第２回　STAMPワークショップ

UNISYS

STAMP／STPAを用いた Cyber-Physical Systemsの検証

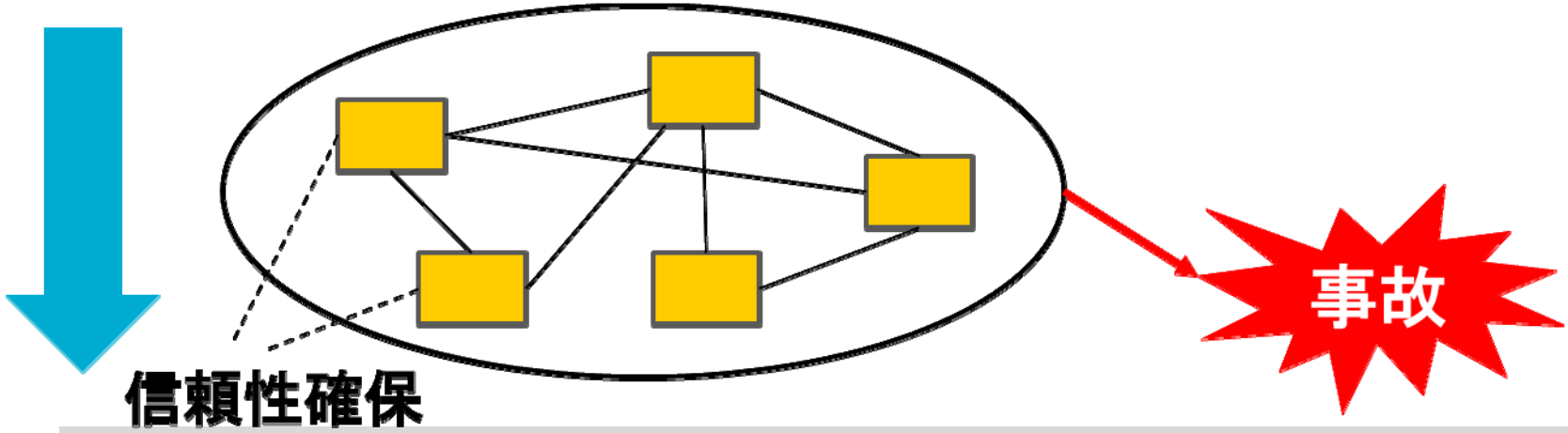
2017年11月29日
日本ユニシス株式会社　青木　善貴
信州大学　小形　真平
大阪大学　中川　博之

背景　CPS(Cyber-Physical-System)

Foresight in sight

- CPSは，物理空間とサイバー空間をまたがる複雑な構成である
  - 多くの種類と数の構成要素がつながる
  - 構成要素の相互作用に起因する事故が起こる

- 個々の構成要素の信頼性が確保されても事故は防ぎきれない



背景　STAMP/STPA

Foresight in sight

- MITのNancy Leveson 教授が考案した安全性解析手法

- 多くの構成要素からなるシステムにも対応

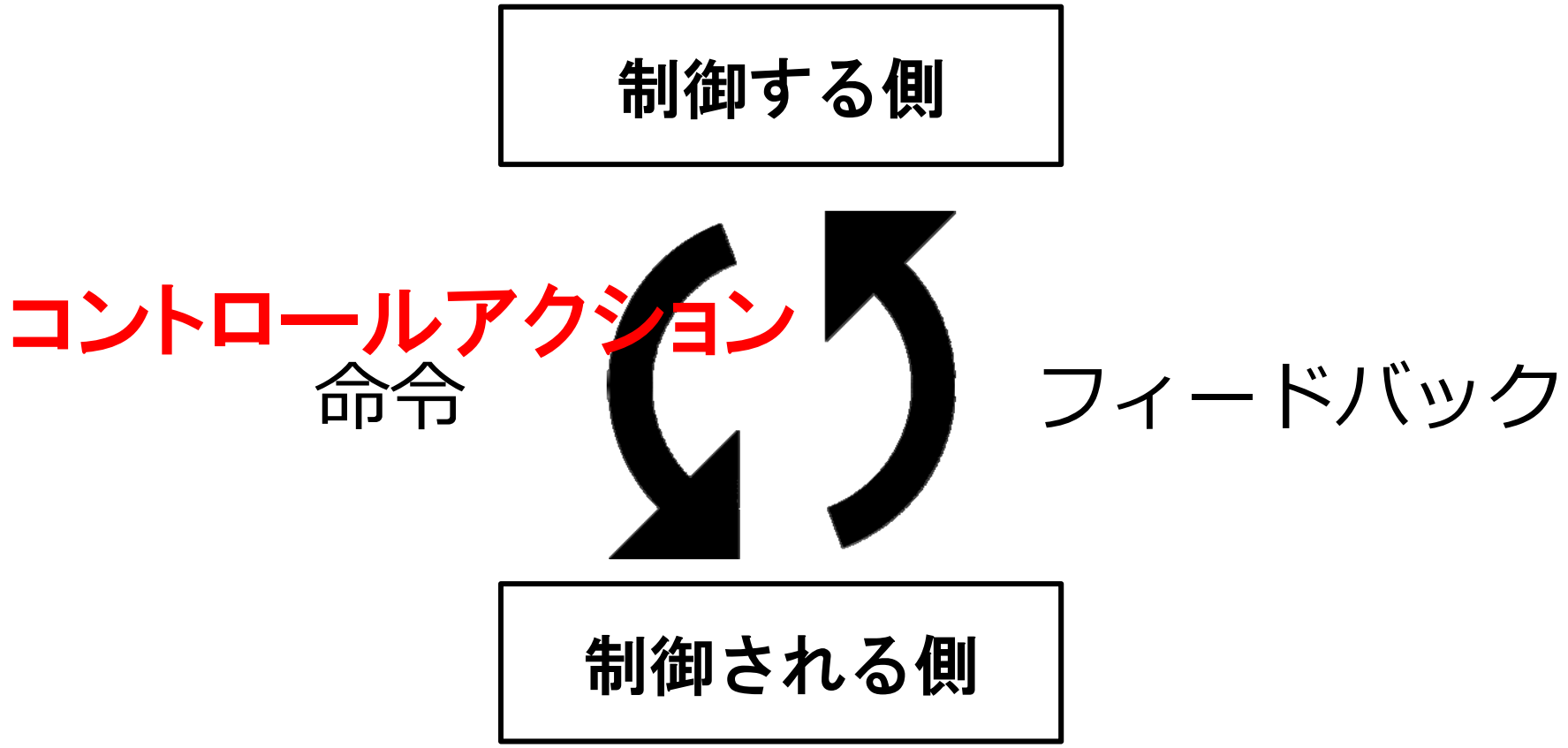
  米国：NASA、航空、自動車、医療など適用が進んでいる

  日本：事例はまだ少ない。JAXAでは試行。IPAが「はじめてのSTAMP/STPA」を公開。IoTシステムへの適用を期待。

背景　コントロールループ

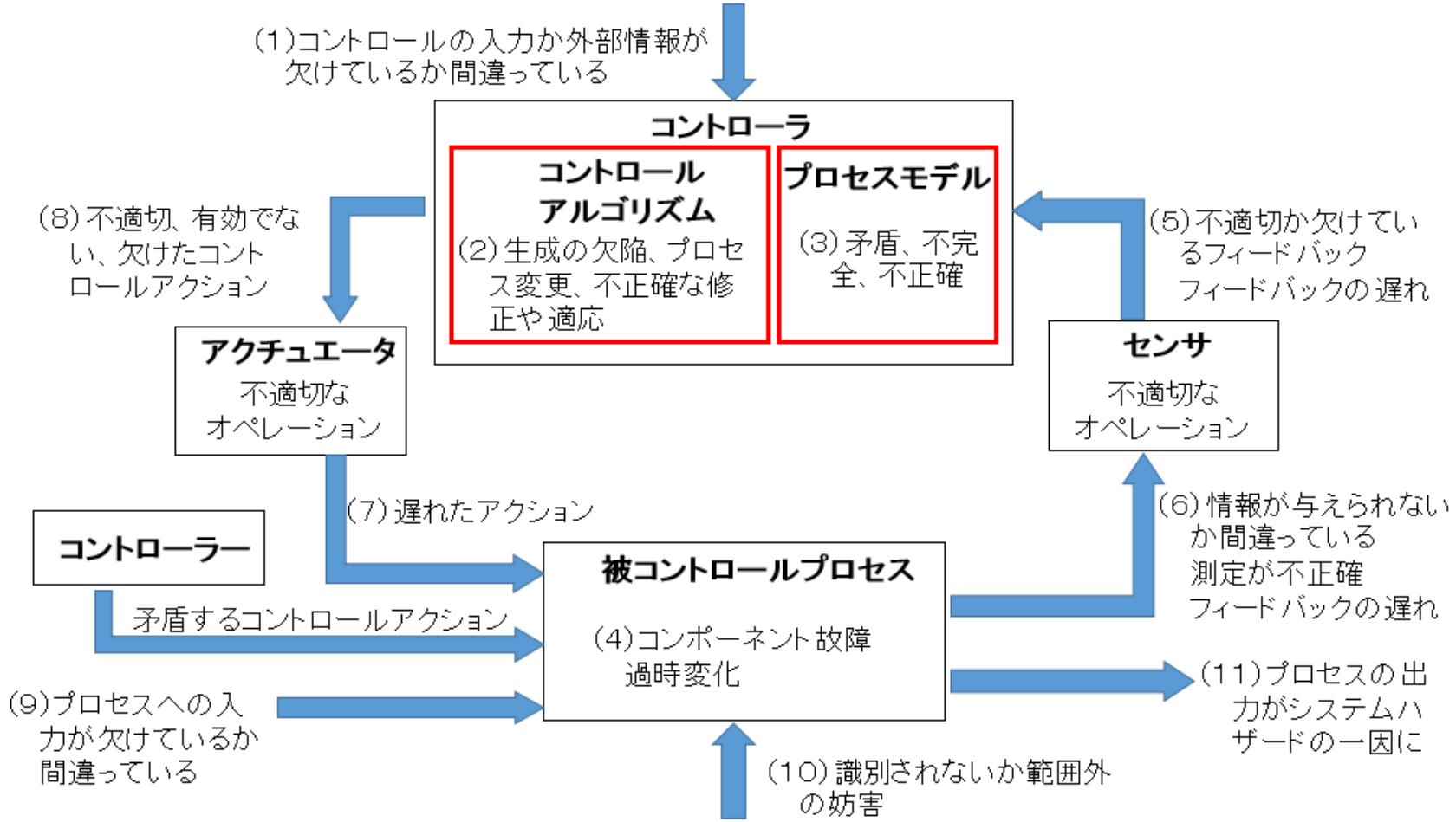
Foresight in sight

構成要素間の相互関係に着目した安全性の解析



背景　コントロールループ

Foresight in sight



CPSのコントロールループの問題

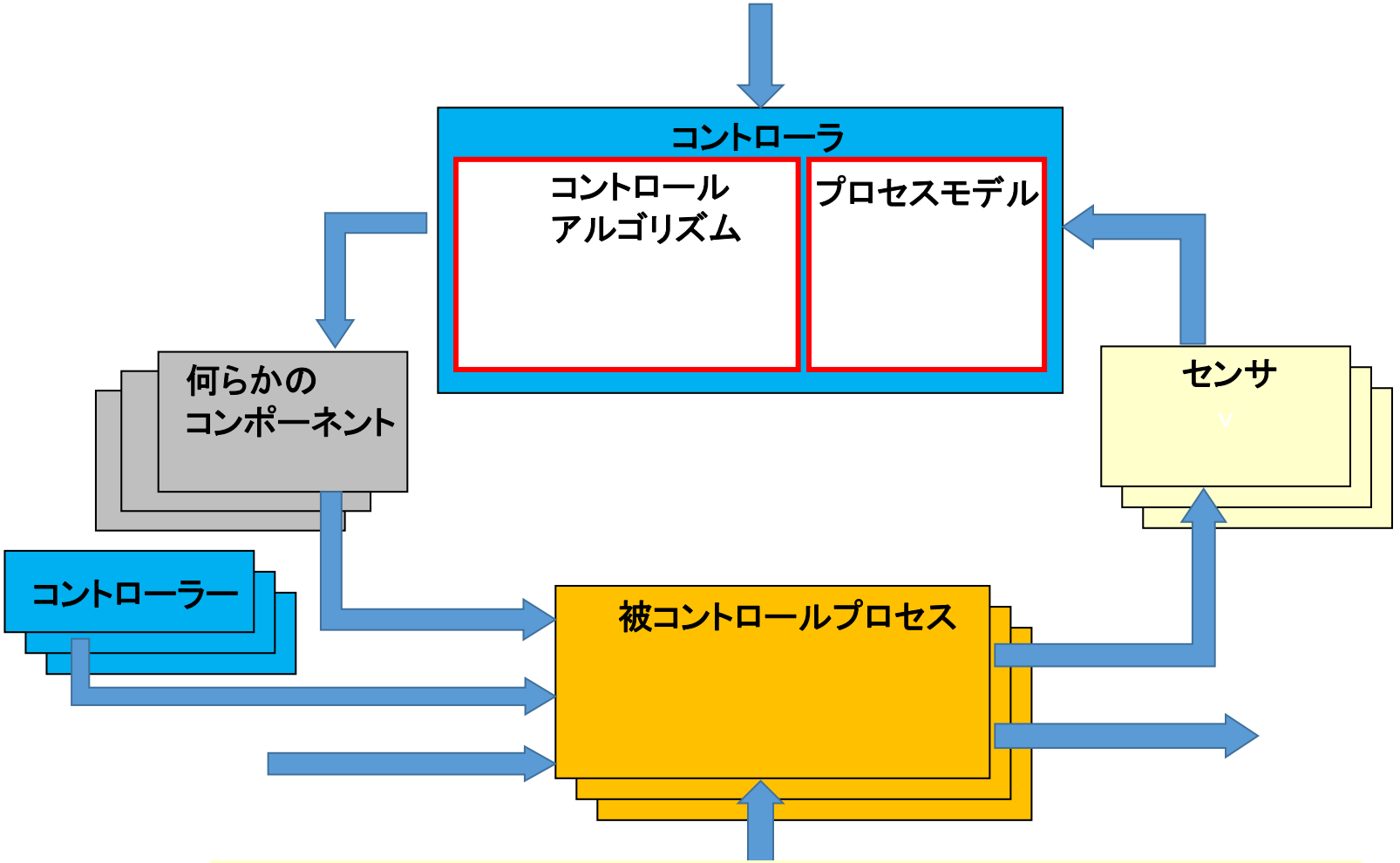
Foresight in sight

- CPSは構成要素間でやりとする媒体が多様
  - 一つ一つの構成要素が複数の役割　振る舞いを行う
- 複数のシステムが並行して動作する様な場合
  - コントロールループの特定が難しい
  - 相互作用による不具合の判定が難しい

UCA(Unsafe Control Action)の設定すら難しいかも？

複雑なコントロールループ

Foresight in sight



コントロールループは本当に回っているのか？

問題と解決アイディア

Foresight in sight

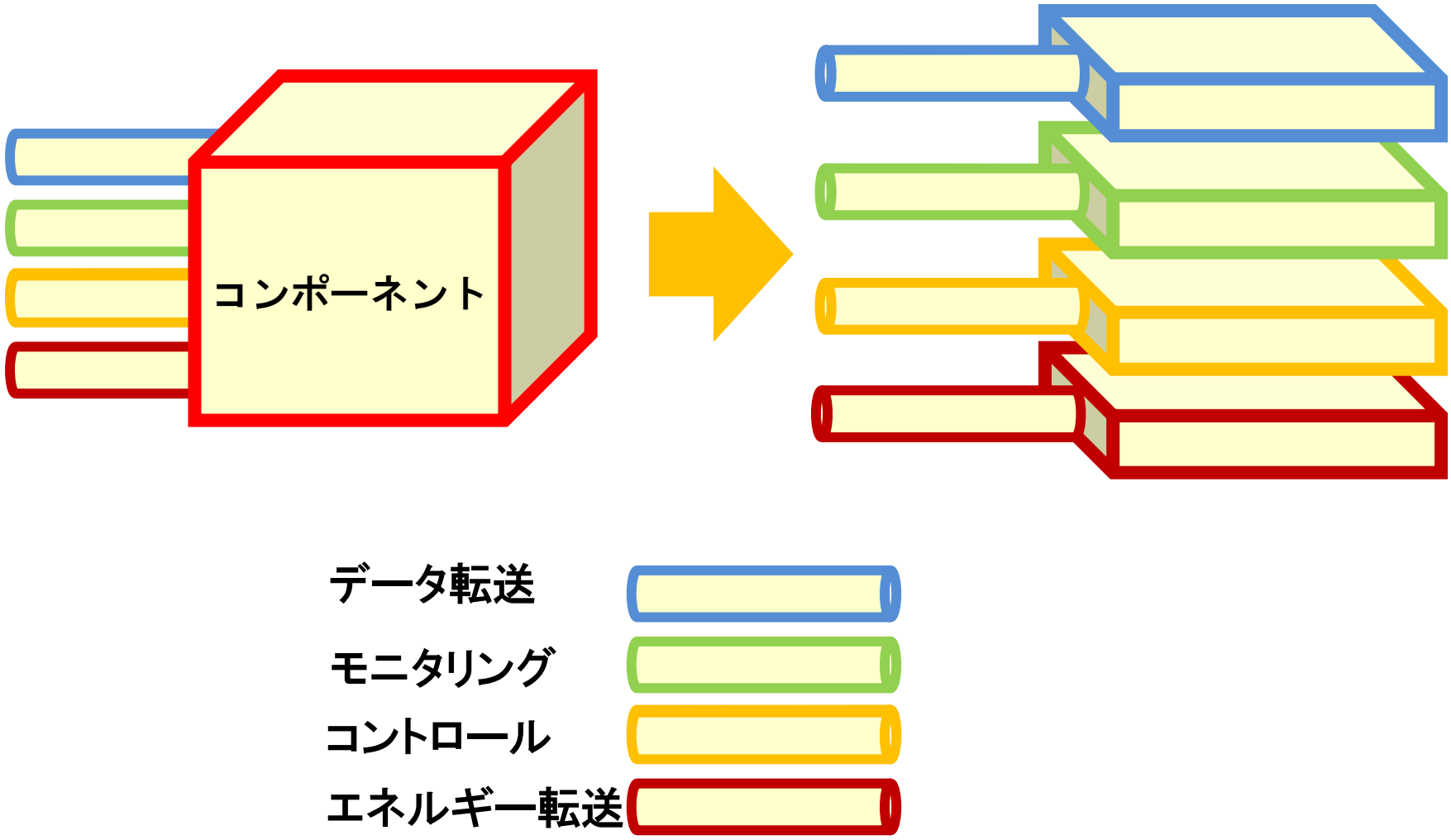
- 複雑なCPSを相互関係を頭の中だけで検証するのは難しい

- 検証するのはあくまで相互関係のみとして
  コントロールループが回っているかどうかを
  検証できないか

提案　階層化による振る舞いの整理

Foresight in sight

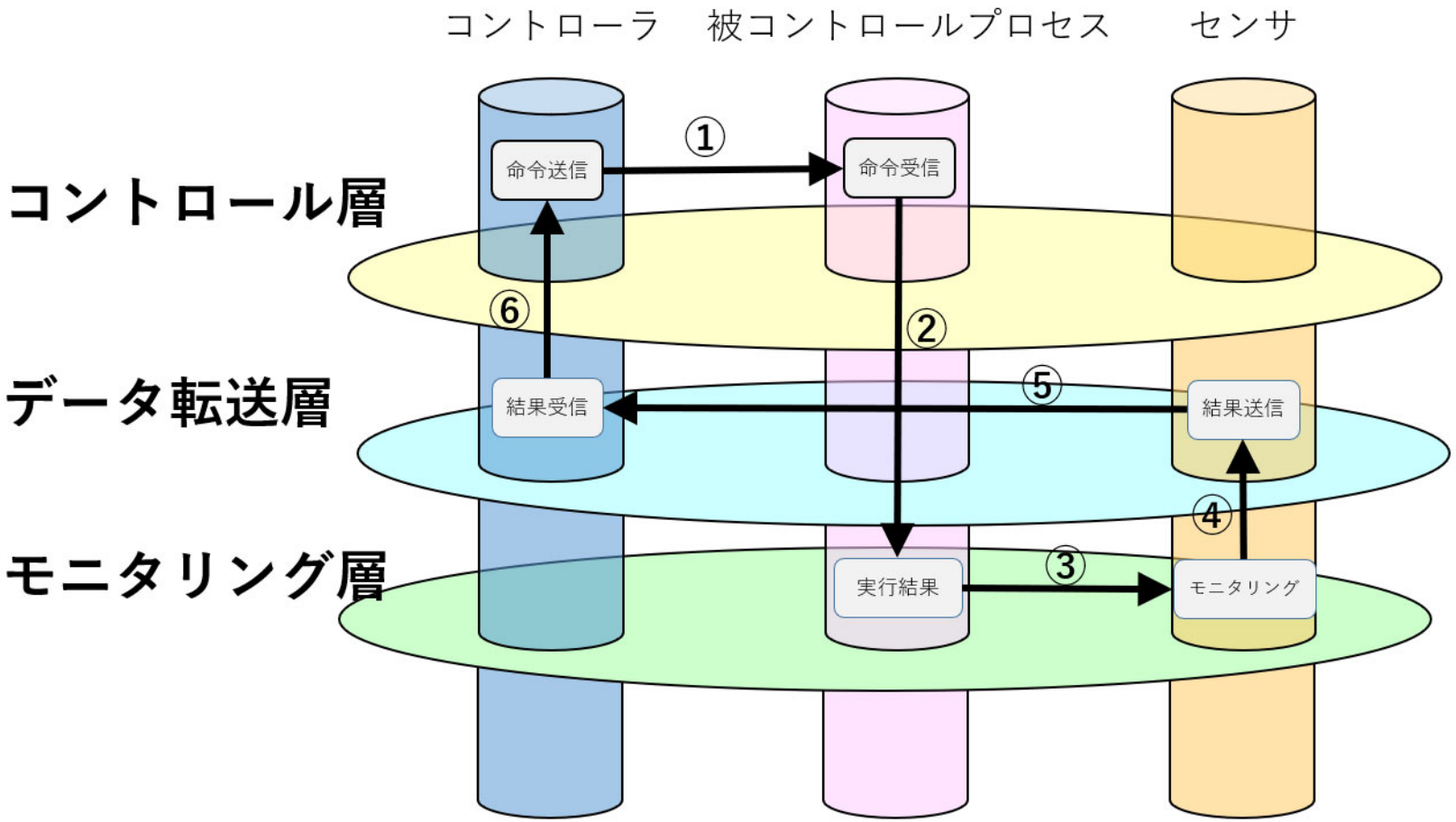
- 機能を詳細化するのではなく、振る舞いを階層化する



提案　モデルのイメージ

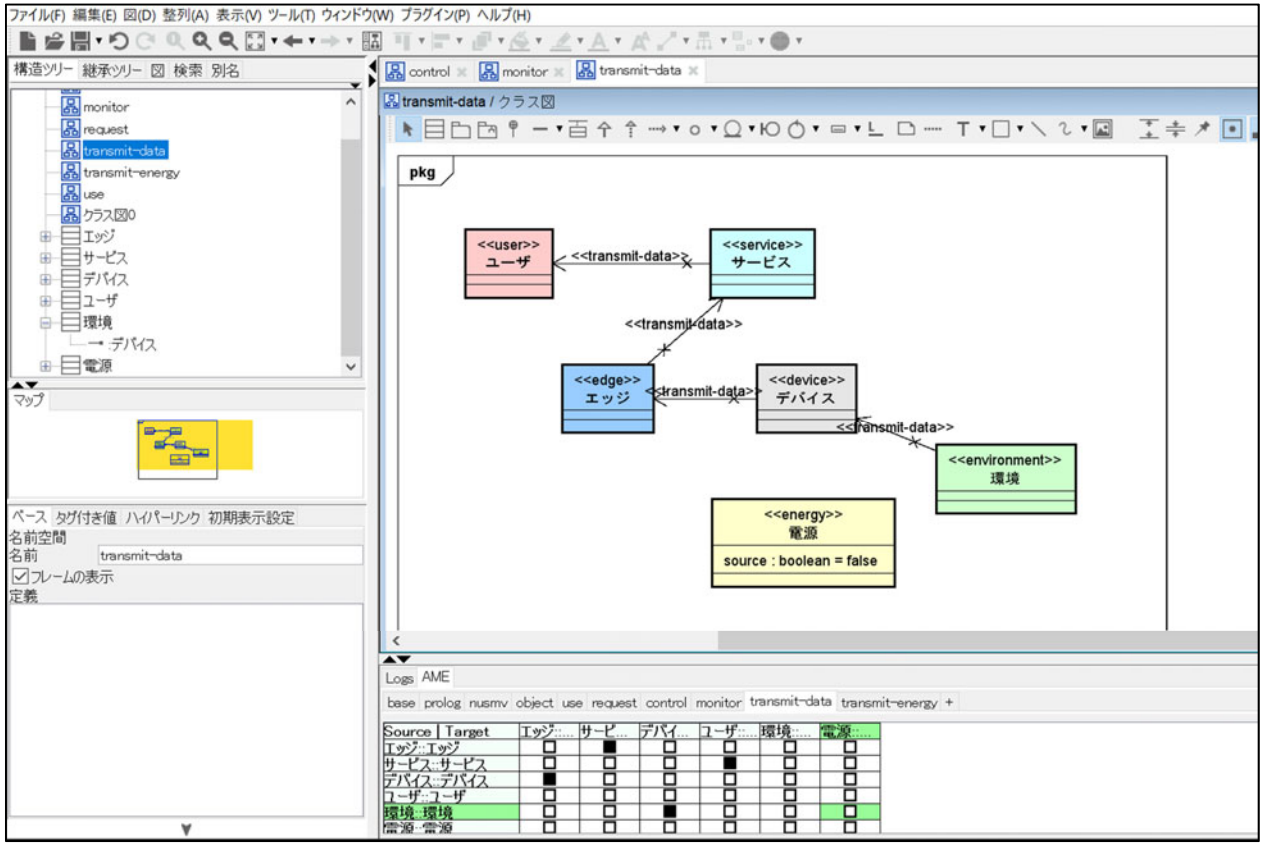
Foresight in sight

- 層ごとに分割してループを捉える



TORTE:IoTのアーキテクチャをモデル化する手法　信州大学、大阪大学との共同研究

- 要求分析工程向けたIoT システムアーキテクチャのモデリング手法を利用
  - 信州大学、大阪大学と共同研究



提案　構成要素間の関係の種類

Foresight in sight

種類	
Control	相手の振る舞いを変更する
Monitor	相手を監視する
Transmit-data	相手へデータを送る
Transmit-energy	相手へエネルギーを送る
Request	相手へデータを要求する

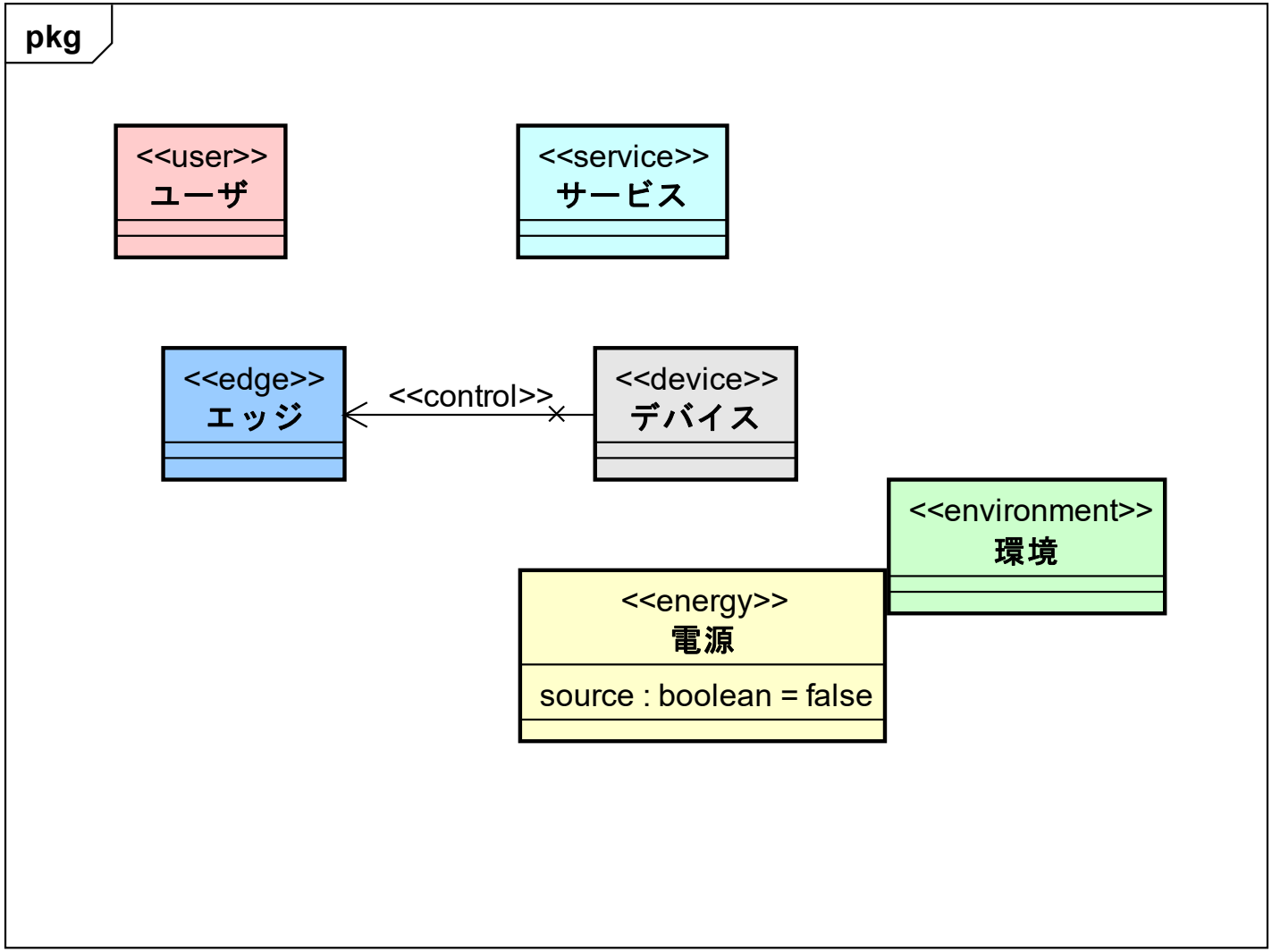
提案　構成要素の種類

Foresight in sight

種類	
Service	サイバー空間に展開されるサービス
Device	物理空間に展開されるデバイス
Environment	物理空間にある環境
Energy	物理空間にあり、エネルギーを送信、受信するもの
Edge	物理空間にありネットワークを構成するもの

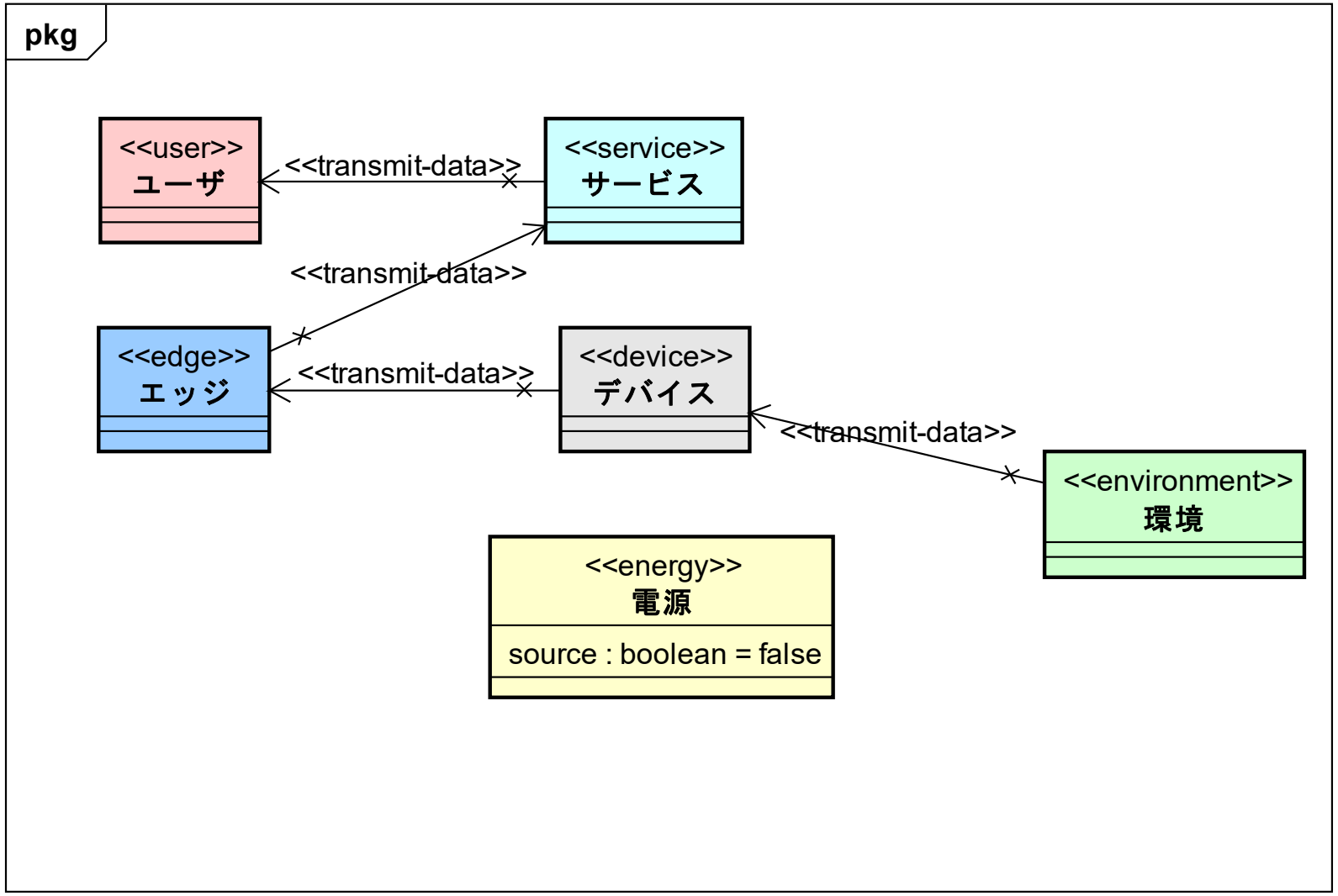
TORTE　定義例　コントロール層

Foresight in sight



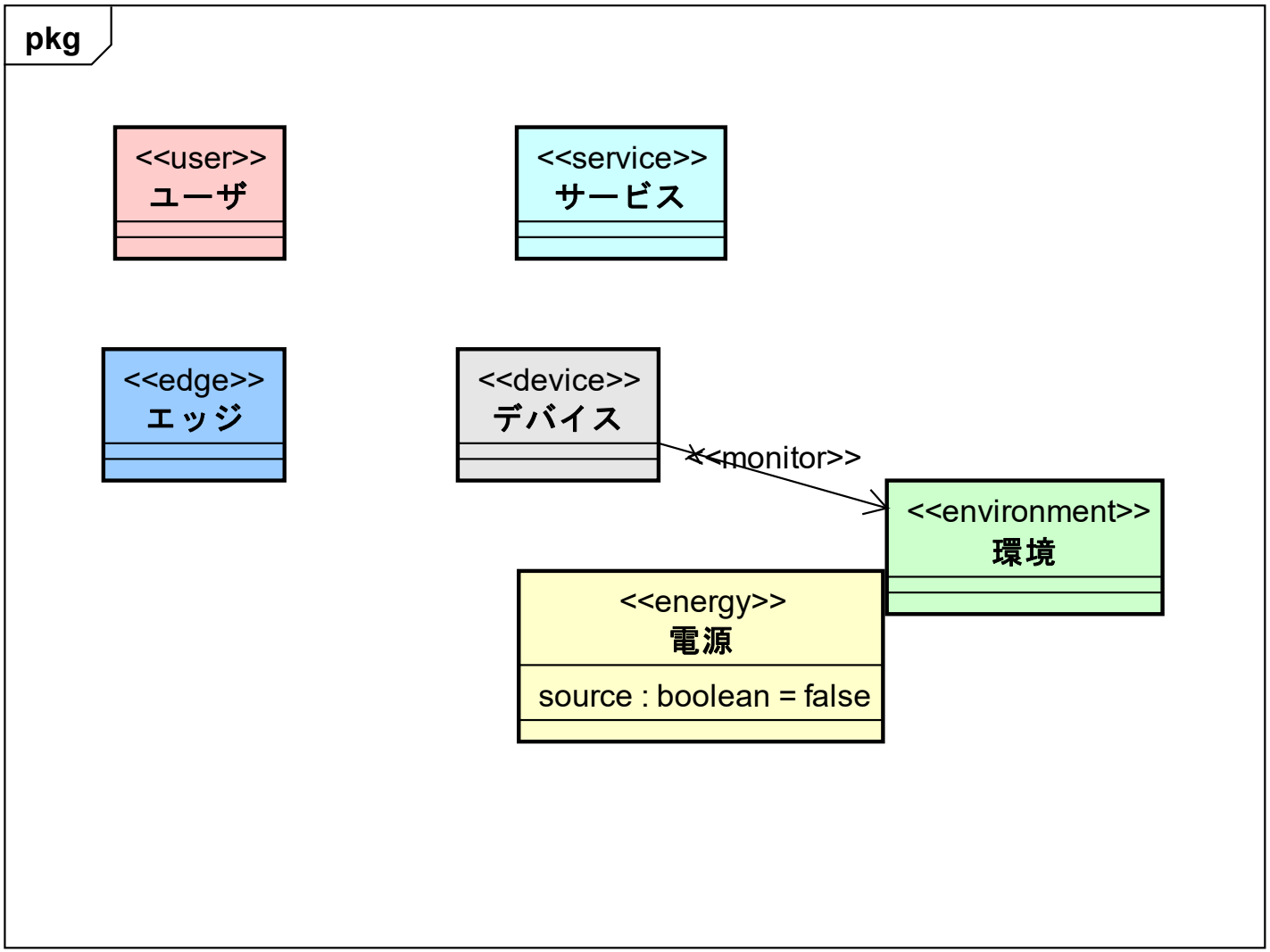
TORTE　定義例　データ転送層

Foresight in sight



TORTE　定義例　モニタリング層

Foresight in sight



提案　相互作用の検証

Foresight in sight

- 相互作用による不具合の発生は、形式手法のひとつであるモデル検査で検証する

  コントロールループが回り続けているかを検証する

- 振る舞いの整理により、定義すべき状態が明確になる

  ⇒検査モデルを作成する

- モデル検査ツールとしてNuSMVを想定

- あくまで相互作用の検証

適用事例　概要説明１

- 交通制御システム(traffic control system)
  - V2D(Vehicle-to-Device)により制御する
  - 想定するハザードはクルマがぶつかること

J. G. Filho; N. Przigoda; R. Wille; R. Drechsler, Towards a model-based verification methodology for Complex Swarm Systems (Invited paper), 2016 Sixth International Symposium on Embedded Computing and System Design (ISED),2016より

適用事例　構成

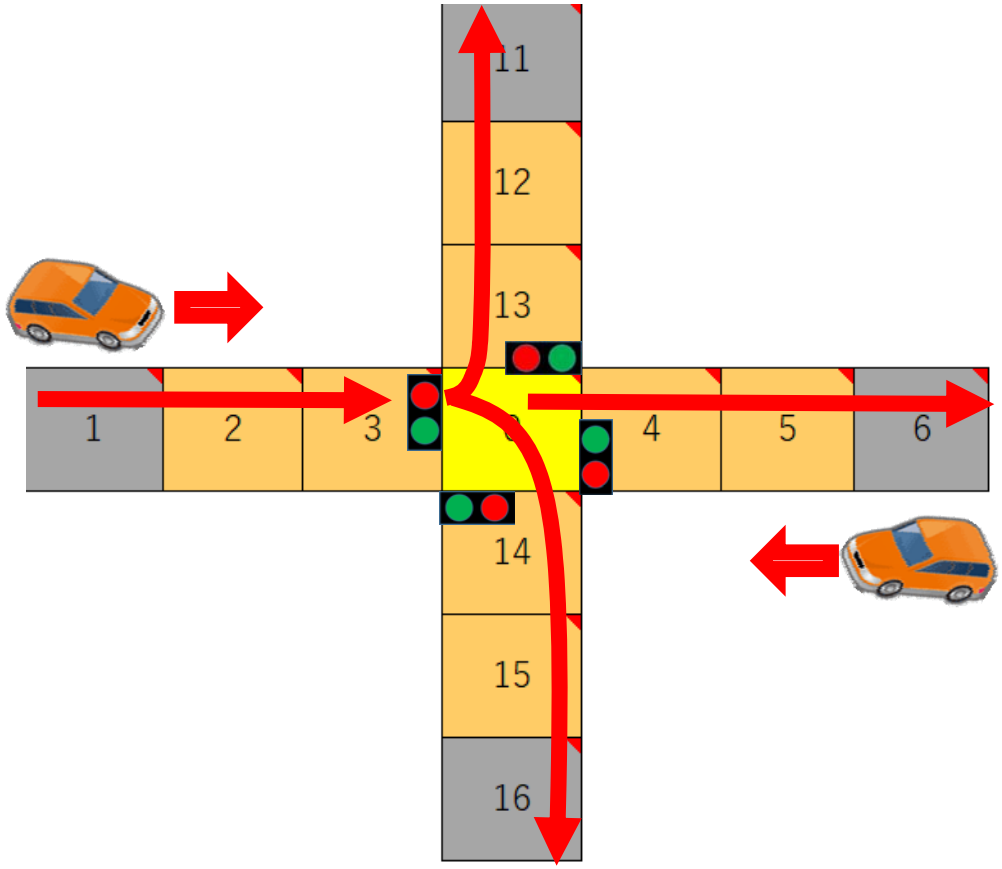
Foresight in sight

- システムの構成
  - Vehicle（クルマ：普通、自動、緊急）
  - Traffic Light（信号機：水平、垂直）
  - Street Slot（スロット単位に分割した道路）
  - STLCA（スマート信号制御アプリ）
  - ETLCA（緊急信号制御アプリ）
  - VSA（車両安全アプリ）
  - Device

適用事例　モデル

Foresight in sight

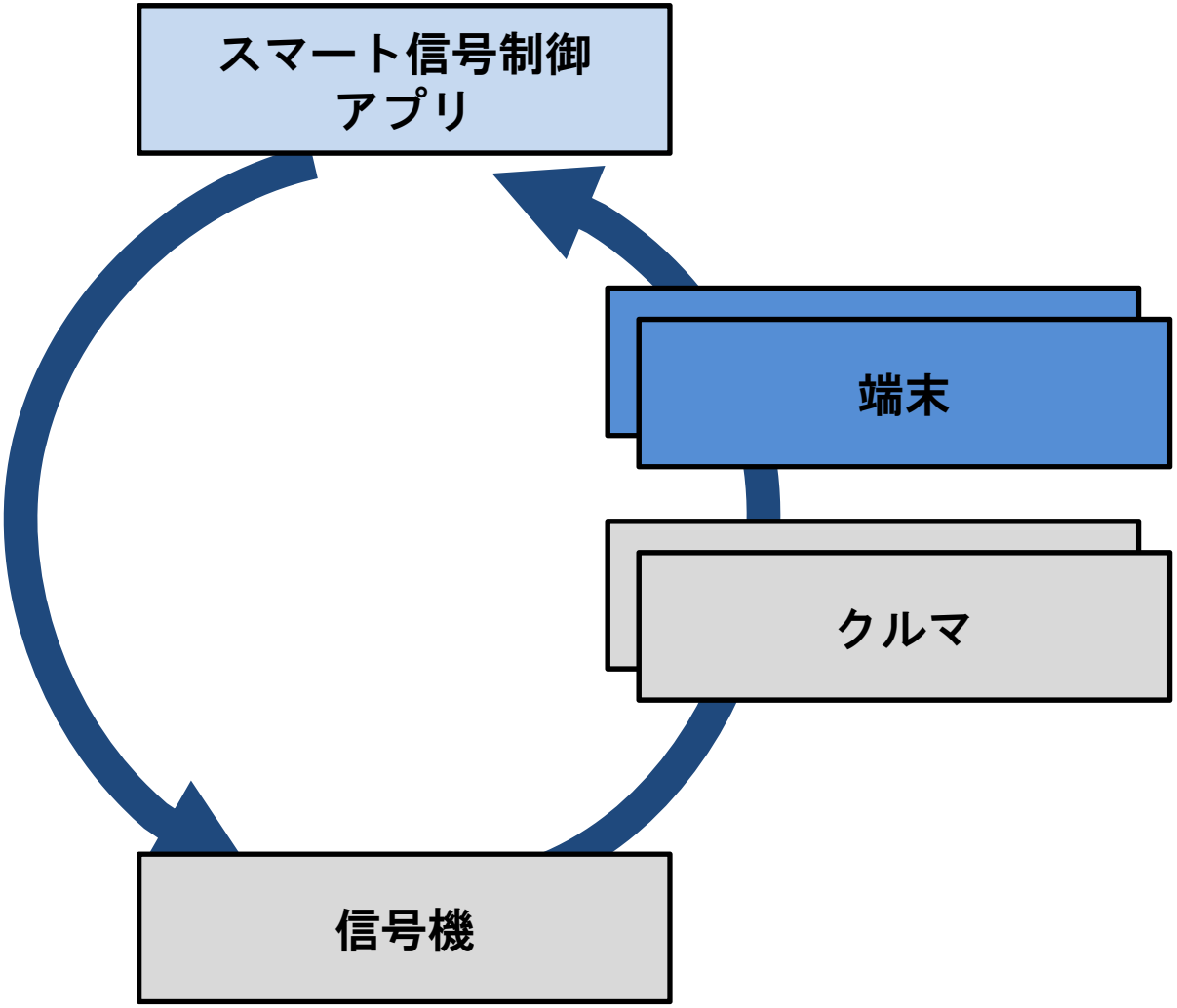
- 交差点をモデルとする
  - スロットベース
  - 水平・垂直方向に信号がある
  - クルマ(自動)を二台
  - UCAは？



適用事例2　交通制御システム

Foresight in sight

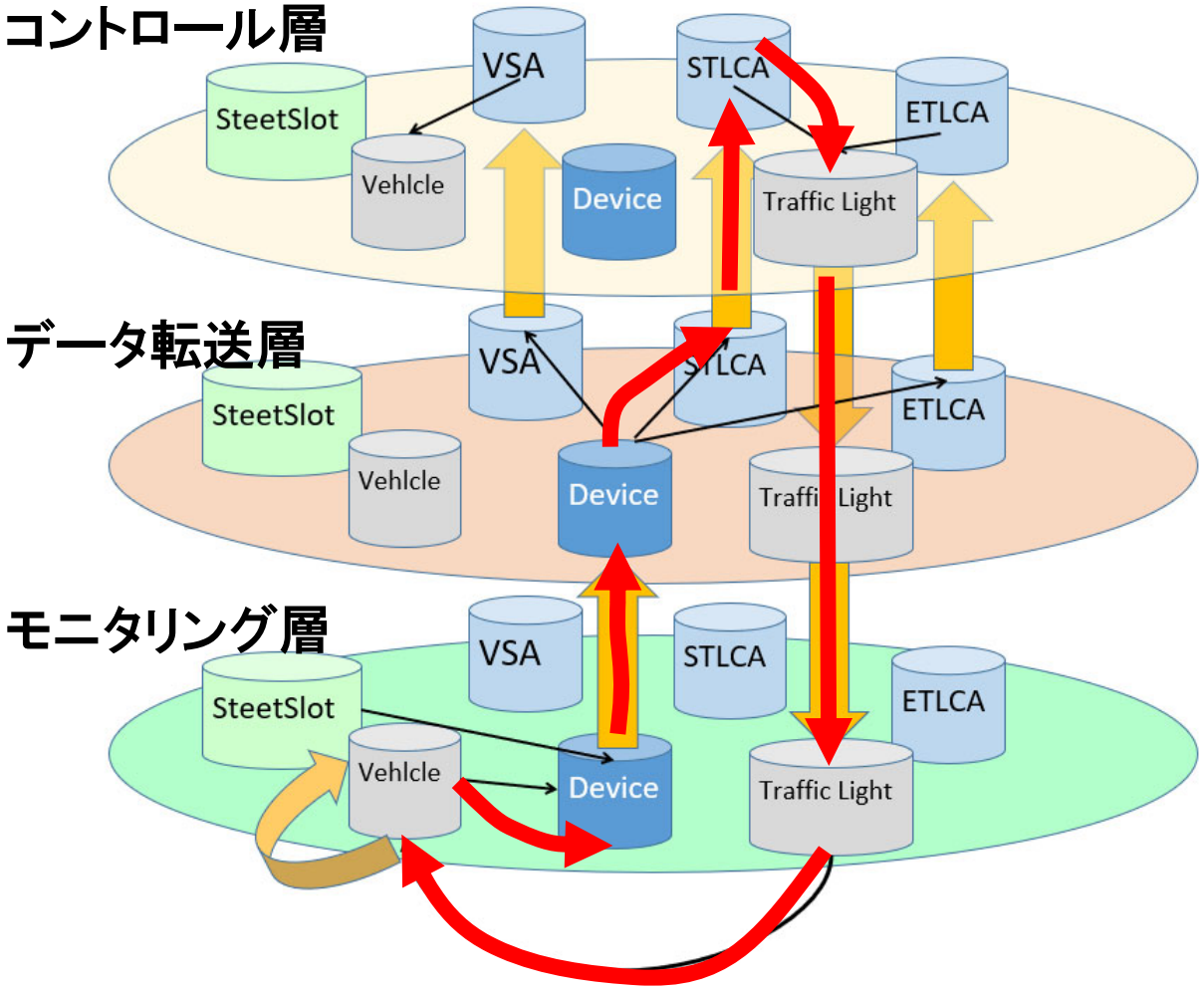
- コントロールループ



適用事例　コントロールループ

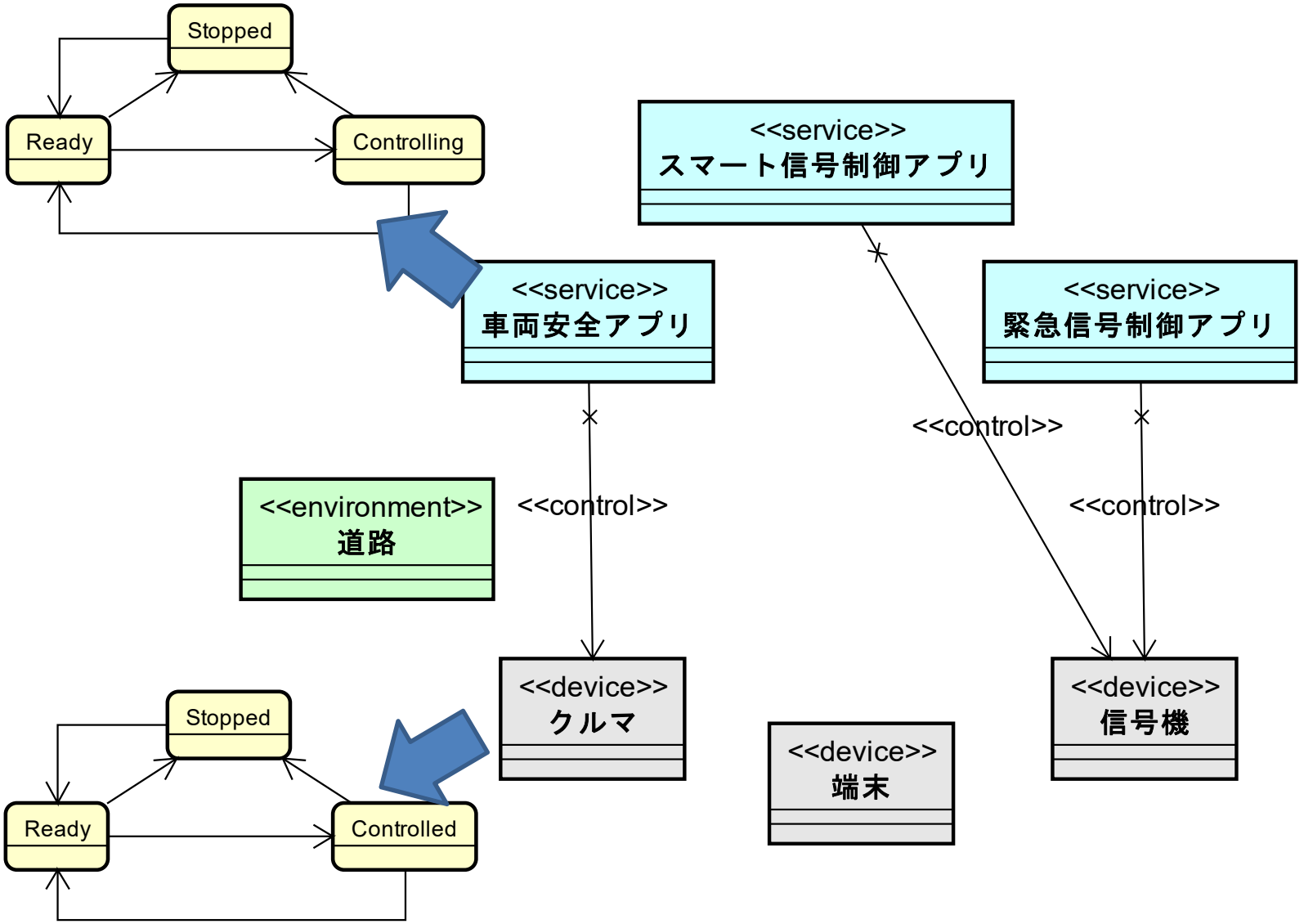
Foresight in sight

- 層を分けたコントロールループ



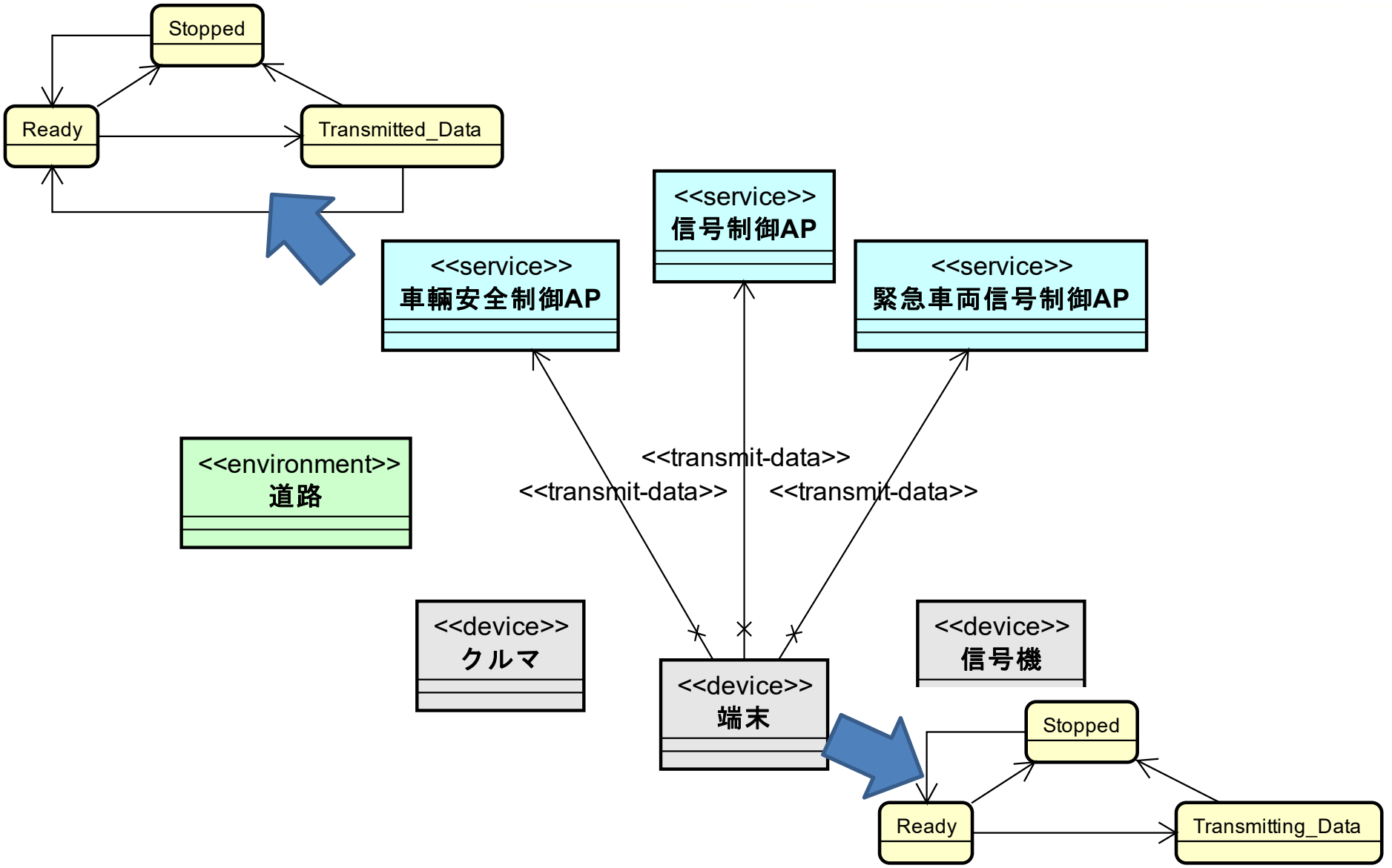
適用事例　TORTE定義　コントロール層

Foresight in sight



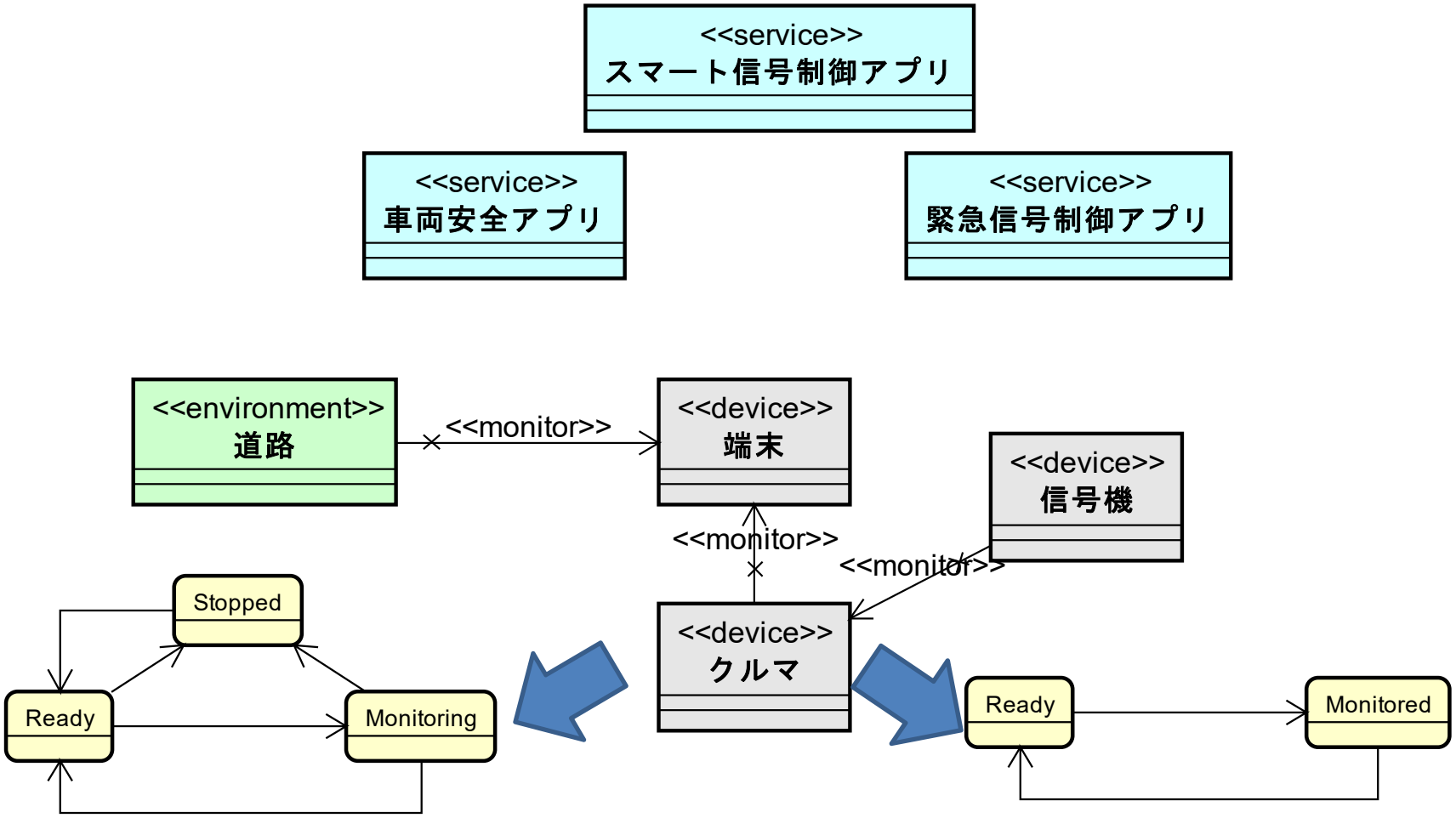
適用事例　TORTE定義　データ転送層

Foresight in sight



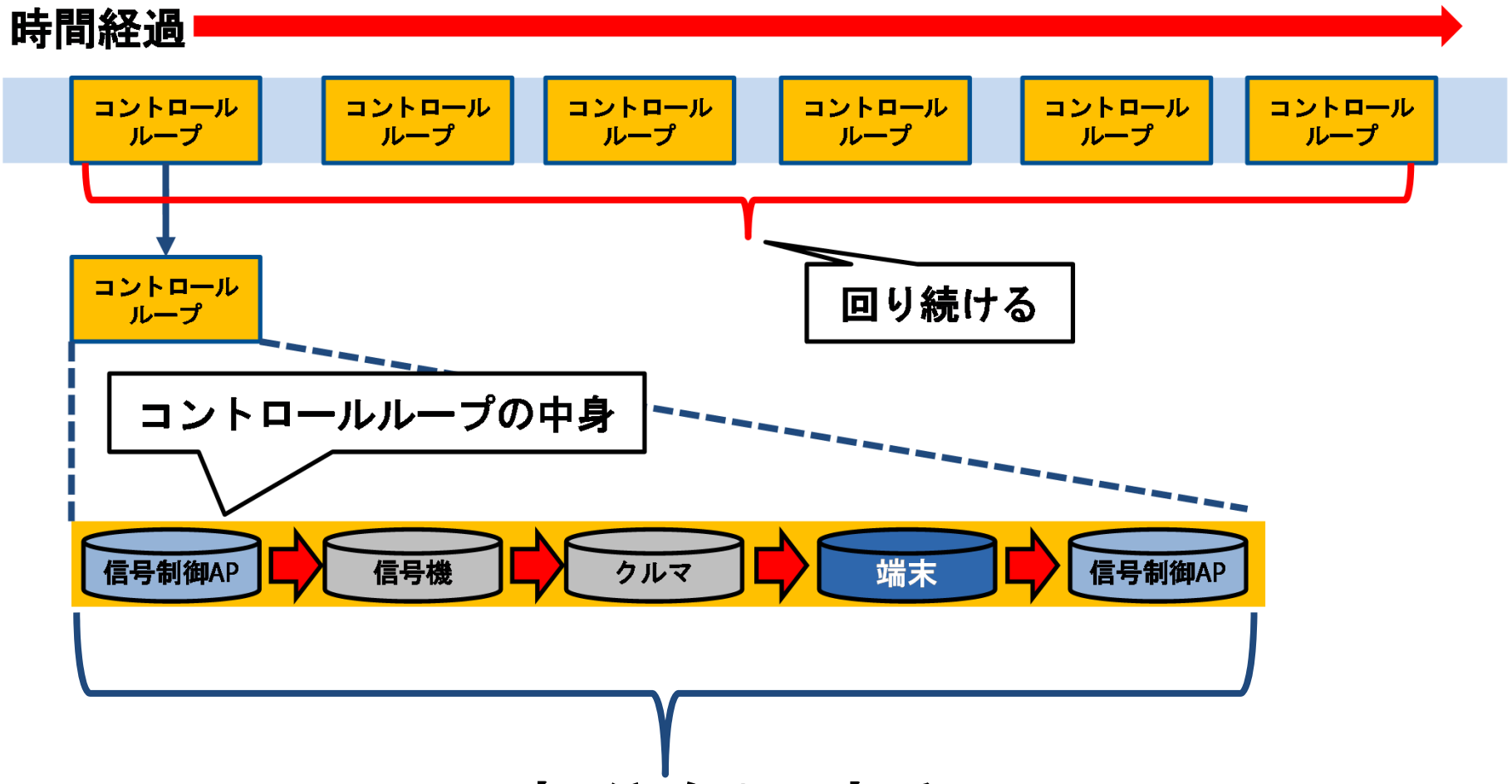
適用事例　TORTE定義　モニタリング層

Foresight in sight



コントロールループの検査

Foresight in sight



適用事例　検査式の内容

Foresight in sight

- 検査式の内容は以下のとおり

  デバイスがクルマをモニタリング

  ＆それ以降の時点で、**クルマがモニタリングされる**

  ＆それ以降の時点で、**デバイスがSTLCAへデータ転送する**

  ＆それ以降の時点で、 **STLCAがデータを受信する**

  ＆それ以降の時点で、 **STLCAが信号機を制御する**

  ＆それ以降の時点で、**信号機が制御される**

  ＆それ以降の時点で、**クルマが信号機をモニタイング**

  ＆それ以降の時点で、**信号機がモニタリングされる**

  上記処理が無限回繰り返せるか。

- 結果は**FALSE**になる。

検査　実行

Foresight in sight

検査式：□ ◇ （S）
S＝信号制御AP⇒信号機⇒クルマ⇒端末⇒信号制御APの遷移
検査結果：「満たされない」
確認できた原因：クルマの接近しすぎによる緊急停止.

反例

Foresight in sight

-> State: 1.24 <-	Monitoring	Monitored	Ready	Controlling	Ready	Monitoring	Monitored	TRUE
-> State: 1.25 <-	Monitoring	Monitored	Ready	Controlling	Ready	Monitoring	Monitored	TRUE
-> State: 1.26 <-	Monitoring	Monitored	Ready	Controlling	Controlled	Monitoring	Monitored	FALSE
-> State: 1.27 <-	Monitoring	Monitored	Transmitted	Controlling	Ready	Monitoring	Monitored	FALSE
-> State: 1.28 <-	Monitoring	Monitored	Transmitted	Controlling	Ready	Monitoring	Monitored	FALSE
-> State: 1.29 <-	Monitoring	Monitored	Transmitted	Controlling	Ready	Monitoring	Monitored	FALSE
-> State: 1.30 <-	Monitoring	Monitored	Transmitted	Controlling	Ready	Monitoring	Monitored	FALSE
-> State: 1.31 <-	Monitoring	Monitored	Transmitted	Controlling	Ready	Monitoring	Monitored	FALSE
-> State: 1.32 <-	Monitoring	Monitored	Transmitted	Controlling	Ready	Monitoring	Monitored	FALSE
-> State: 1.33 <-	Monitoring	Monitored	Transmitted	Controlling	Ready	Monitoring	Monitored	FALSE
-> State: 1.34 <-	Monitoring	Monitored	Transmitted	Controlling	Ready	Monitoring	Monitored	FALSE
-> State: 1.35 <-	Monitoring	Monitored	Transmitted	Controlling	Ready	Monitoring	Monitored	FALSE
-> State: 1.36 <-	Monitoring	Monitored	Transmitted	Controlling	Ready	Monitoring	Monitored	FALSE
-> State: 1.37 <-	Monitoring	Monitored	Transmitted	Controlling	Ready	Monitoring	Monitored	FALSE
-> State: 1.38 <-	Monitoring	Monitored	Ready	Controlling	Controlled	Stopped	Monitored	FALSE
-> State: 1.39 <-	Monitoring	Monitored	Ready	Controlling	Ready	Stopped	Ready	FALSE
-> State: 1.40 <-	Monitoring	Monitored	Ready	Controlling	Controlled	Stopped	Monitored	FALSE
-> State: 1.41 <-	Monitoring	Monitored	Transmitted	Controlling	Ready	Stopped	Ready	FALSE
-> State: 1.42 <-	Monitoring	Monitored	Transmitted	Controlling	Ready	Stopped	Ready	FALSE
-> State: 1.43 <-	Monitoring	Monitored	Transmitted	Controlling	Ready	Stopped	Ready	FALSE
-> State: 1.44 <-	Monitoring	Monitored	Transmitted	Controlling	Ready	Stopped	Ready	FALSE
-> State: 1.45 <-	Monitoring	Monitored	Transmitted	Controlling	Ready	Stopped	Ready	FALSE
-> State: 1.46 <-	Monitoring	Monitored	Transmitted	Controlling	Ready	Stopped	Ready	FALSE
-> State: 1.47 <-	Monitoring	Monitored	Ready	Controlling	Controlled	Stopped	Monitored	FALSE
-> State: 1.48 <-	Monitoring	Monitored	Ready	Controlling	Ready	Stopped	Ready	FALSE

適用事例　検査結果

Foresight in sight

- FALSEになった原因
  - クルマのモニタリングが中断されたため、
    ループが止まった
  - クルマの接近しすぎ、同時に交差点に進入して、左⇒右**クルマが左折**、もう右⇒左の**クルマが右折**したため
    緊急停止⇒走行終了⇒機能停止⇒モニタリング中断
- UCAは「交差点内に(左折)対向車がいるのに右折を開始する」
- 安全制約は「右折時に交差点内で(左折)対向車がいる場合は右折を開始しない」

まとめ

Foresight in sight

- 場合によっては、コントロールループをモデル検査で検証できると思われる
- 事例を提示することにより、CPSにおけるUCAを検討する手がかりになる
- 課題
  - コントロールループの特定方法・・自動検出
  - UCAを決めてからの適用方法
- 今後の予定
  - TORTEモデル⇒検査モデル変換の自動化

    ⇒自動生成のツールを作成中
  - 提案手法の特徴整理

    ⇒他の事例へも適用して本手法の特徴を確認する

Foresight in sight

UNISYS