Business Cube & Partners

安全認証に向けたシステムズエンジニアリングの活用

※本資料は「オートモーティブソフトウェアフロンティア2018 」で発表された内容の一部を抜粋したものです

ビジネスキューブ・アンド・パートナーズ株式会社

本日のアジェンダ

Business Cube & Partners

- 会社紹介
- システムズエンジニアリングの活用
  - システムズエンジニアリング活用の背景
  - STAMP/STPAによるハザード分析
  - 適用の流れ
- まとめ

本日のアジェンダ

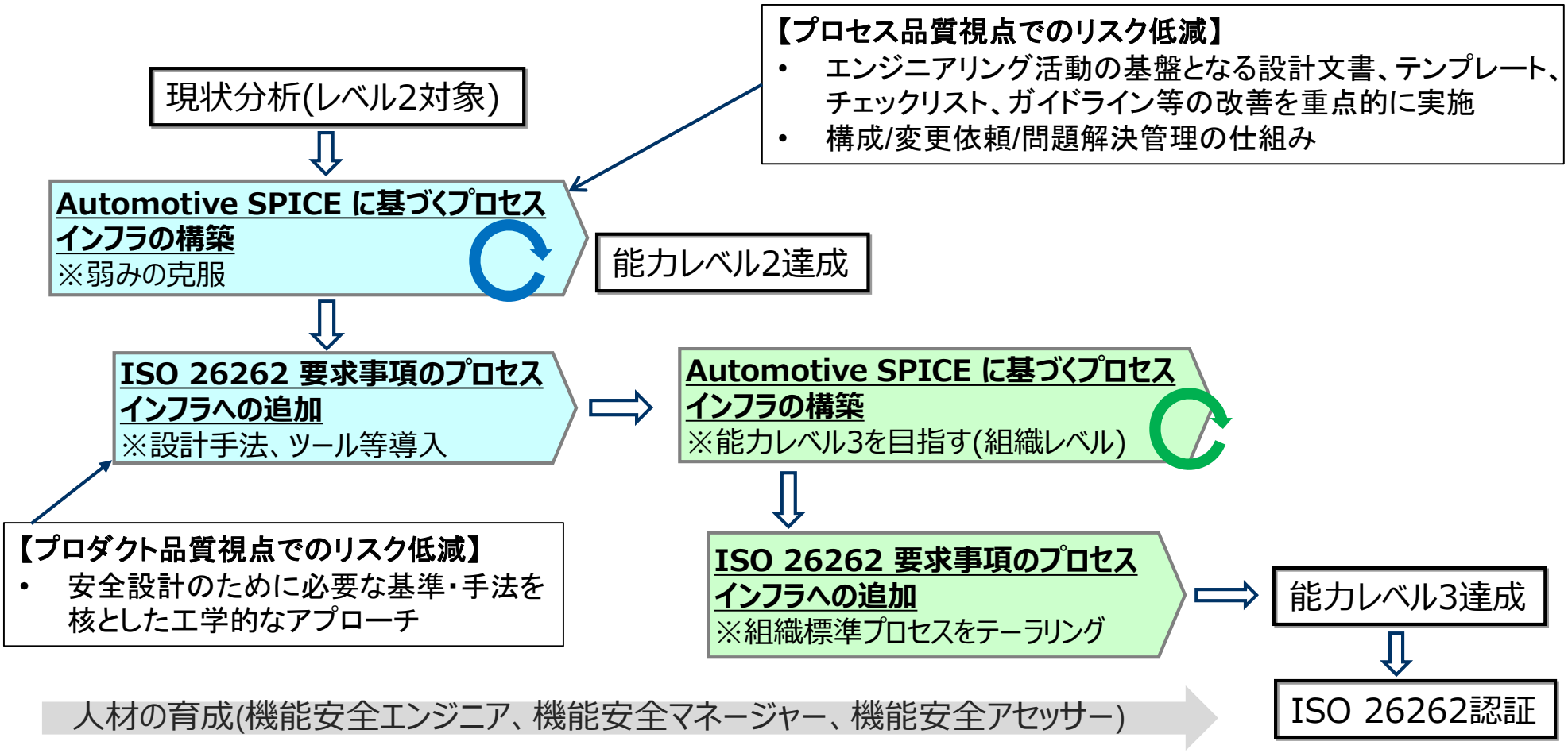
Business Cube & Partners

- 会社紹介
- システムズエンジニアリングの活用
  - システムズエンジニアリング活用の背景
  - STAMP/STPAによるハザード分析
  - 適用の流れ
- まとめ

システムズエンジニアリング活用の背景

Business Cube & Partners

- ISO 26262対応に向けた下地作りのアプローチ



システムズエンジニアリング活用の背景

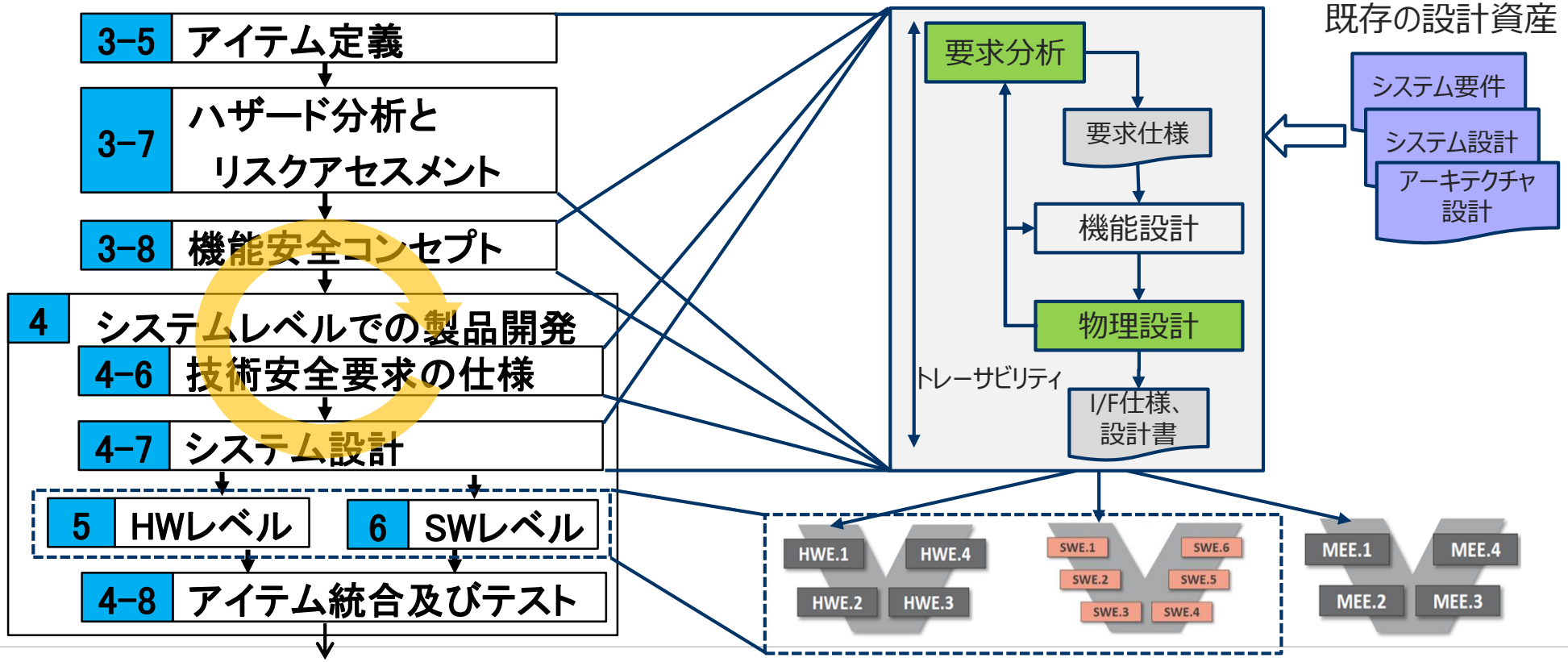
Business Cube & Partners

- 前述の「ISO 26262対応に向けた下地作りのアプローチ」を通して、お客様のプロジェクトから見えた多くの課題(プロセスの側面以外)：
  - システムの要求分析、システム要件定義、機能分割、コンポーネントへの割り当て、アーキテクチャ設計間の連続性が切れている
    - 文書ベースで情報が漏れている
    - アプリケーションデータ(適合データ以外で特に、コンフィギュレーションを決めるパラメータ)が、実装工程で、登場する(自動車のバリエーション、プロダクトライン)
  - ソフトウェアアーキテクチャ設計の根拠が明確になっていない
    - 複数候補からの選択理由が残っていない
  - トレーサビリティが部分的にしか取れていない
    - 詳細設計とソースコード、テストケースは取れていることが多いが、要件、アーキテクチャ間のトレーサビリティが取れていない
  - 納期が遅れる傾向にある
    - 課題管理はしているが、課題の分析が不十分

システムズエンジニアリング活用の背景

Business Cube & Partners

- 安全設計のために必要な基準・手法を核とした工学的なアプローチが不十分
  - 安全性解析(ハザード分析、リスクアセスメント)
  - 機能安全ゴール→機能安全要求→機能安全コンセプト



システムズエンジニアリング活用の背景

Business Cube & Partners

- 前述の課題を整理した結果、必要なソリューション：
  - 要求分析から、システム要件、機能定義、アーキテクチャ設計、機能とアーキテクチャ設計の割り当てを、サブシステム、コンポーネントレベルに、段階的に設計を進め、かつ、上位に戻って容易に変更ができる手段
    - バリエーションを考慮した設計
  - 各システム設計レベルに応じた分析・解析手段を適用
    - システム設計情報を安全性解析に使用
  - セーフティケースなど構造化された議論に展開する(GSN)

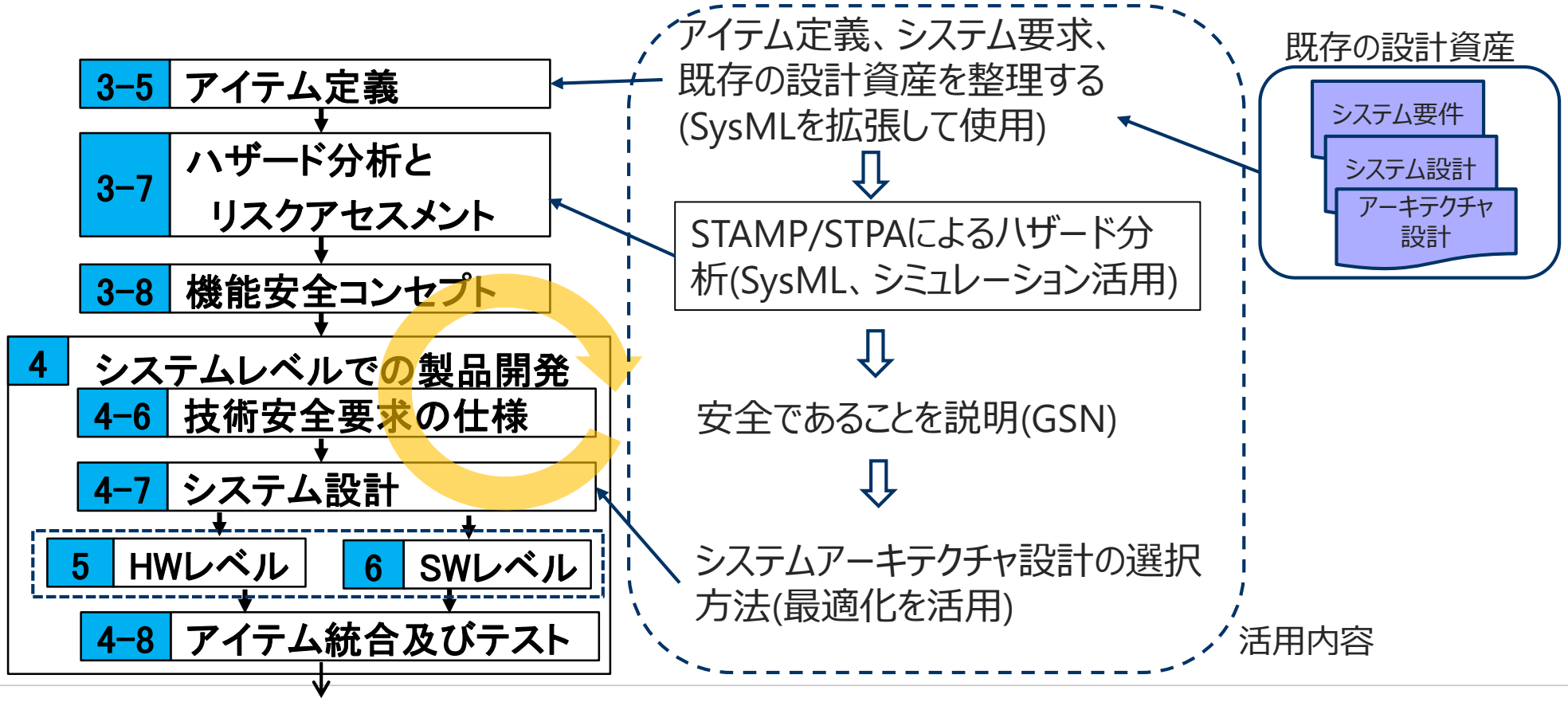
⇩

- モデルベースシステムズエンジニアリング(MBSE)のアプローチが必要
  - 要求分析、機能定義、アーキテクチャ設計をセットにした設計
  - 安全性解析手法、検証手段と連携
  - アーキテクチャ選択の思考

システムズエンジニアリング活用の背景

Business Cube & Partners

- どのような活用をしていくか？
  - SysMLは一つの道具なので、仕立てる：用途に合わせて、SysML表記を拡張
  - シミュレーション環境、最適化技術＋データ(PLM、実測データ)と連携



本日のアジェンダ

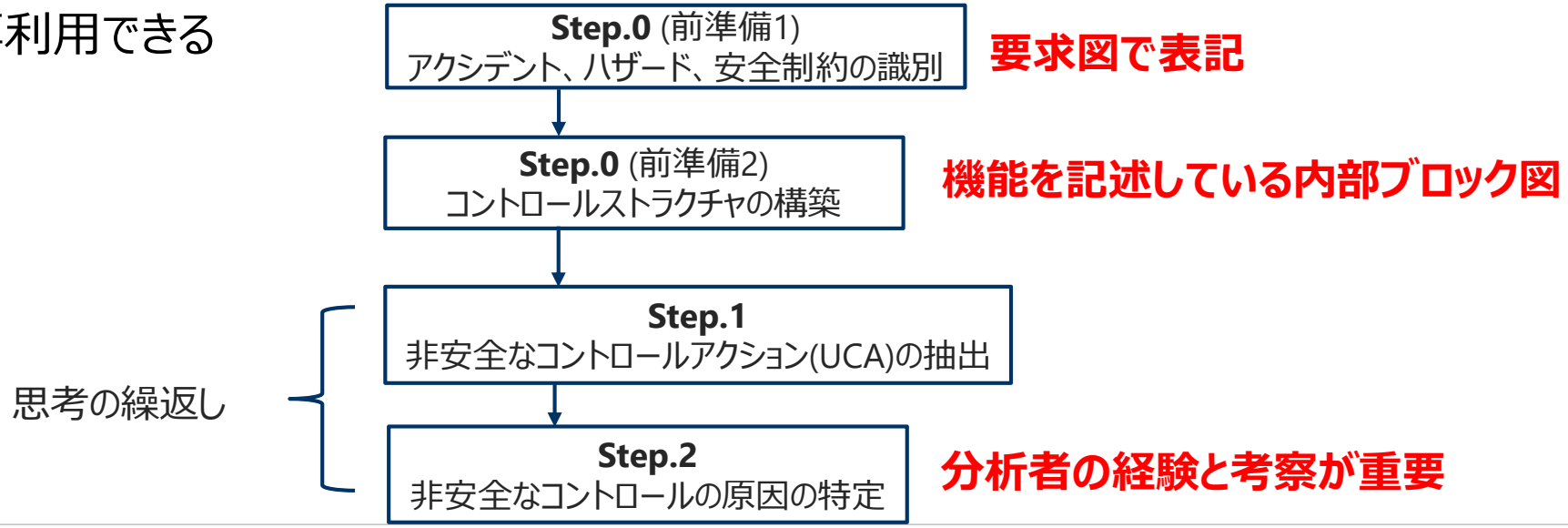
Business Cube & Partners

- 会社紹介
- システムズエンジニアリングの活用
  - システムズエンジニアリング活用の背景
  - STAMP/STPAによるハザード分析
  - 適用の流れ
- まとめ

STAMP/STPAによるハザード分析

Business Cube & Partners

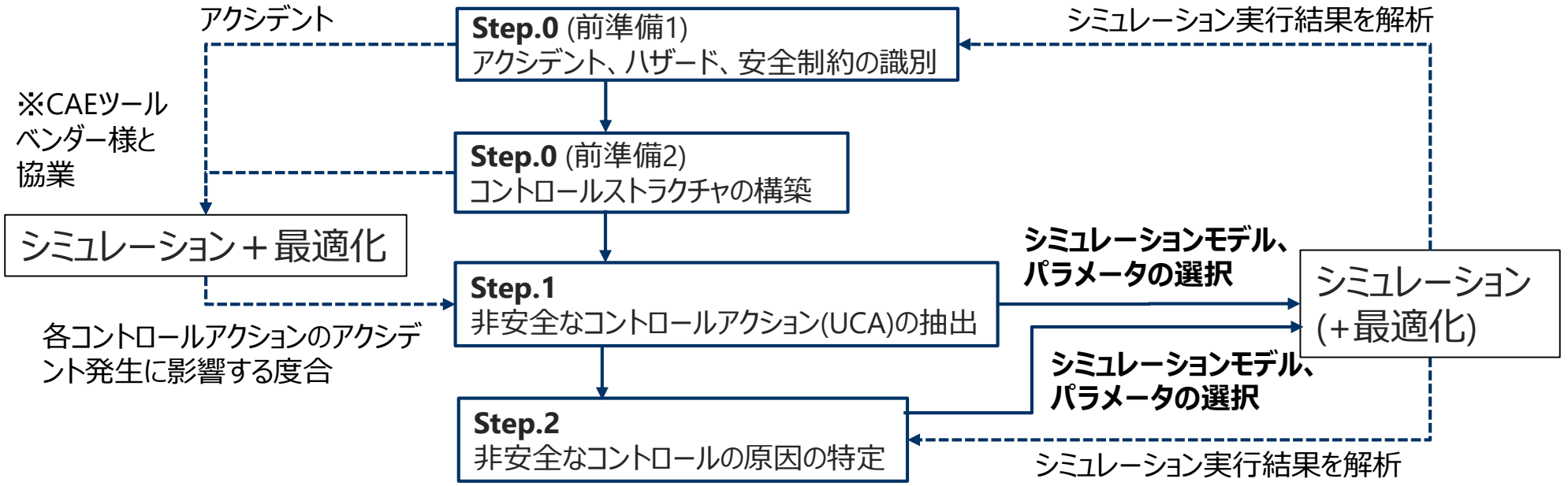
- STPAによる解析
  - システム全体から対象とするシステムまで、少しずつフォーカスをあてる(システムズエンジニアリングアプローチとの相性が良い)
  - ただし、ハザードの原因を特定するのに、経験や考察が重要
- 環境条件を見える化し、シミュレーションを併用して検討することにより、想定外を防止していきたい
  - 既存の開発プロジェクトをベースにした開発では、開発資産のシミュレーションモデルが再利用できる



STAMP/STPAによるハザード分析

Business Cube & Partners

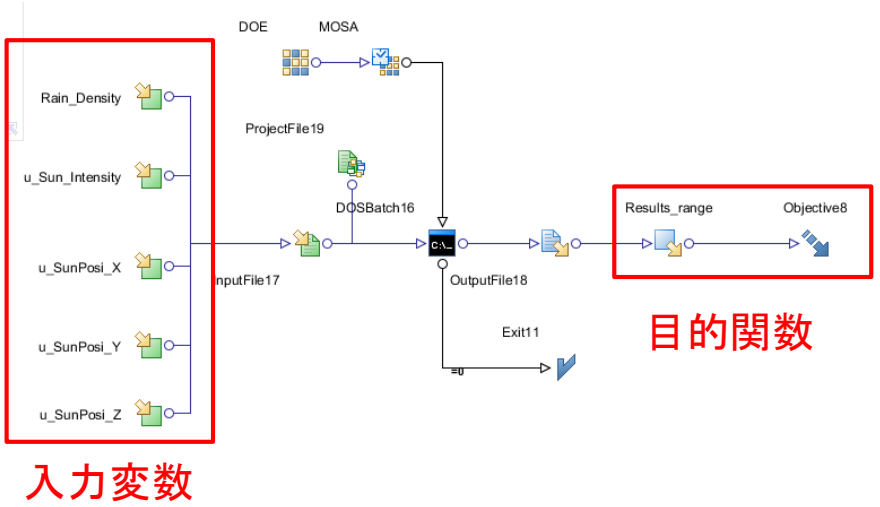
- シミュレーションを適用する分析：
  1. アクシデントの発生に関係する因子を最適化手法との組合せで探る
  2. 被制御対象にフォーカスしたシミュレーション
     - ガイドワードに沿って、その性質を生成する振舞いモデル
     - 振舞いの特性を決めるパラメータ
     - システムに影響を与える外部パラメータ(環境)



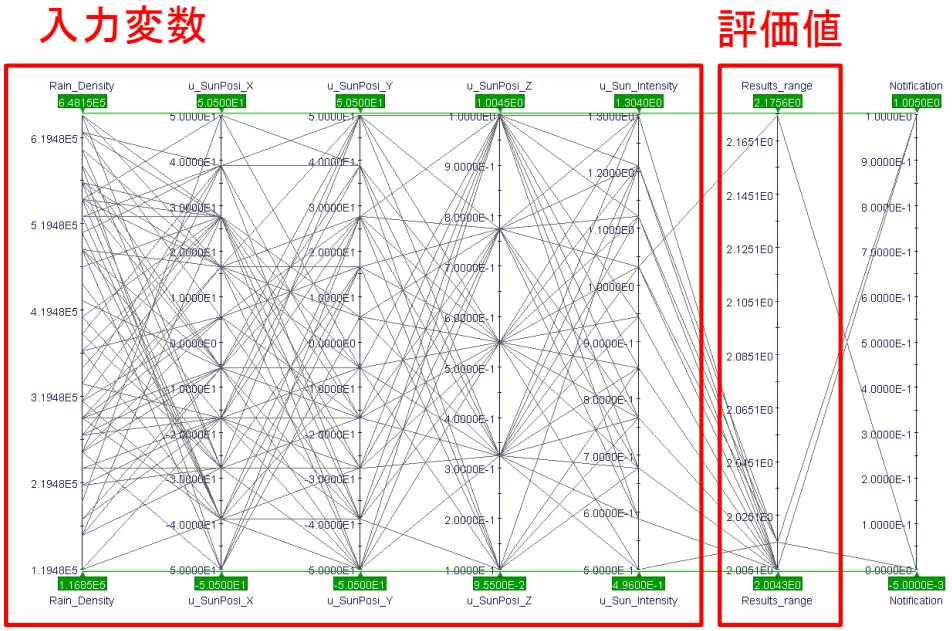
STAMP/STPAによるハザード分析

Business Cube & Partners

1. アクシデントの発生に関係する因子を最適化手法との組合せで探る
   - アクシデントを定量化し、その値を最大化、もしくは、最小化する入力の組み合わせを探す
     - アクシデントの定量化ができないケースもある
   - アクシデントの定量化例：
     - “前方の車両に追突する” ⇒ 前方車両との“距離”を最小化する入力を探索する



※CAEツールベンダー様の協力

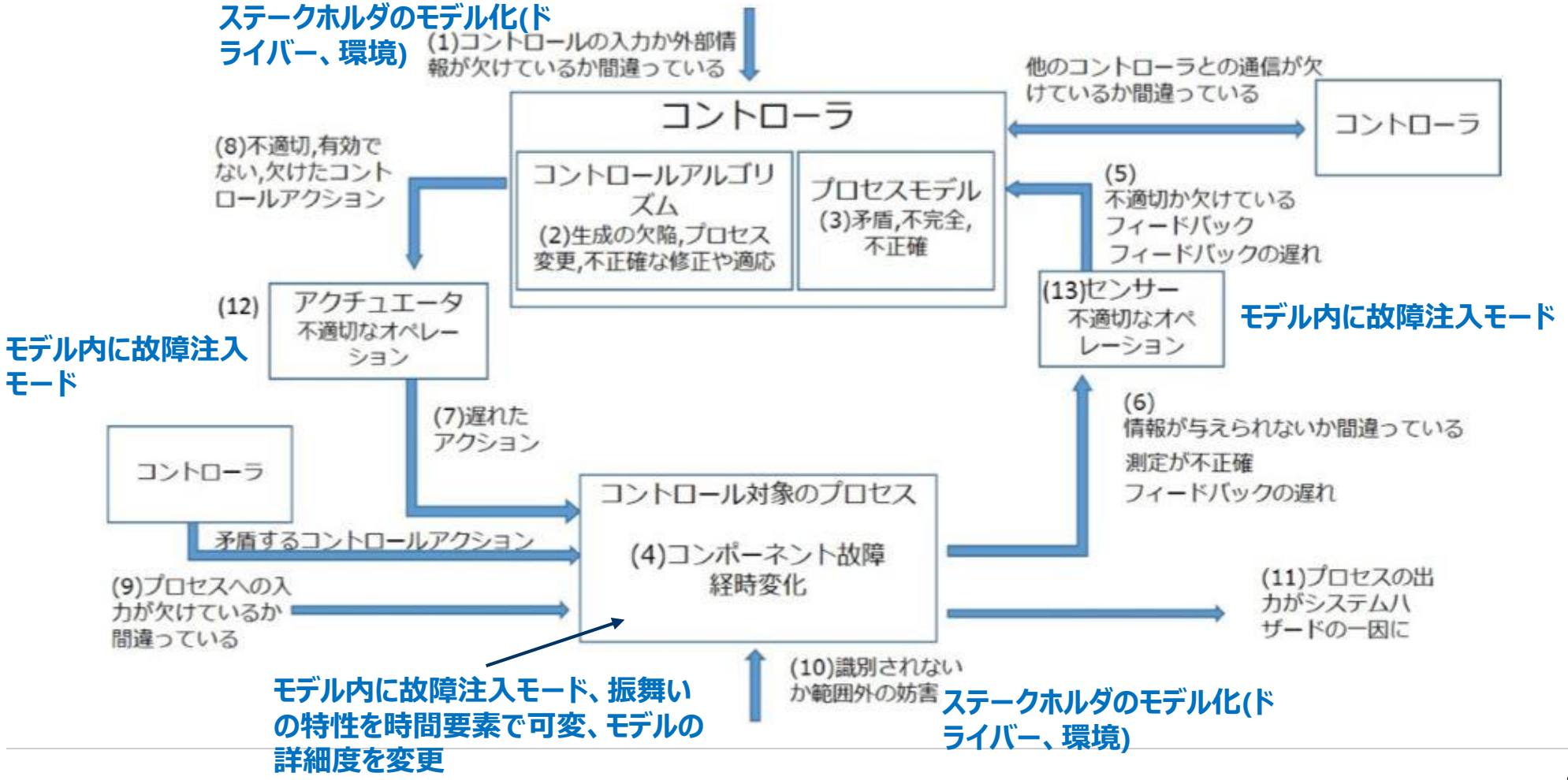


STAMP/STPAによるハザード分析

Business Cube & Partners

2. 被制御対象にフォーカスしたシミュレーション

- ハザード要因の特定を支援するガイドワードを考慮したモデル作成



本日のアジェンダ

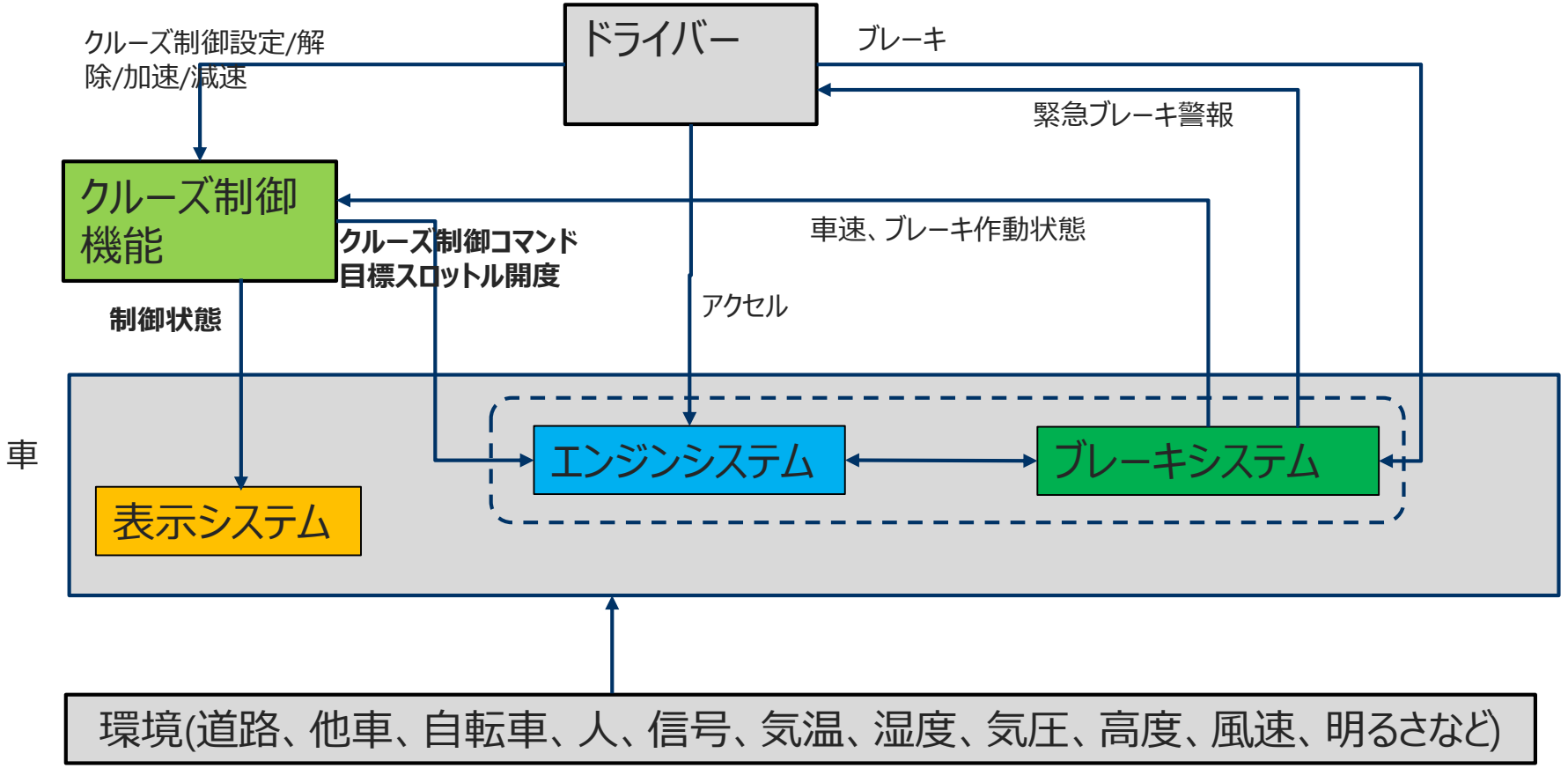
Business Cube & Partners

- 会社紹介
- システムズエンジニアリングの活用
  - システムズエンジニアリング活用の背景
  - STAMP/STPAによるハザード分析
  - 適用の流れ
- まとめ

適用の流れ

Business Cube & Partners

- 例：クルーズコントロール機能
  - 登場人物：ドライバー、クルーズ制御機能、車(エンジンシステム、ブレーキシステム、表示システム)、環境



適用の流れ

Business Cube & Partners

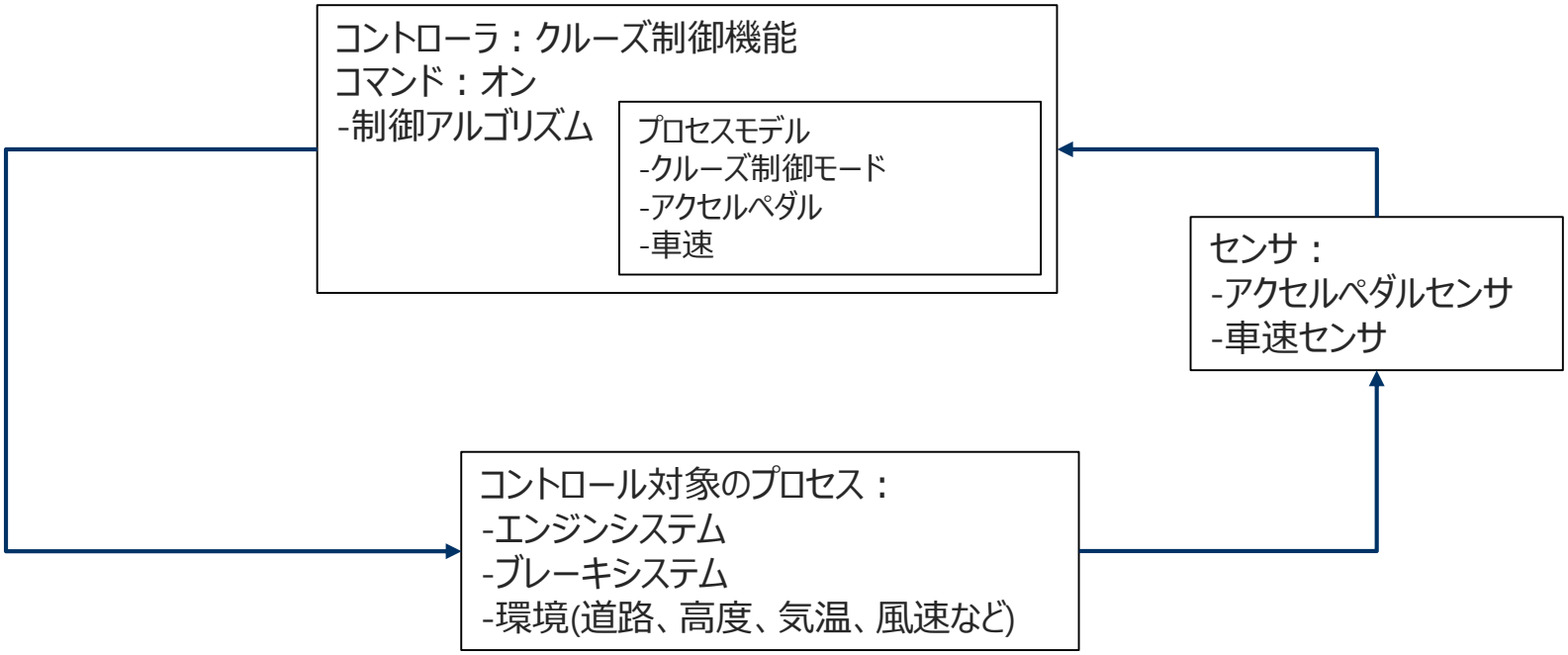
- アクシデント
  - Acc1：前方の車両に追突する
- ハザード
  - Hz1：クルーズ制御作動中に車両が加速
- 安全制約
  - Sc1：クルーズ制御作動中は、設定車速を超えてはならない
- UCAの識別

No	コントロールアクション	Not Providing	Providing causes hazards	Too early/Too late	Stop too soon/Applying too long
1	クルーズ制御コマンド	・ブレーキ踏んで減速中にオフコマンドが出力されない(UCA_01) ・アクセルペダル踏んで加速中にオフコマンドが出力されない(UCA_02)	**・オンコマンドが出力されるが、車両が加速する**(UCA_03)	・ドライバーがセットする前に、クルーズ制御がオンになる	
2	目標スロットル開度	・オンコマンド出力中に、範囲内の目標開度値が出力されない	・常に全開指示がでる		・設定車速に達しても目標開度が変わらない
3	制御状態	・制御状態が送信されない			

適用の流れ

Business Cube & Partners

- UCAの要因を特定する
  - UCA：“オンコマンドが出力されるが、車両が加速する”
    - クルーズ制御が実行されていると、車両速度は目標速度に追従する



このUCAに対して、コントロールストラクチャに
相当するモデルを被コントロール対象にする

適用の流れ

- シミュレーションモデルの準備とポイント
  - 被コントロール対象に、複数のシステム「エンジン」、「車両」モデルを含む
    - それぞれのモデルの抽象度(振舞いレベル)を考える
      - クルーズ制御機能から見てエンジンは、スロットル要求に基づいて、トルクが変動するレベル(特性マップでの振舞い)
      - 車両(ブレーキ)モデルからエンジンを見ると、ブレーキ作動時のエンジンモデルは、点火も考慮したい
    - 【注意】 振舞いを厳密に数式でモデル化している場合、モデル特性を決めるパラメータを自由に変更すると、シミュレーション計算上の不整合(計算の発散、不安定)になるケースもある
  - シミュレーションモデル内のパラメータの選択
    - 「環境」に関わるパラメータは、基本的にシミュレーションで変更する対象にする
      - 現実にあり得ない状況の組み合わせをカバーすることはできるが、そこまで要求されない

適用の流れ

Business Cube & Partners

- シミュレーション結果を分析し、コントロールループで安全制約が破られる原因のガイドワードに分類してみる

	①上位からの指示や外部情報の誤り・欠落	②不適切なコントロールアクション	③不整合、不完全又は、不正確なプロセスモデル	④コンポーネントの故障・経年変化	⑤不適切なフィードバック(遅れ、喪失)	⑥不正確な情報の供給、情報の欠如	⑦操作の遅れ	⑧不適切なコントロールアクション	⑨コントロールアクションの喪失	⑩未確認、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	⑫アクチュエータの動作が不十分	⑬センサの動作が不十分
UCA_01													
UCA_02													
UCA_03:**オンコマンドが出力されるが、車両が加速する**		スロットル開度値が範囲外を出力						ブレーキシステムから、ABS作動時のトルク制御と同時要求		クルーズ制御が勾配のきつい下り坂でオン			

本日のアジェンダ

Business Cube & Partners

- 会社紹介
- システムズエンジニアリングの活用
  - システムズエンジニアリング活用の背景
  - STAMP/STPAによるハザード分析
  - 適用の流れ
- まとめ

まとめ

Business Cube & Partners

- 本セッションで、お話したこと：
  - ISO 26262対応に向けた下地作りのアプローチを通して、見えた課題に対して、システムズエンジニアリングを活用する流れを紹介した
  - その中で、STAMP/STPAによるハザード解析に、シミュレーションと最適化技術を活用し、分析者の思考を支援する方法を紹介した

- これから更に、システムズエンジニアリングを活用していく
  - 安全要求、コスト(PLMデータ)、再利用性(プロダクトライン)を観点に入れたアーキテクチャ設計と複数のアーキテクチャ設計からの選択決定手段を体系化する

Business Cube & Partners

お問合せは下記までお気軽にご連絡ください。

ビジネスキューブ・アンド・パートナーズ株式会社
コンサルティング事業部
consulting@biz3.co.jp
http://biz3.co.jp