HITACHI
Inspire the Next

第２回 STAMP Workshop in Japan

28 November, 2017

システムモデルを用いたSTAMP/STPA試行の事例紹介

株式会社 日立産業制御ソリューションズ
橋本　岳男
Takeo Hashimoto
Embedded Systems Engineering Group
Hitachi Industry & Control Solutions, Ltd.

HITACHI
Inspire the Next

Contents

1. 会社紹介
2. Motivation
3. システムモデルについて
4. ドライバ異常時安全停車システム（事例紹介）
5. まとめ

HITACHI
Inspire the Next

Contents

HITACHI
Inspire the Next

株式会社　日立産業制御ソリューションズ

- 代表者：取締役社長　木村 亨
- 資本金：30 億円
  （日立製作所 100%出資）
- 設立　：2014年4月
- 社員数：3, 752 名（2017年4月）
- 本社
  - 茨城本社　茨城県日立市
  - 東京本社　東京都台東区（秋葉原大栄ビル）

【他の拠点】
・事業拠点：6 ヵ所
・営業拠点：8 ヵ所

日立グループの産業ソリューション事業における中核企業

産業ソリューション
・製造管理（自動車等）
・ガス/プラント監視制御
・SAP® *1エンジニアリング
・医薬品製造管理システム
・自動車製造管理システム

組込みエンジニアリング
・車載情報システム
・車両制御システム
・画像処理・認識
・組込みソフト・ハード　国内シェア 6位*2

システムエンジニアリング
・情報システム（金融他）
・プラントエンジニアリング
・ビッグデータ解析
・自治体向け通信システム
・鋳造シミュレーション

セキュリティソリューション
・フィジカルセキュリティ
・モニタリング（カメラ）
・映像配信ソリューション
・指静脈認証装置
国内シェア 1位（41%）*3

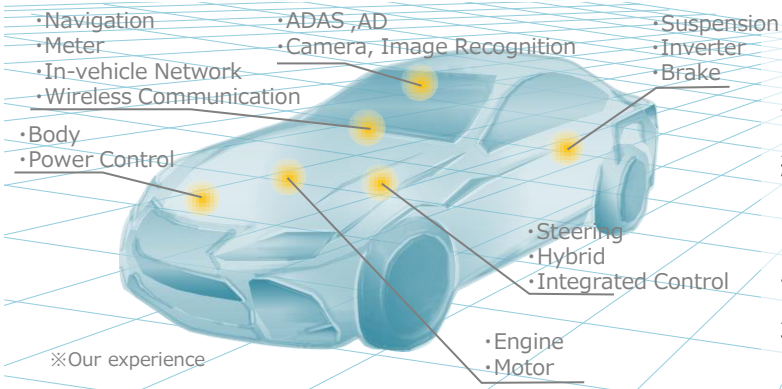
*1 SAPは、SAP AGのドイツおよびその他の国における登録商標または商標です。
*2 組込みソフト事業ミック経済研究所調べ（エンベデットシステム・ソリューション市場：2015年度実績）
*3 富士経済調べ（2016年セキュリティ関連市場の将来展望：2015年度実績）

1. 会社紹介

HITACHI
Inspire the Next

私たちは、お客さまが開発現場で抱えるさまざまな課題を解決する

”Engineering Service Provider” です。



自動車システムの高度化・複雑化により、
安全性や利便性の向上に関わる
組込み技術の重要性が高まっています。
当社は、長年培ってきた組込み技術と車両制御、
車載情報機器開発で蓄積した技術を融合し、
最適化した自動車開発ソリューションを提供します。

組込み技術　**機能安全**　**セキュリティ**

■ **自己紹介**　**橋本岳男(Takeo Hashimoto)**
業務経歴　**無線通信システム開発従事後、現在は、自動車制御システム開発担当**

HITACHI
Inspire the Next

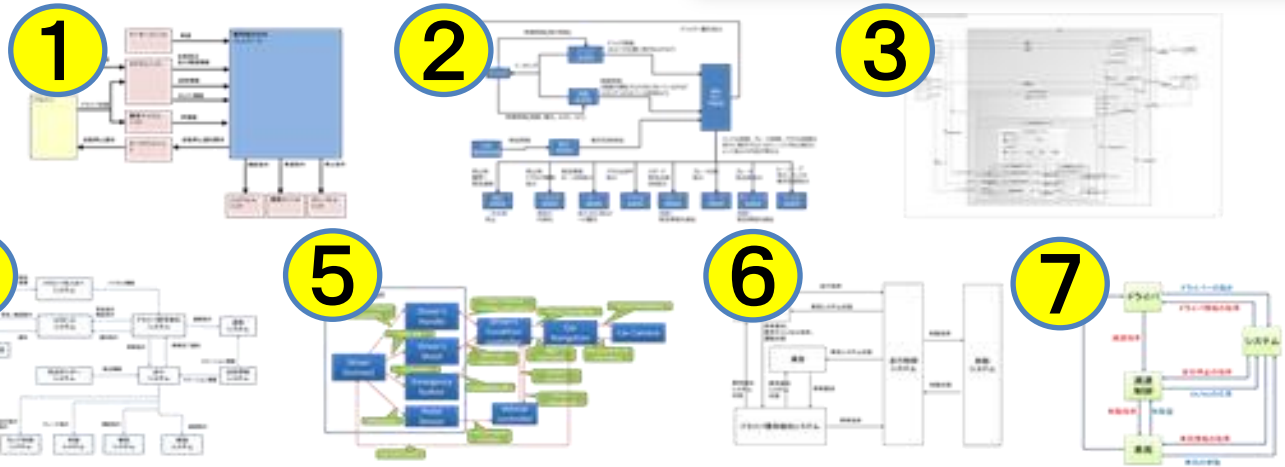
Contents

2. Motivation

HITACHI
Inspire the Next

【実験】 被験者：7名
ある事例に対してコントロールストラクチャーを記述

【結果】
7パターン（同じものは一つも無し）
登場人物、抽象度、相互作用もそれぞれ異なるものが出てきた。



分析対象の想定アーキテクチャ、分析の目的が異なることによるバラツキ

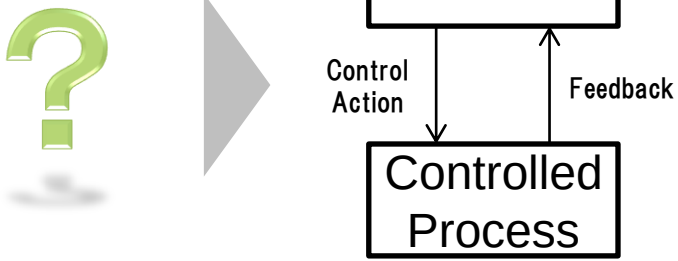
2. Motivation

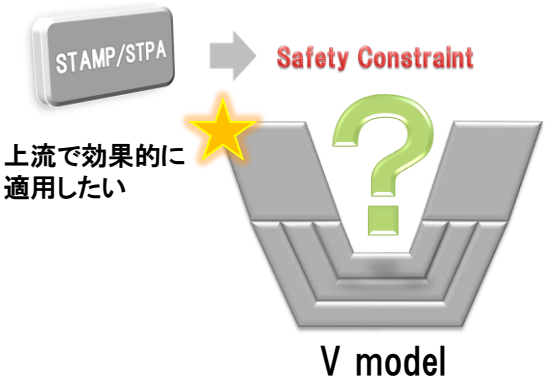
HITACHI
Inspire the Next

Challenge

- システムズエンジニアリングアプローチによる試行

- システムモデルの活用により(※後述)
  1) STPA分析の過程の可視化
  2) STPA分析の結果(安全制約)をシステム設計へ反映





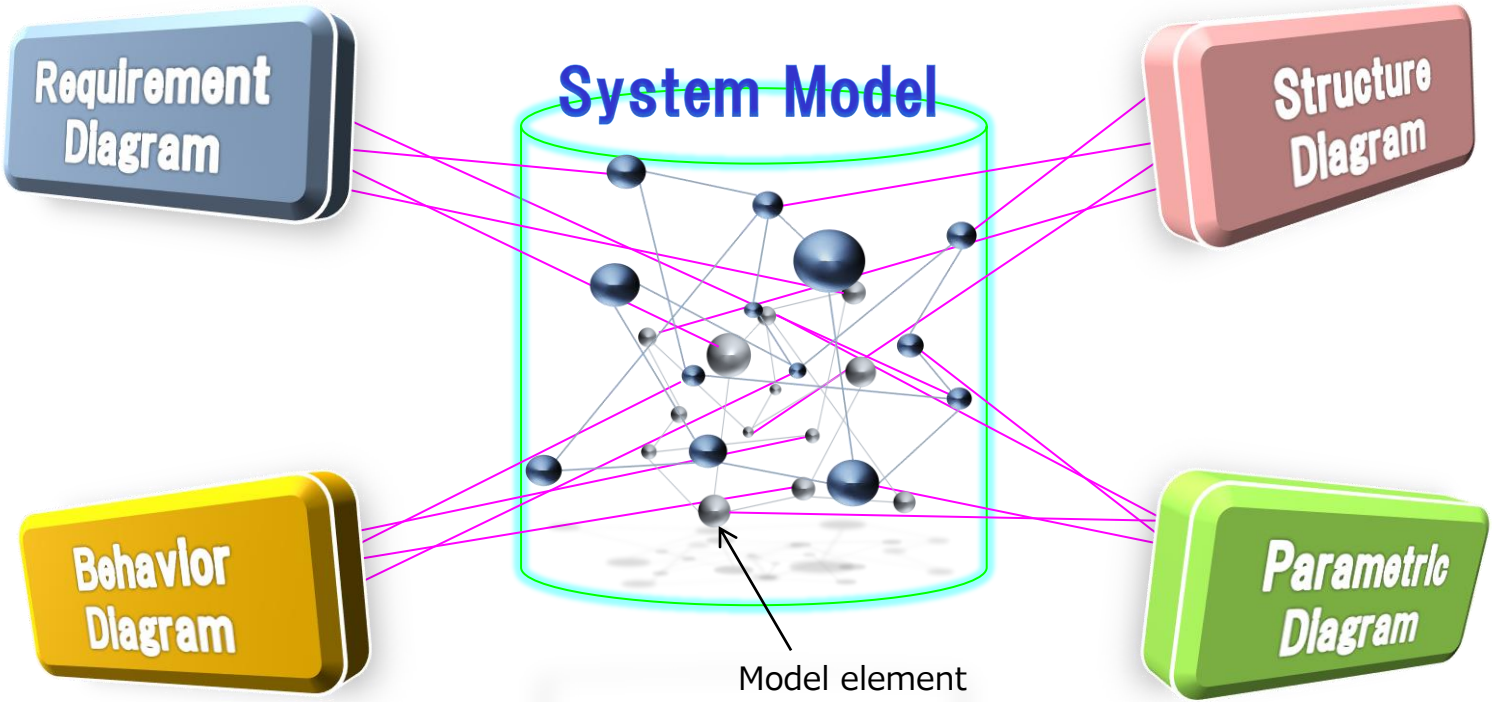
HITACHI
Inspire the Next

Contents

3. システムモデルについて

HITACHI
Inspire the Next

システムモデルのイメージ　（SysMLのケース）



3. システムモデルについて

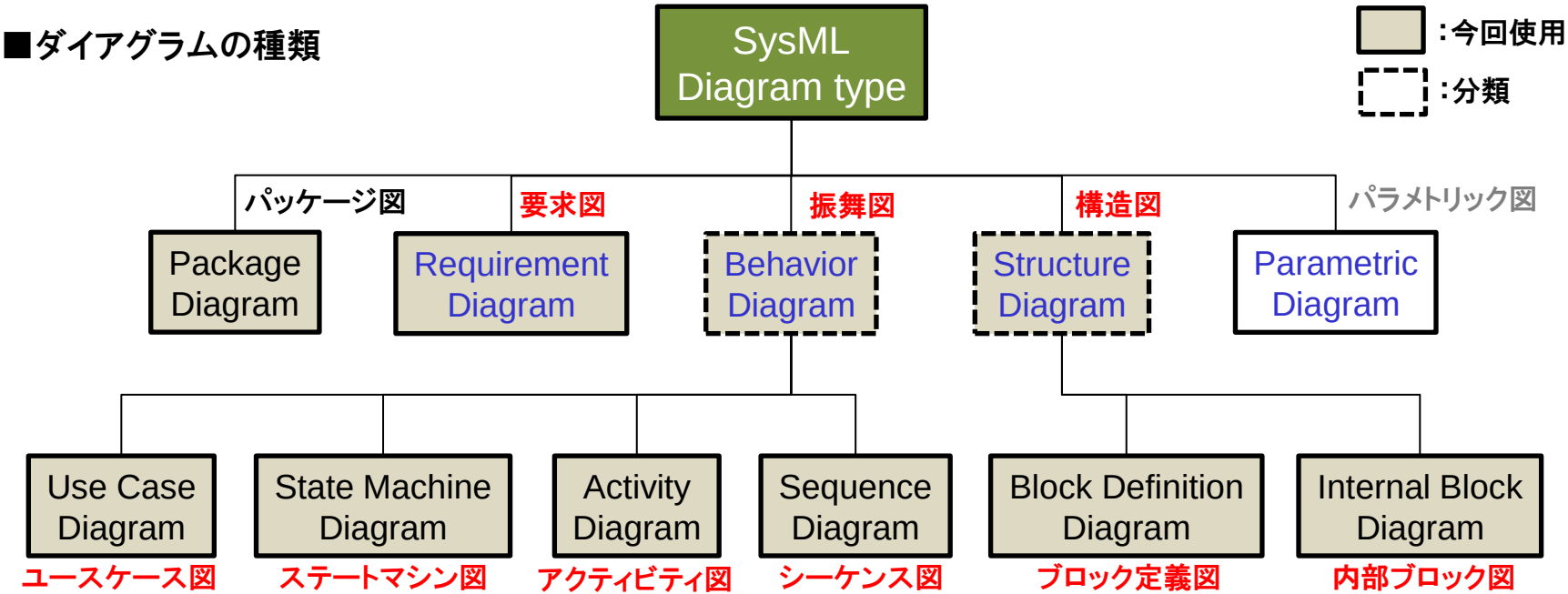
HITACHI
Inspire the Next

OMG SysML™は、Object Management Group® (OMG®)の米国およびその他の国における登録商標または商標です。

※SysMLv1.5より、ISO/IEC 19514:2017(E)として国際標準化

本事例では、システムの記述言語の一つである OMG Systems Modeling Language(OMG SysML™)を選択

■ダイアグラムの種類



HITACHI
Inspire the Next

試行ステップとSysMLダイアグラム活用マップ(一例)

Activity		SysML Diagram type					Table /Matrix
		Package	Requirement	Behavior	Structure	Parametric	
Define Preliminary Architecture (Intended function)		✓ Package (model setup, View & viewpoint)	✓ Requirement (Responsibility)	✓ Use Case ✓ Activity ✓ State Machine	✓ Block Definition ✓ Internal Block	- (MOEs)	✓ Matrix
STAMP/STPA	Step0 (SC,CS)	-	✓ Requirement (Safety Constraints)	✓ State Machine (Process Model)	✓ Internal Block (Control Structure)	-	✓ Matrix
	Step1 (UCA)	-	-	✓ Sequence ✓ State Machine		-	✓ Table
	Step2 (HCF)	-	-	✓ Activity ✓ Sequence		-	✓ Table
Derive Safety Requirements		-	✓ Requirement	-	-	-	✓ Table

HITACHI
Inspire the Next

試行ステップとシステムモデルとの関係

Cameo Systems Modeler™は、No Magic社の米国およびその他の国における登録商標または商標です。

Activity	SysML Diagram type					Table /Matrix
	Package	Requirement	Behavior	Structure	Parametric	
Define Preliminary Architecture (Intended function)	✓ Package (model setup, View & viewpoint)	✓ Requirement (Responsibility)	✓ Use Case ✓ Activity ✓ State Machine	✓ Block Definition ✓ Internal Block	- (MOEs)	✓ Matrix
STAMP/STPA Step0 (SC,CS)	-	✓ Requirement (Safety Constraints)	✓ State Machine (Process Model)		-	✓ Matrix
STAMP/STPA Step1 (UCA)	-	-	✓ Sequence ✓ State Machine	✓ Internal Block (Control Structure)	-	✓ Table
STAMP/STPA Step2 (HCF)	-	-	✓ Activity ✓ Sequence		-	✓ Table
Derive Safety Requirements	-	✓ Requirement	-	-	-	✓ Table

①コンセプト(Output)

③STPA結果(Output)

Systems Engineering

System model

STAMP/STPA

Preliminary Architecture Definition

④STPA結果(Input)

②コンセプト(Input)

Step0: Safety Constraint Control Structure
Step1: Unsafe Control Action
Step2: Hazardous Casual Factor

モデリングツールは、No Magic社のCameo Systems Modeler™を使用

HITACHI
Inspire the Next

Contents

1. 会社紹介
2. Motivation
3. システムモデルについて
4. **ドライバ異常時安全停車システム（事例紹介）**
5. まとめ

4. ドライバ異常時安全停車システム（事例）

（免責事項）
本事例は、仮想システムを題材としており、実際の開発および関連する製品、知的財産権等とは一切関係ありません。

HITACHI
Inspire the Next

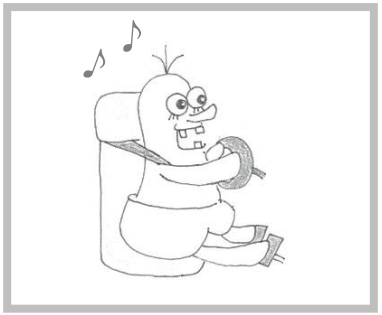
（仮想）ドライバ異常時安全停車システム　Emergency Stop Active Safety System

責務： ドライバの異常を検知したら自動的に車両を安全に停車する

前提： 既存の自動ブレーキシステム（衝突被害軽減ブレーキ）に上記責務を追加する

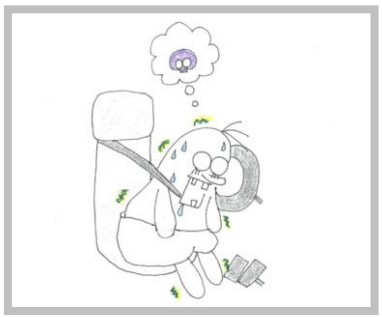
➡ より開発現場に近い想定を設定（既存システムの統合や機能追加により新たな価値を提供）

Normal



Abnormal case

飲酒・居眠り

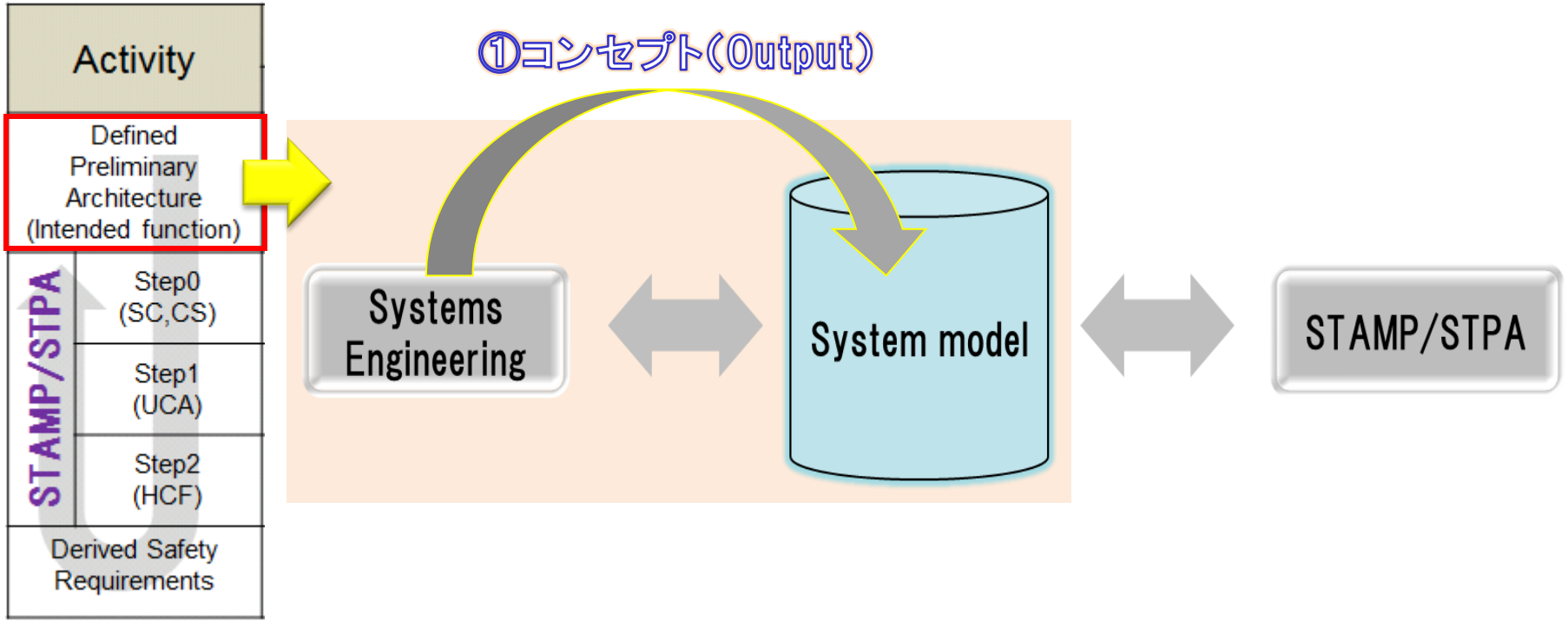


急病

危険

...etc

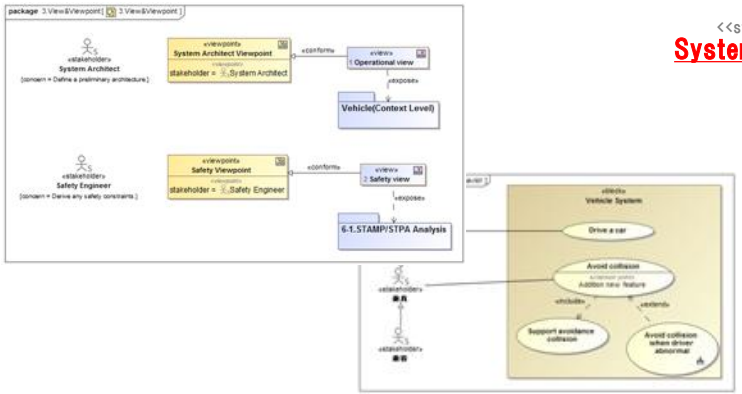
4. ドライバ異常時安全停車システム（事例）

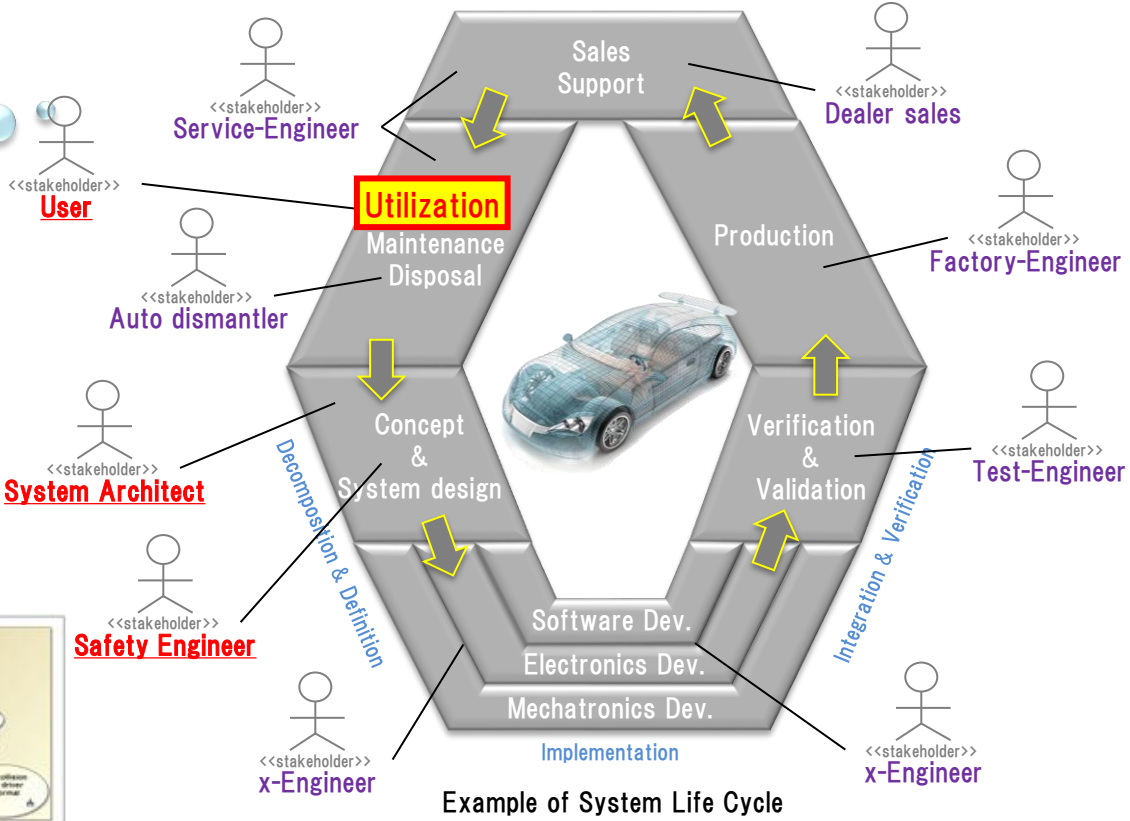


4. ドライバ異常時安全停車システム（事例）

HITACHI
Inspire the Next

Stakeholderの識別とニーズの獲得（今回は、UserにおけるView Point）





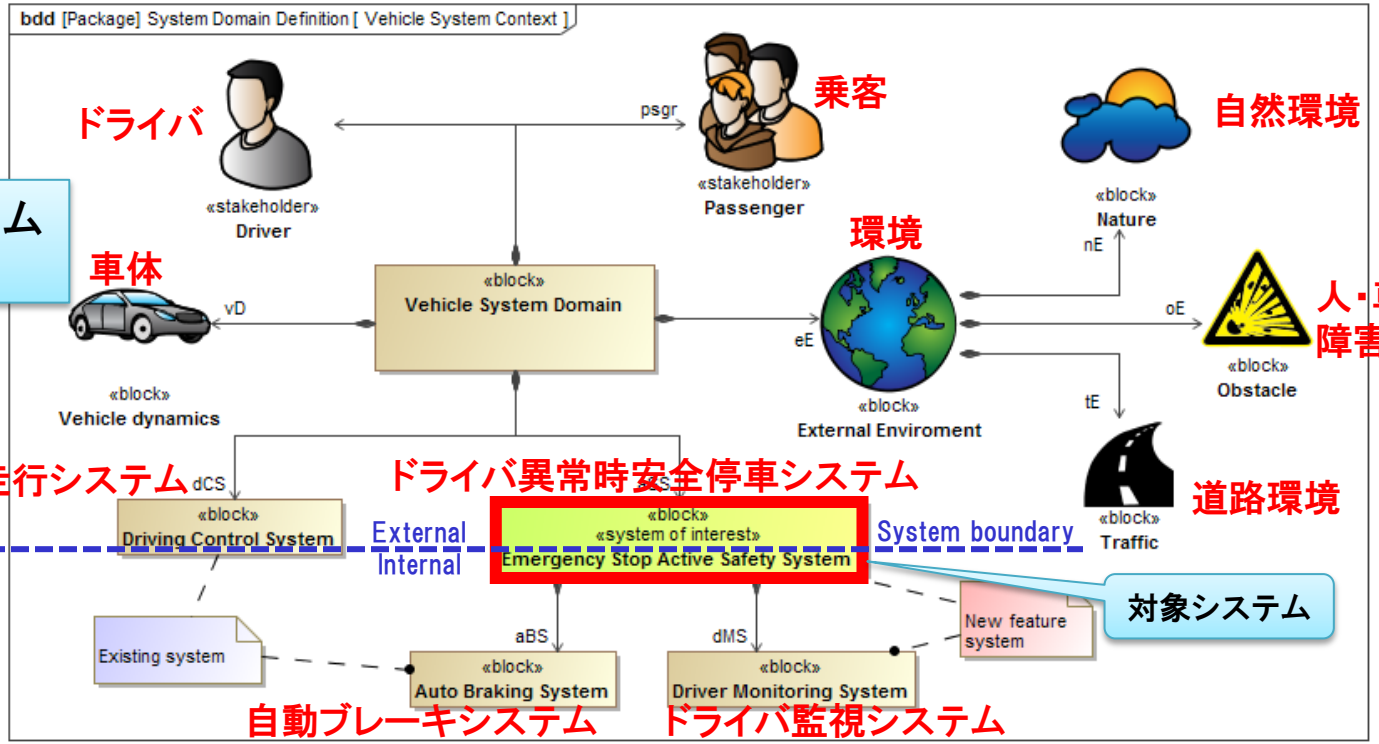
Example of System Life Cycle

4. ドライバ異常時安全停車システム（事例）

HITACHI
Inspire the Next

対象システムと登場人物を定義（Context Levelでシステム境界を明確化）

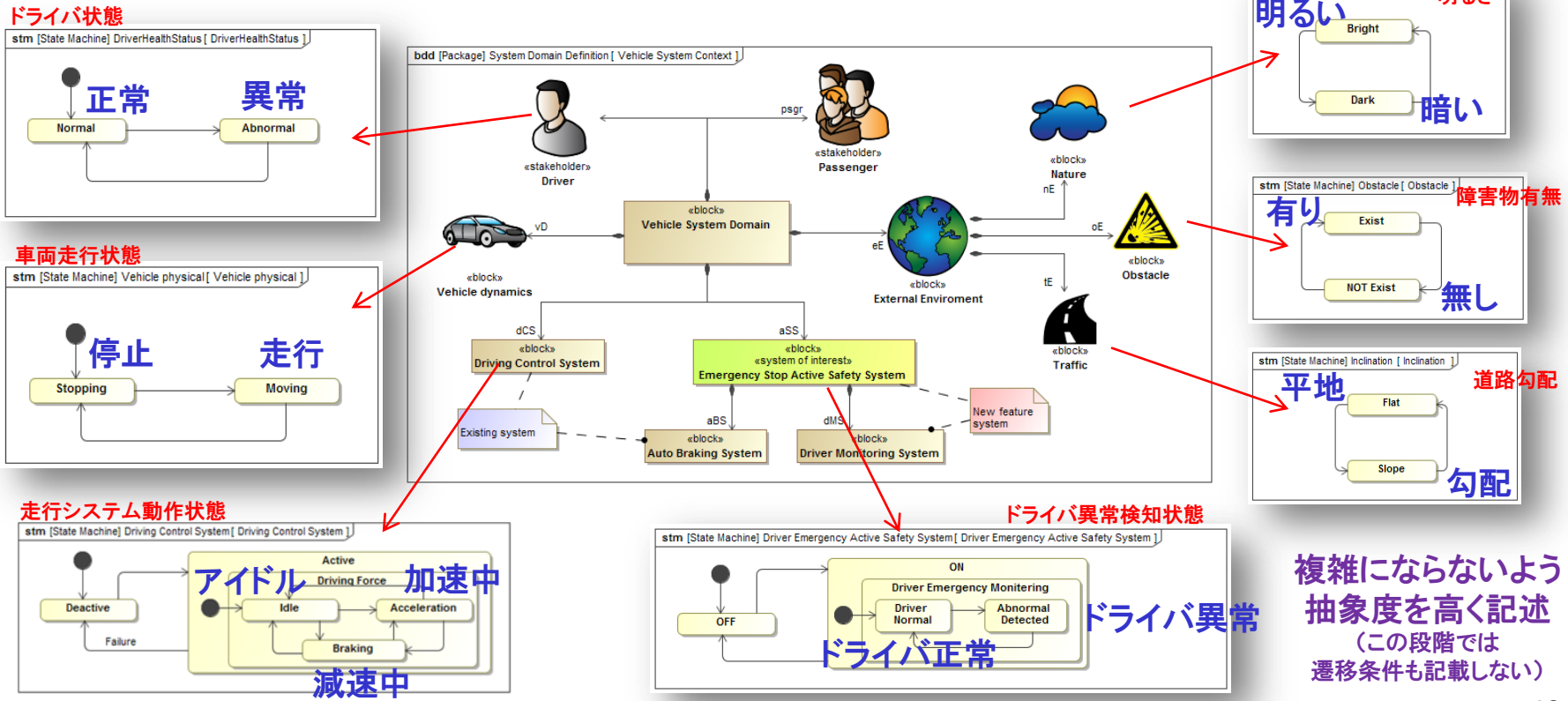
今回は、システムの外部に着目



4. ドライバ異常時安全停車システム（事例）

HITACHI
Inspire the Next

システムの使われ方、使う環境に対して
各コンポーネントの想定されるコンディション、シチュエーションの識別例

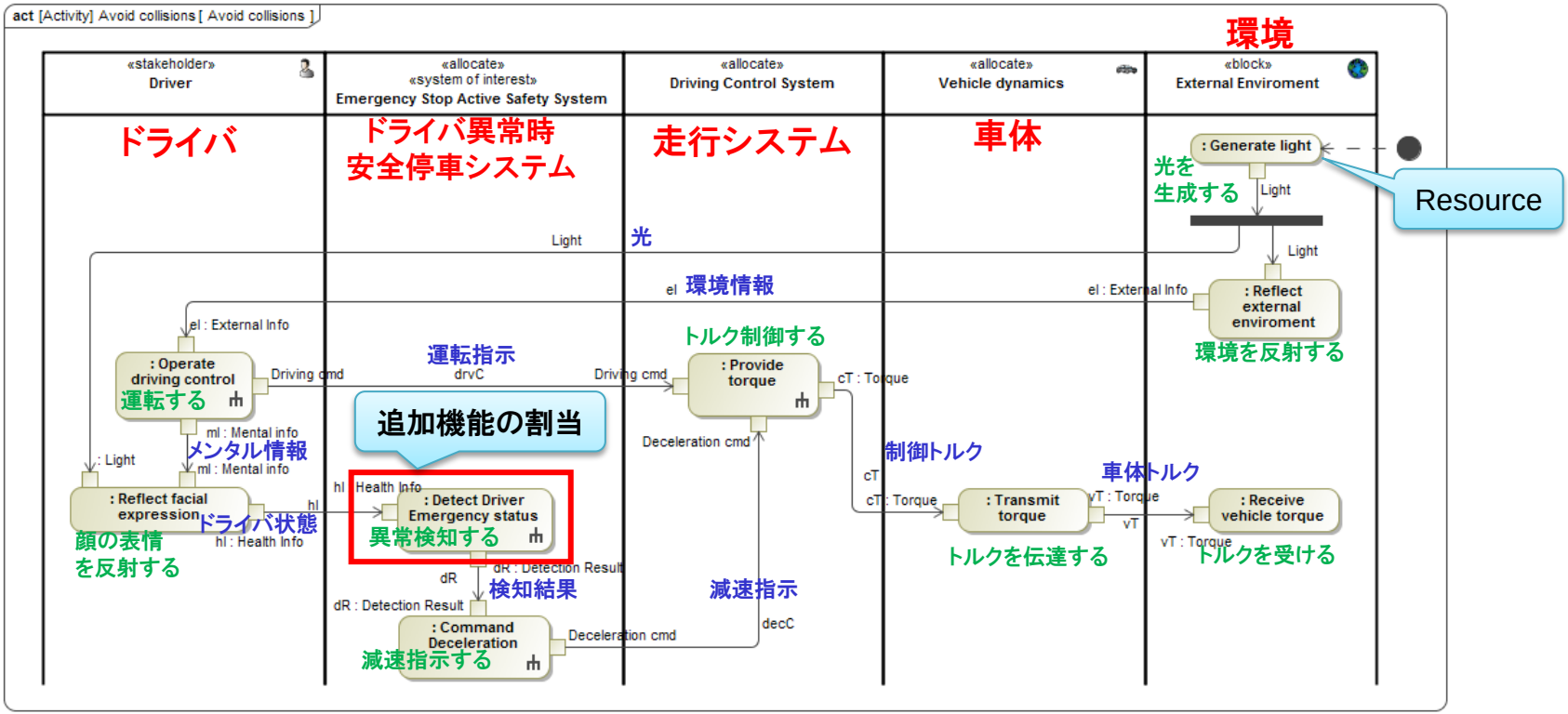


複雑にならないよう抽象度を高く記述
（この段階では遷移条件も記載しない）

4. ドライバ異常時安全停車システム（事例）

HITACHI
Inspire the Next

Context Levelの振舞いと相互作用を定義

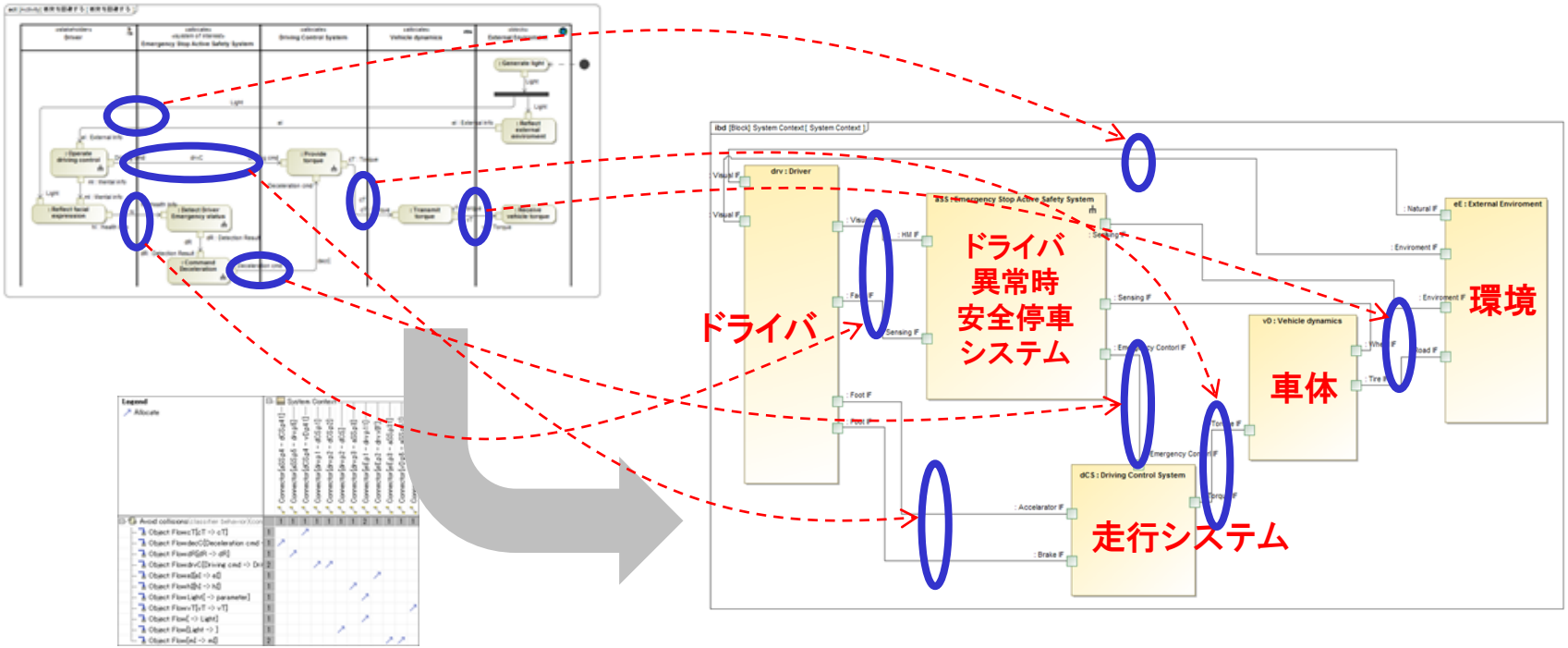


抽象度をコントロール（機能（振舞）の階層化）

4. ドライバ異常時安全停車システム（事例）

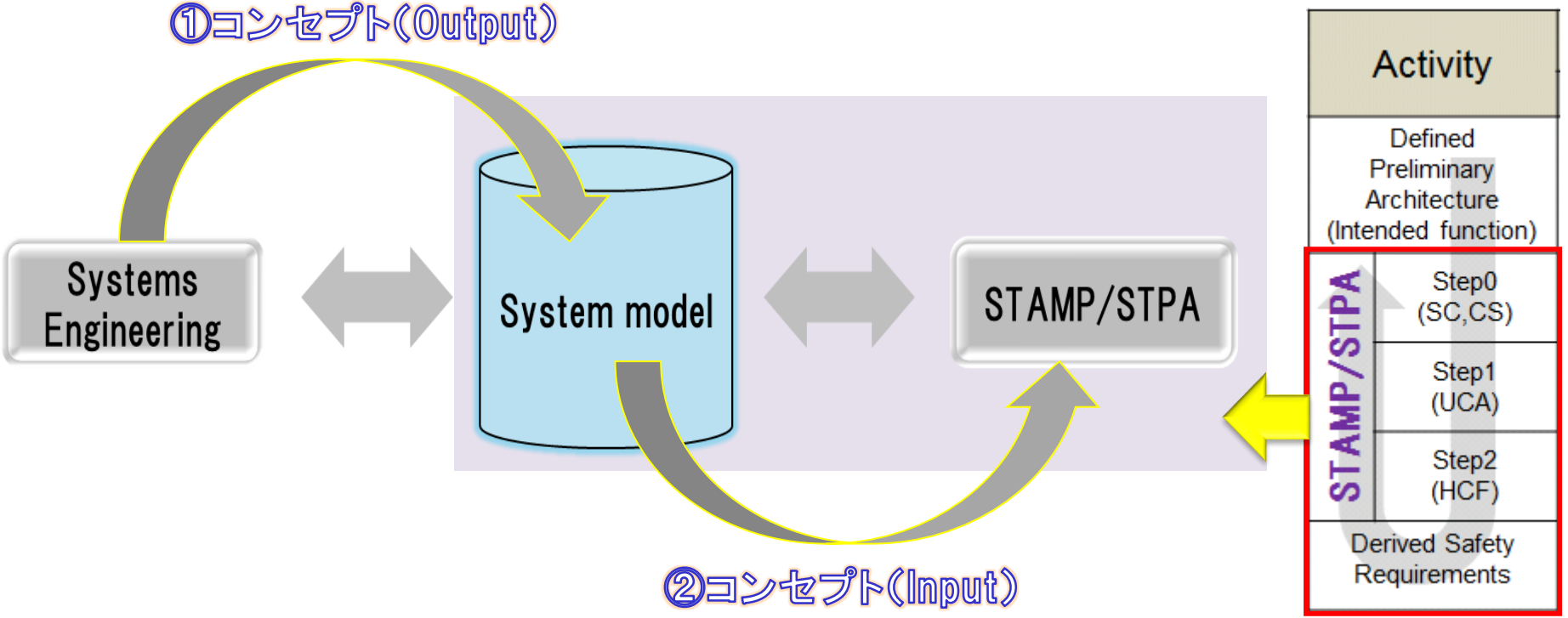
HITACHI
Inspire the Next

Context Levelの振舞いからインターフェースを識別し、コンポーネント間の構造（Interconnection）を定義



4. ドライバ異常時安全停車システム（事例）

HITACHI
Inspire the Next

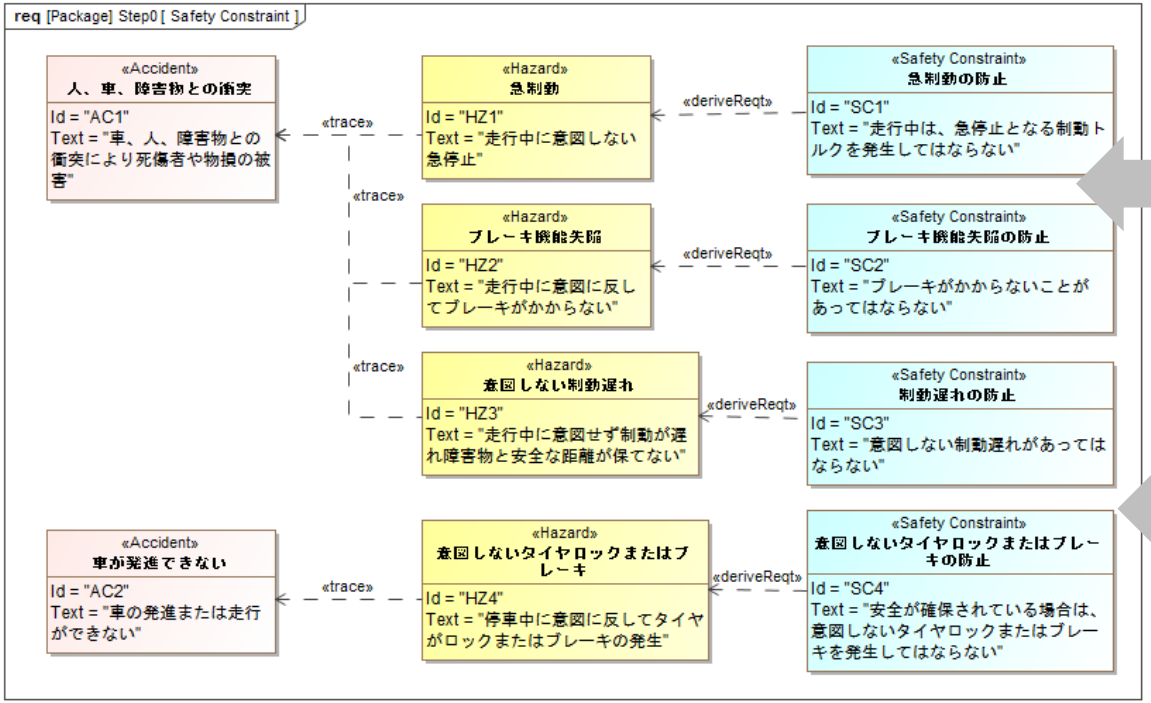


4. ドライバ異常時安全停車システム（事例）

HITACHI
Inspire the Next

STAMP/STPA＜Step0＞： 安全制約の識別

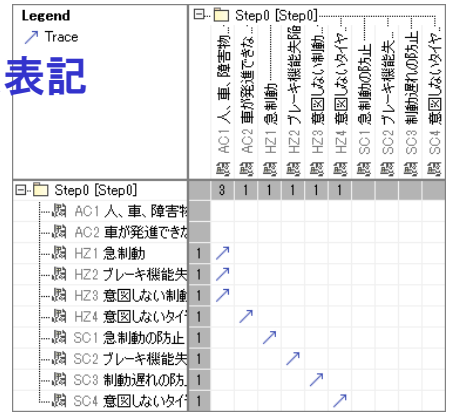
アクシデント、ハザード、安全制約を導出し、結果を紐付け追従性を確保



Table表記

#	Name	Text	Id	Traced To	Derived	Derived From
1	AC1 車、障害物との衝突	車、人、障害物との衝突により死傷者や物損の被害	AC1			
2	HZ1 急停止	走行中に意図しない急停車	HZ1	AC1	SC1	
3	HZ2 ブレーキ機能失陥	走行中に意図に反してブレーキがかからない	HZ2	AC1	SC2	
4	SC1 急停止の防止	走行中は、急停止となる制動トルクを発生	SC1	HZ1		HZ1
5	SC2 ブレーキ機能失陥の防止	ブレーキがかからないことがあってはならない	SC2	HZ2		HZ2

Matrix表記



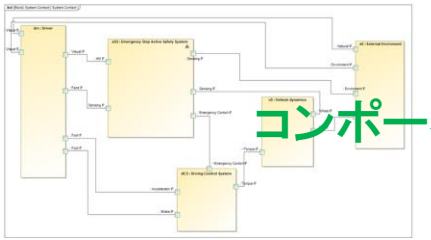
※ <<Accident>>、<<Hazard>>、<<Safety Constraint>>は、SysML標準にはないため、STAMP用にプロファイルを追加

4. ドライバ異常時安全停車システム（事例）

HITACHI
Inspire the Next

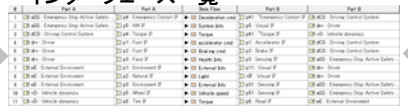
STAMP/STPA＜Step0＞： Control Structure(CS図)の構築

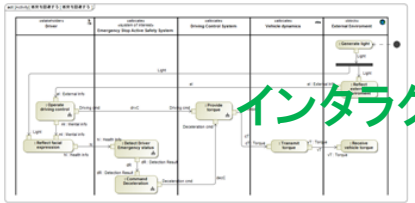
Preliminary Architecture(構造・振舞)からSTPA分析用にCS図を作成



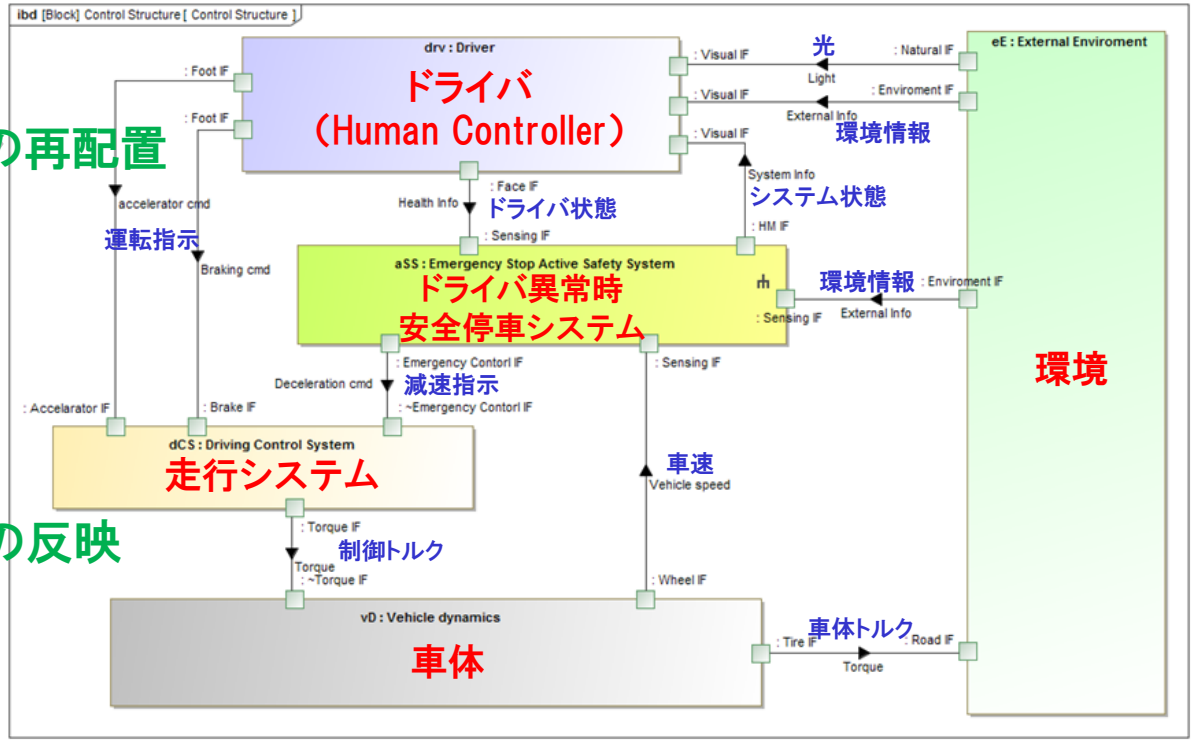
コンポーネントの再配置

インターフェース一覧





インタラクションの反映

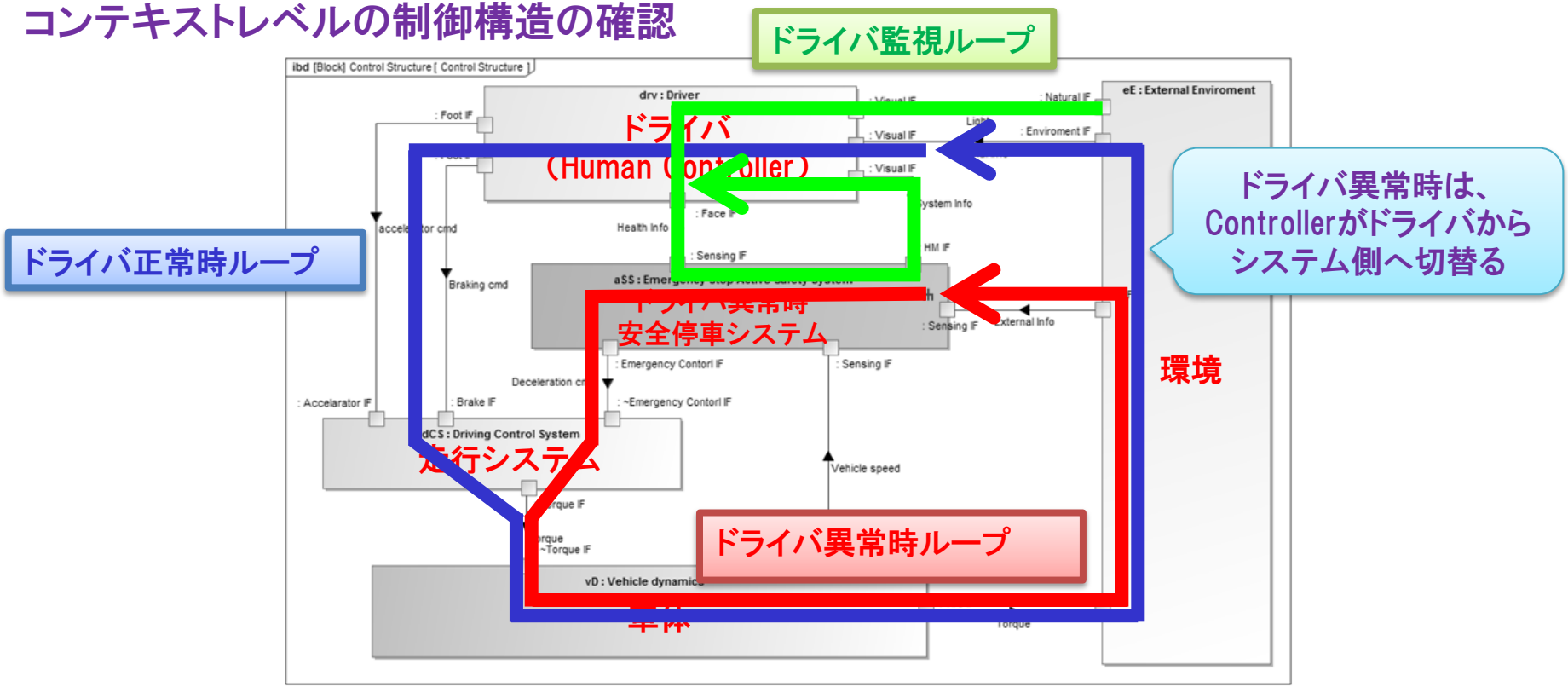


4. ドライバ異常時安全停車システム（事例）

HITACHI
Inspire the Next

STAMP/STPA＜Step0＞： Control Structure(CS図)の構築

コンテキストレベルの制御構造の確認

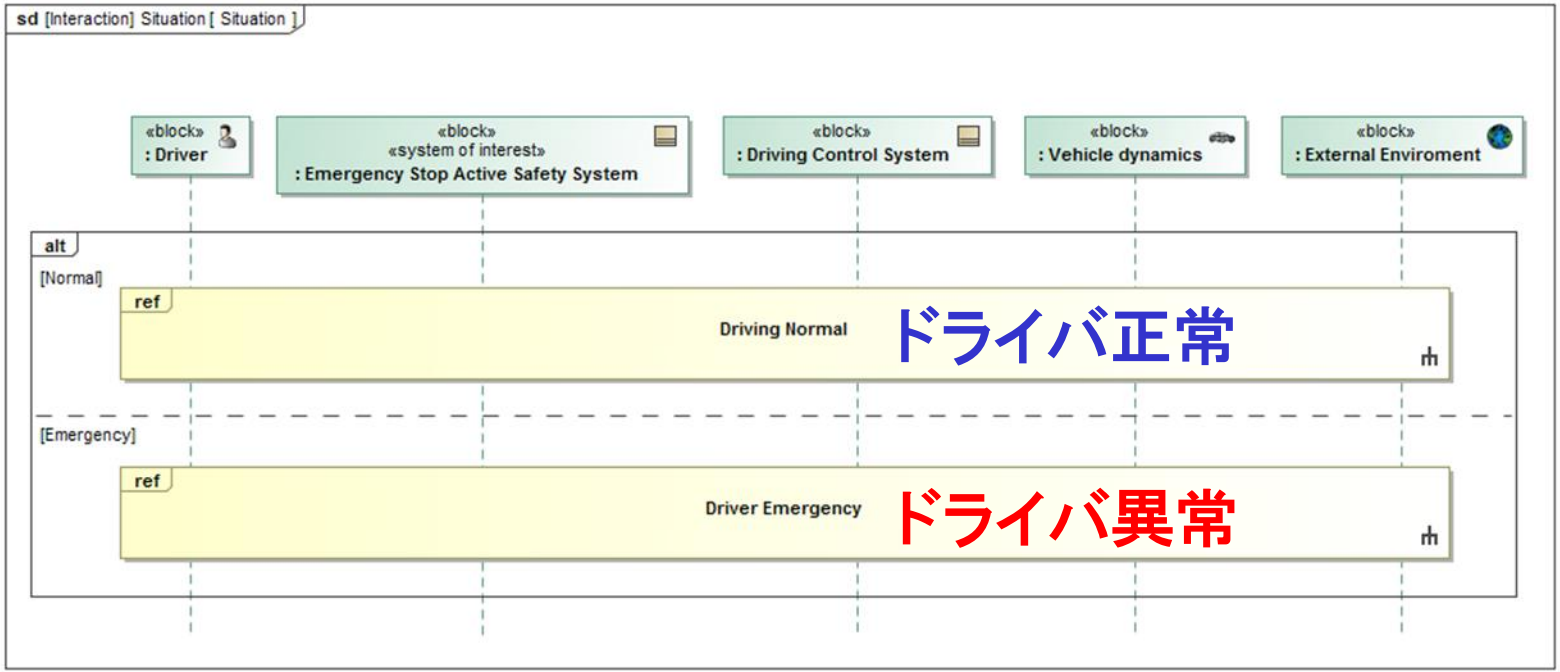


4. ドライバ異常時安全停車システム(事例)

HITACHI
Inspire the Next

STAMP/STPA＜Step1＞: Unsafe Control Actionの識別(UCA)

各コンポーネント間のインタラクションと状態(Context)の時系列変化をシーケンス図で確認



4. ドライバ異常時安全停車システム（事例）

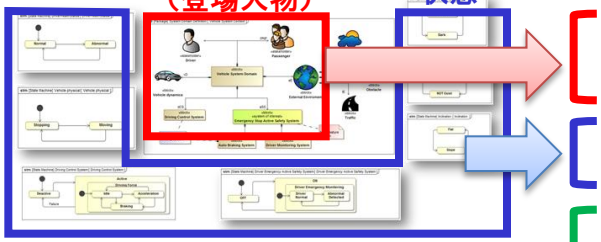
HITACHI
Inspire the Next

STAMP/STPA＜Step1＞： Unsafe Control Actionの識別(UCA)

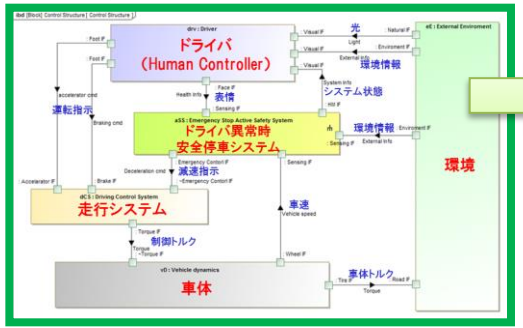
各コンポーネント間のインタラクションと状態（Context）の時系列変化をシーケンス図で確認

コンポーネント
（登場人物）

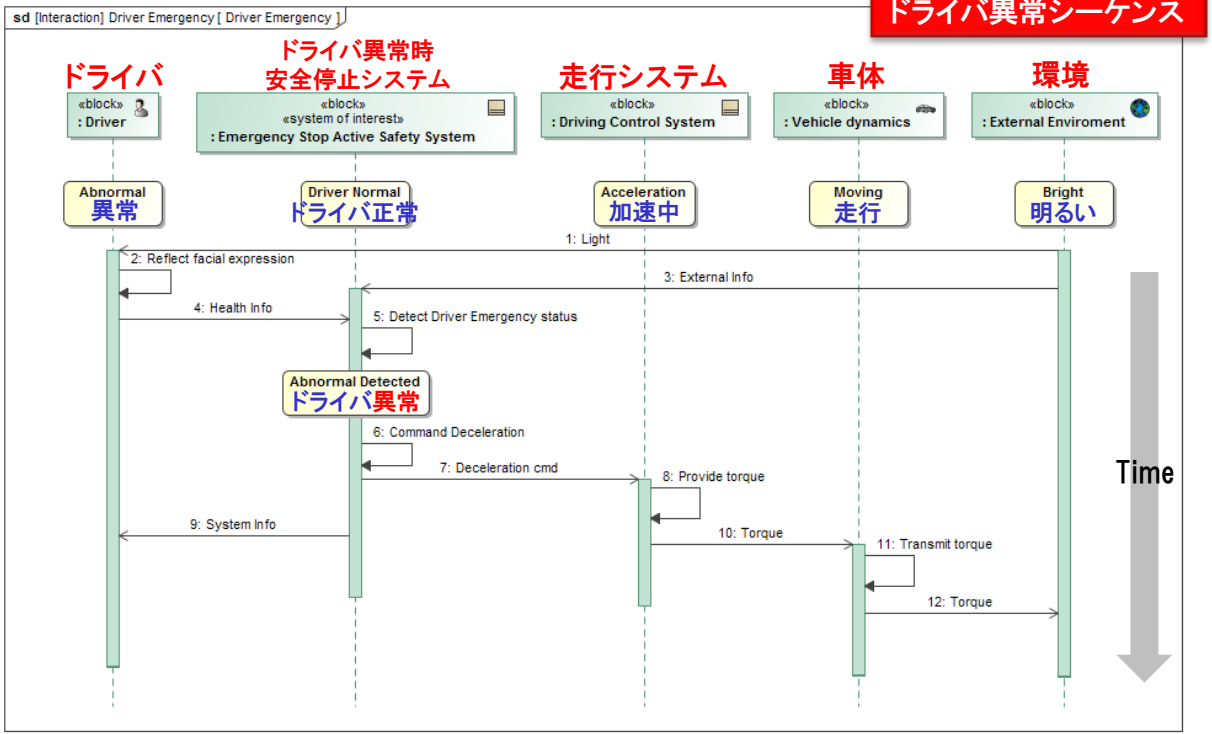
状態



インタラクション



ドライバ異常シーケンス

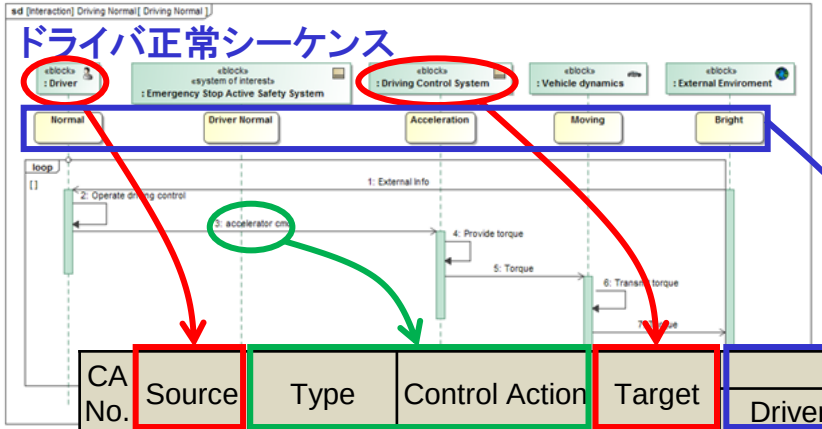


4. ドライバ異常時安全停車システム(事例)

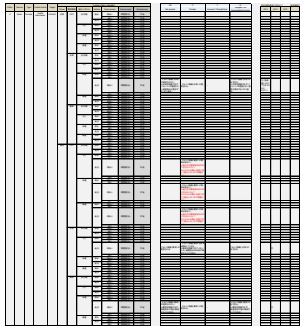
HITACHI
Inspire the Next

STAMP/STPA＜Step1＞: Unsafe Control Actionの識別(UCA)

基本動作からコンセプトの検証＆CAとContextの関係を一覧にする。
分析に必要なContextの組み合わせを一覧にしてガイドワード(N,P,T,D)を使いUCAを抽出



■Process Model
ドライバ　:正常、異常
異常検知:正常、異常
走行　　:アイドル、加速、減速
車体　　:停止、走行
明るさ　:明、暗



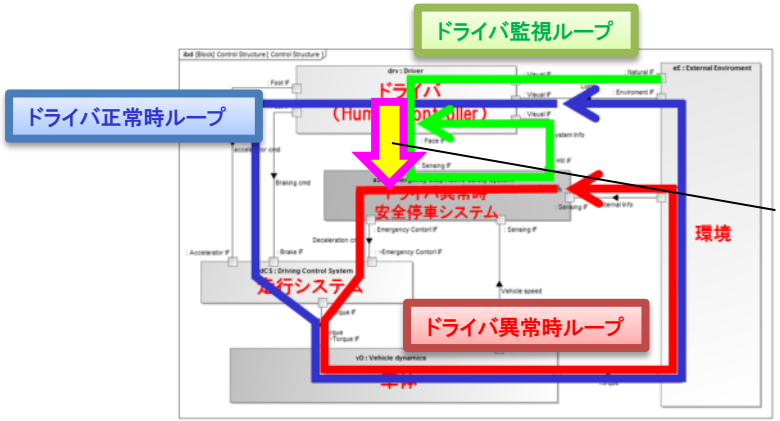
CA No.	Source	Type	Control Action	Target	Context (Value, Valuable)				
					Driver	ESASS	dCS	Vehicle	Environment
					ドライバ	対象システム	走行システム	車体	環境
1	Driver	Provide	Acceleration	dCS	Normal	Driver Normal	Acceleration	Moving	Bright
2	dCS		Torque	Vehicle					
3	Vehicle		Torque	Env.					
4	Driver		Health Info.	ESASS	Abnormal	Driver Normal	Acceleration	Moving	Bright
5	ESASS		Braking	dCS		Abnormal Detected			
6	dCS		Torque	Vehicle					
7	Vehicle		Torque	Env.					

4. ドライバ異常時安全停車システム（事例）

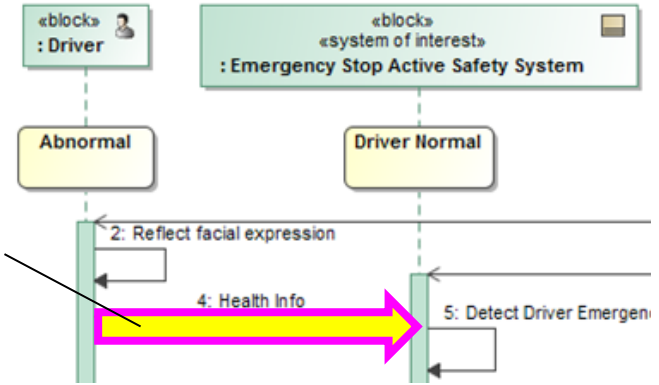
HITACHI
Inspire the Next

STAMP/STPA＜Step1＞： Unsafe Control Action(UCA)の識別

各CAに対する分析により抽出されたUCAの例



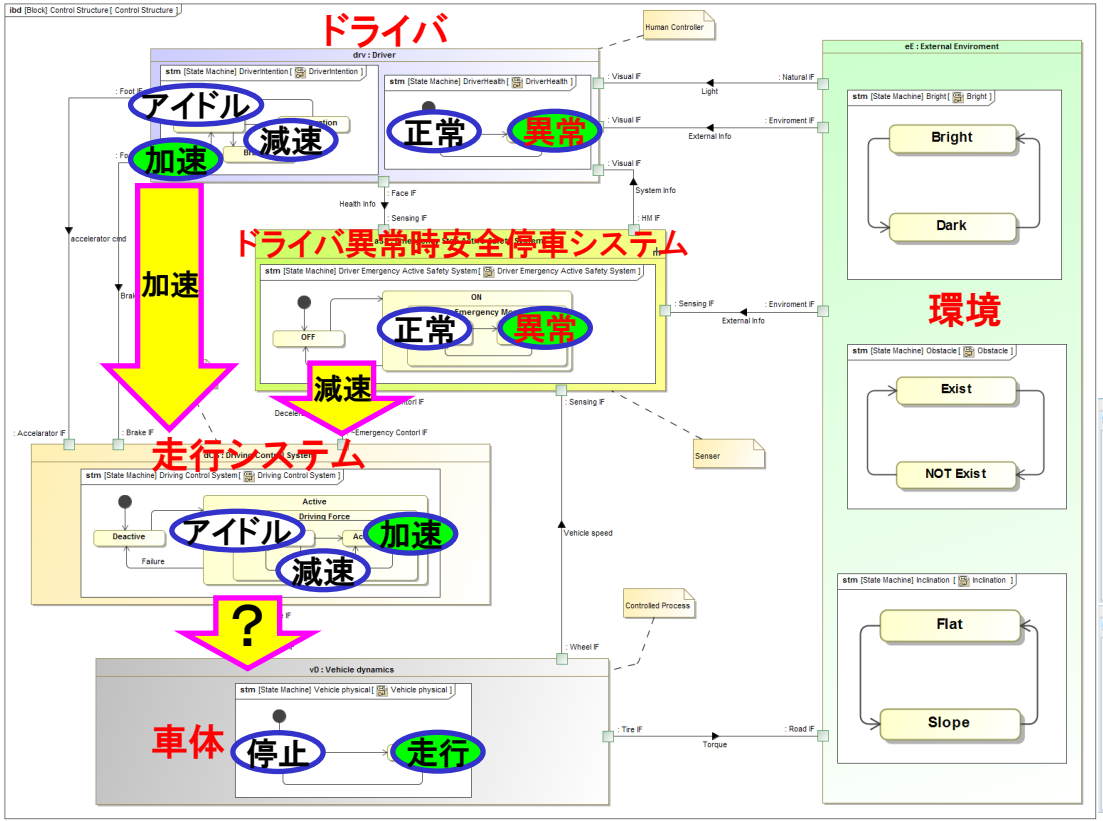
ドライバ状態の通知
（異常／正常）

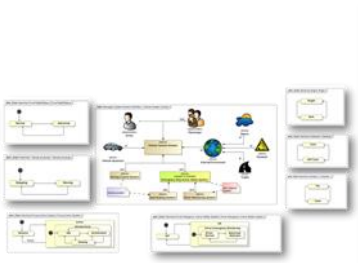


Control Action	N Not providing causes hazard	P Providing cases hazard	T Incorrect Timing/Order	D Stopped Too Soon/Applied too long
ドライバ状態の異常通知（CA-4）	ドライバが異常時にドライバ異常が提供されない。 ⇒異常を認識できず、減速指示が遅れ衝突する（SC3違反）	ドライバが異常時にドライバ異常が提供される。	－	ドライバが異常時にドライバ異常が短すぎる。 ⇒異常を認識できず、減速指示が遅れ衝突する（SC3違反）

4. ドライバ異常時安全停車システム（事例）

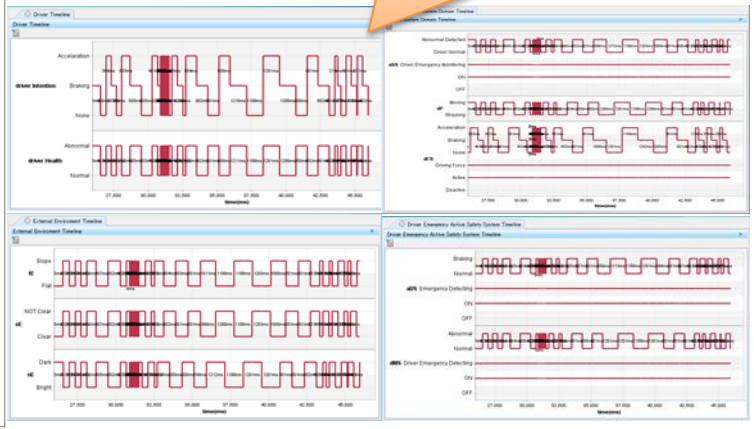
STAMP/STPA＜Step1＞： UCA導出方法





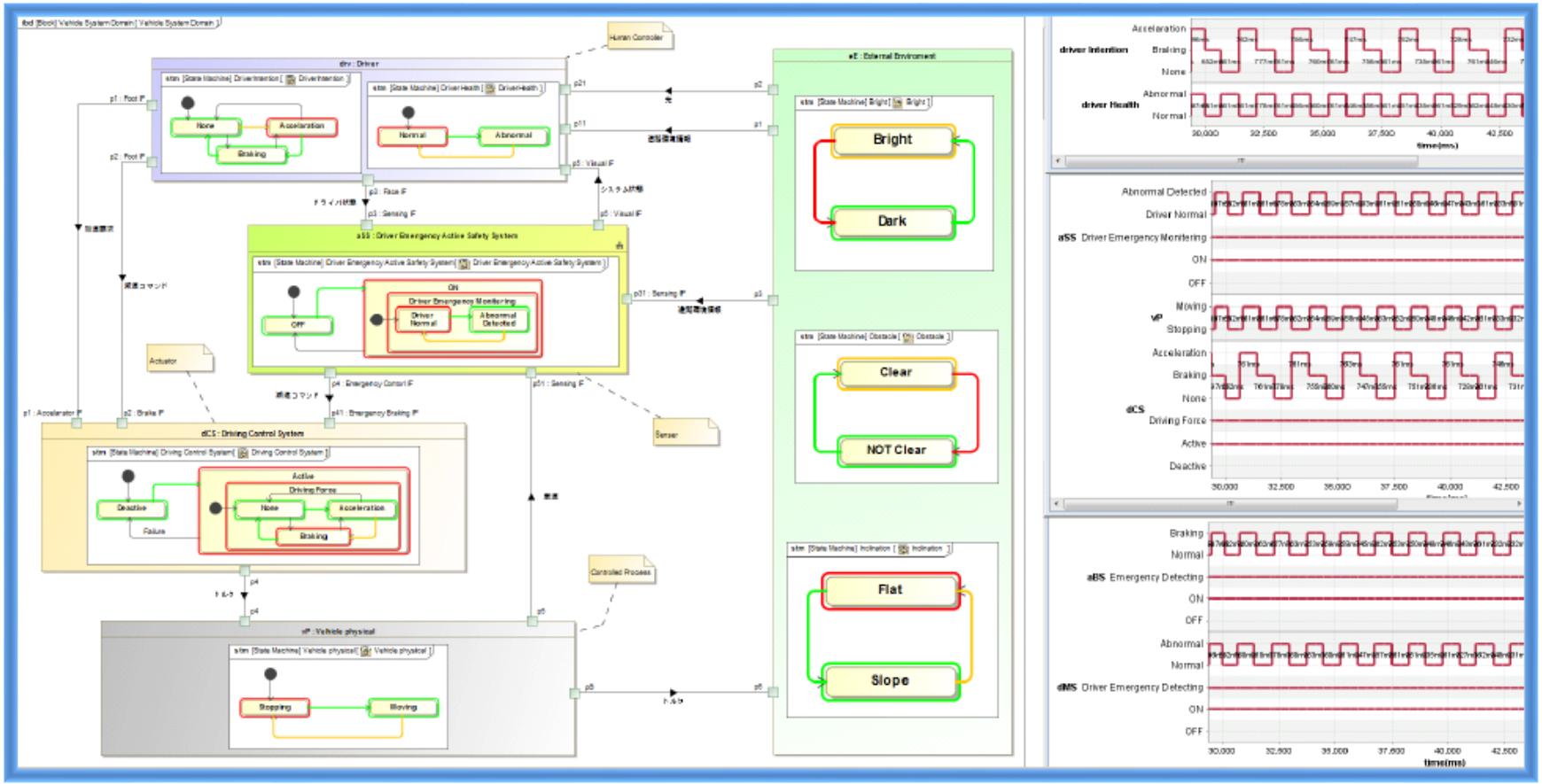
【ご参考】
CS図に状態（コンテキスト）をマッピングしたUCA分析の例

状態遷移の動作結果（組み合わせ）から効率よくUCA抽出できないか今後検討予定



4. ドライバ異常時安全停車システム（事例）

HITACHI
Inspire the Next



4. ドライバ異常時安全停車システム（事例）

HITACHI
Inspire the Next

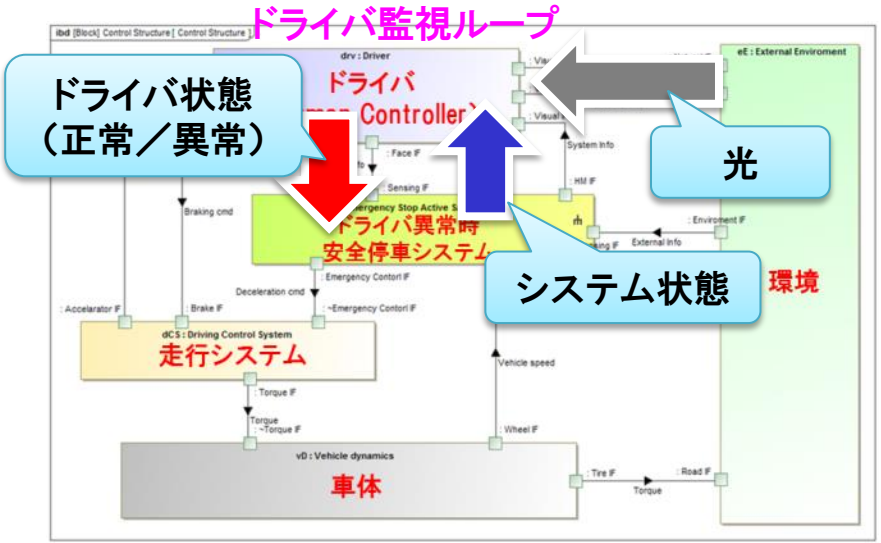
STAMP/STPA＜Step2＞： HCFの特定例

【UCA-1】ドライバ状態（正常／異常）
ドライバ異常を認識できず、減速指示が遅れ衝突する（SC3違反）

シナリオ①
外部環境の光の影響によりシステムがドライバの状態を正しく認識できない。
⇒対策： ドライバ状態の認識は、複数の異なる手段にて判断する。
（検出手段の冗長化）

シナリオ②
ドライバの装飾品（サングラス、マスク）によりシステムが、ドライバの状態を正しく認識できない。
⇒対策： ドライバの状態を正しく認識できない場合は、
その旨をドライバへ通知する。
ユーザマニュアルに利用時の注意点として記載する。

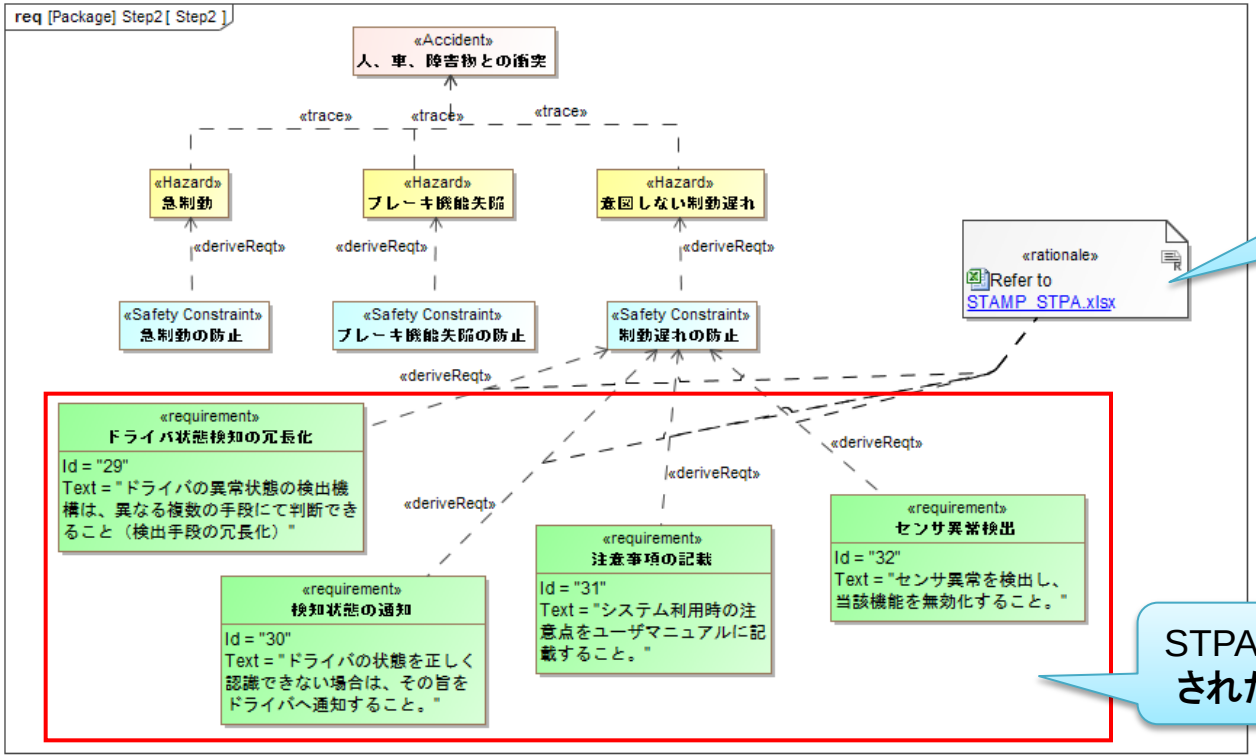
シナリオ③
センサ異常によりドライバの状態を正しく認識できない。
⇒対策： センサ異常を検出し、機能無効化する。
また、ドライバへ通知する。（または、センサの冗長化）



4. ドライバ異常時安全停車システム（事例）

HITACHI
Inspire the Next

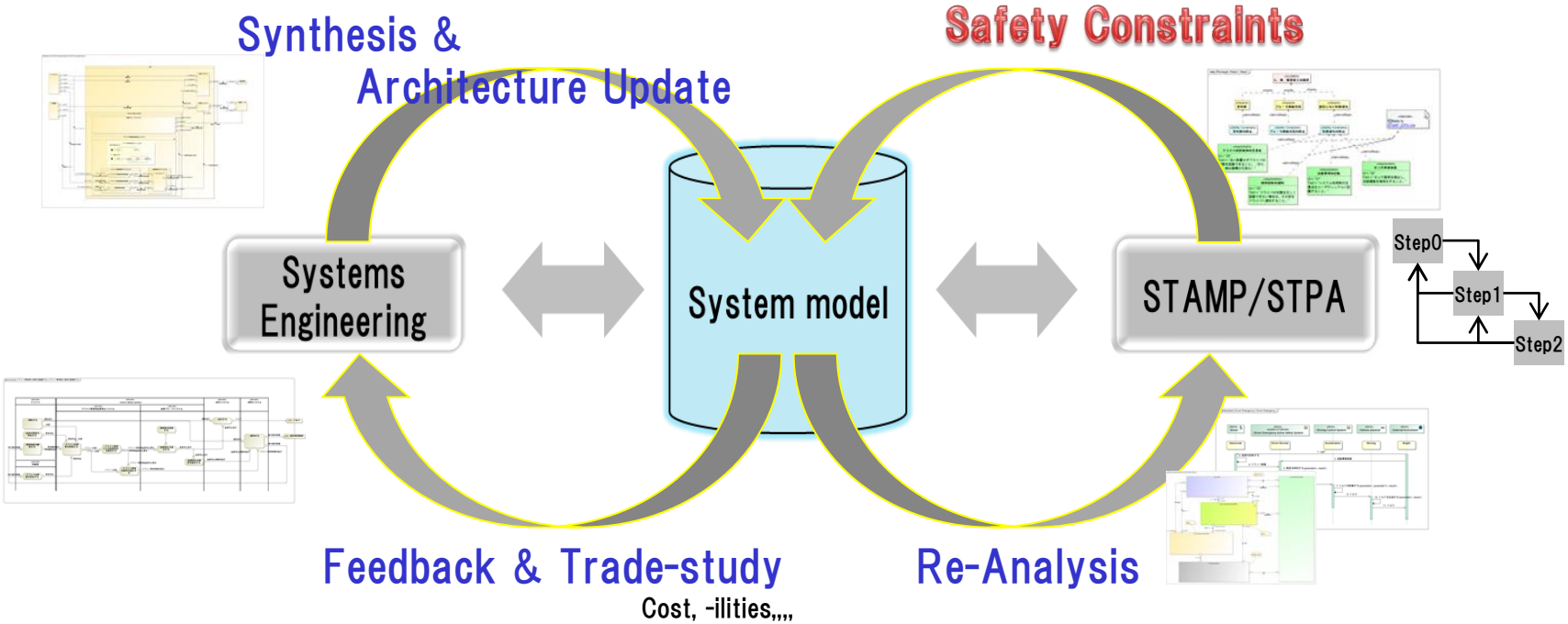
STAMP/STPA＜Step2＞： 対策をシステムへの要求として反映しトレーサビリティを確保
STAMP/STPA分析結果もエビデンスとして登録する。



4. ドライバ異常時安全停車システム（事例）

HITACHI
Inspire the Next

STAMP/STPAによる安全分析の結果を元にシステムズエンジニアリングへ
⇒Iterationを繰り返し、上流の早期に安全リスクを考慮したシステム開発が可能と考えられる。



HITACHI
Inspire the Next

Contents

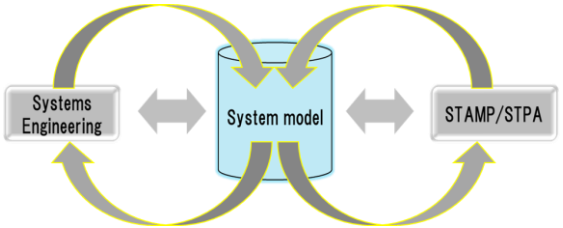
5. まとめ

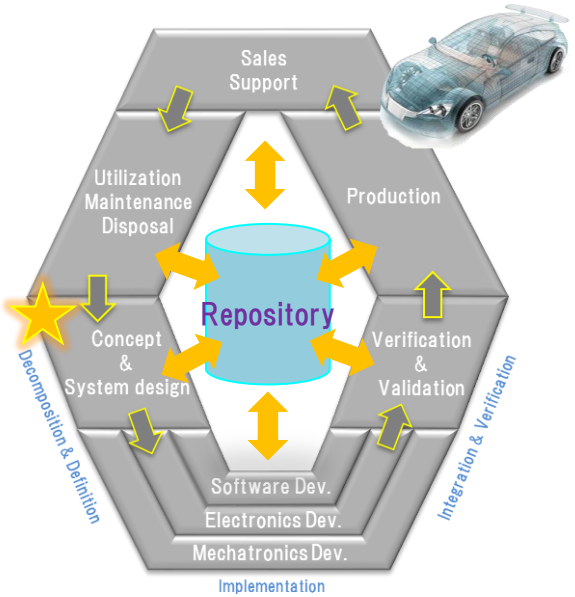
HITACHI
Inspire the Next

- 抽象度の高いコンセプト初期においてもSTAMP/STPAの有効性を確認
  ⇒早期に安全リスクを考慮できる(特に非故障に起因)
  システムアーキテクチャに選択肢をもたらす

- システムモデルを活用することで一貫したシステム開発への導き
  ⇒可視化によるレビュー容易性、
  要求導出および設計エビデンスまでの
  トレーサビリティの確保

- ドライバ以外のStakeholder(販売、メンテナンス、廃棄ステージ等)の視点によるSTAMP/STPA分析も重要
  ⇒様々な視点により網羅性を向上させる
  System、Subsystemと段階的に分析を繰り返しが必要





Example of System Life Cycle

Controlled Processが顔に・・・

HITACHI

Inspire the Next