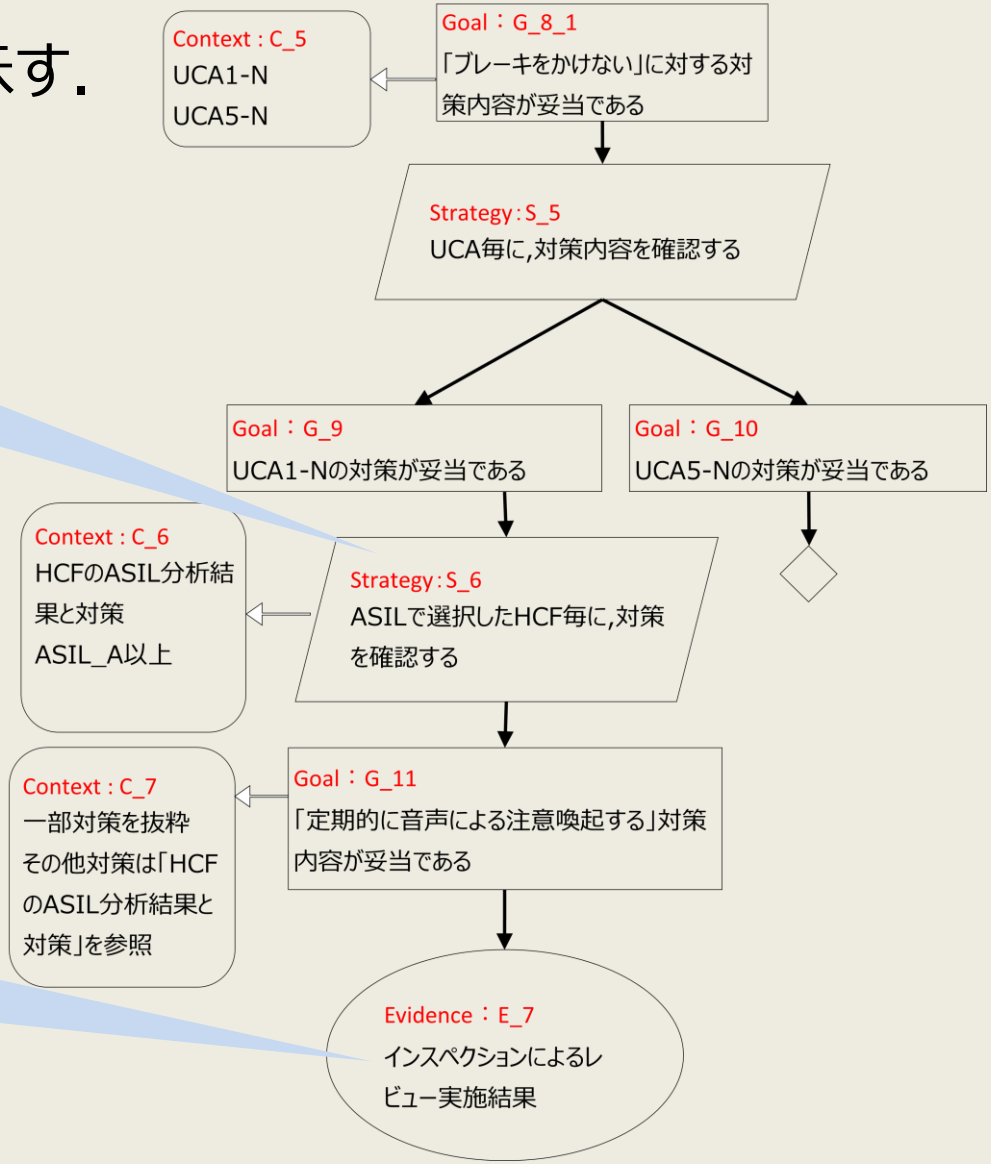
対策内容の妥当性を確認

3.4. 妥当性確認プロセス

- 対策内容が妥当かを示す.

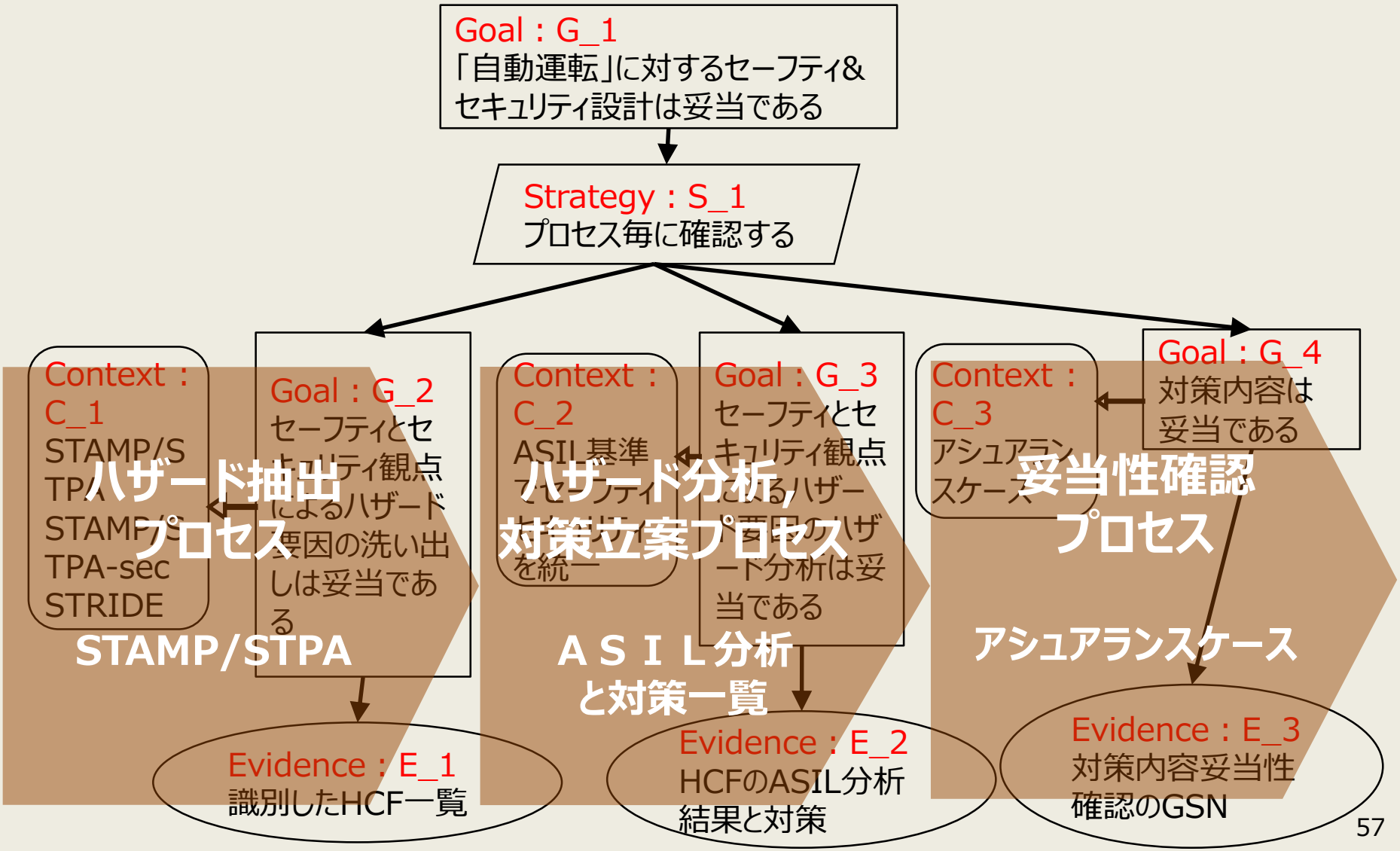
ASIL_A～Dについて,
対策内容が妥当か確認

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

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

謝辞

5. 最後に

ご指導を頂きました

金子主査，髙橋副主査，勅使河原アドバイザ

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