2014年度ソフトウェア工学分野の先導的研究支援事業
成果概要

システムモデルと繰り返し型モデル検査による次世代自動運転車を取り巻くSystem of Systemsのアーキテクチャ設計

慶應義塾大学　西村　秀和

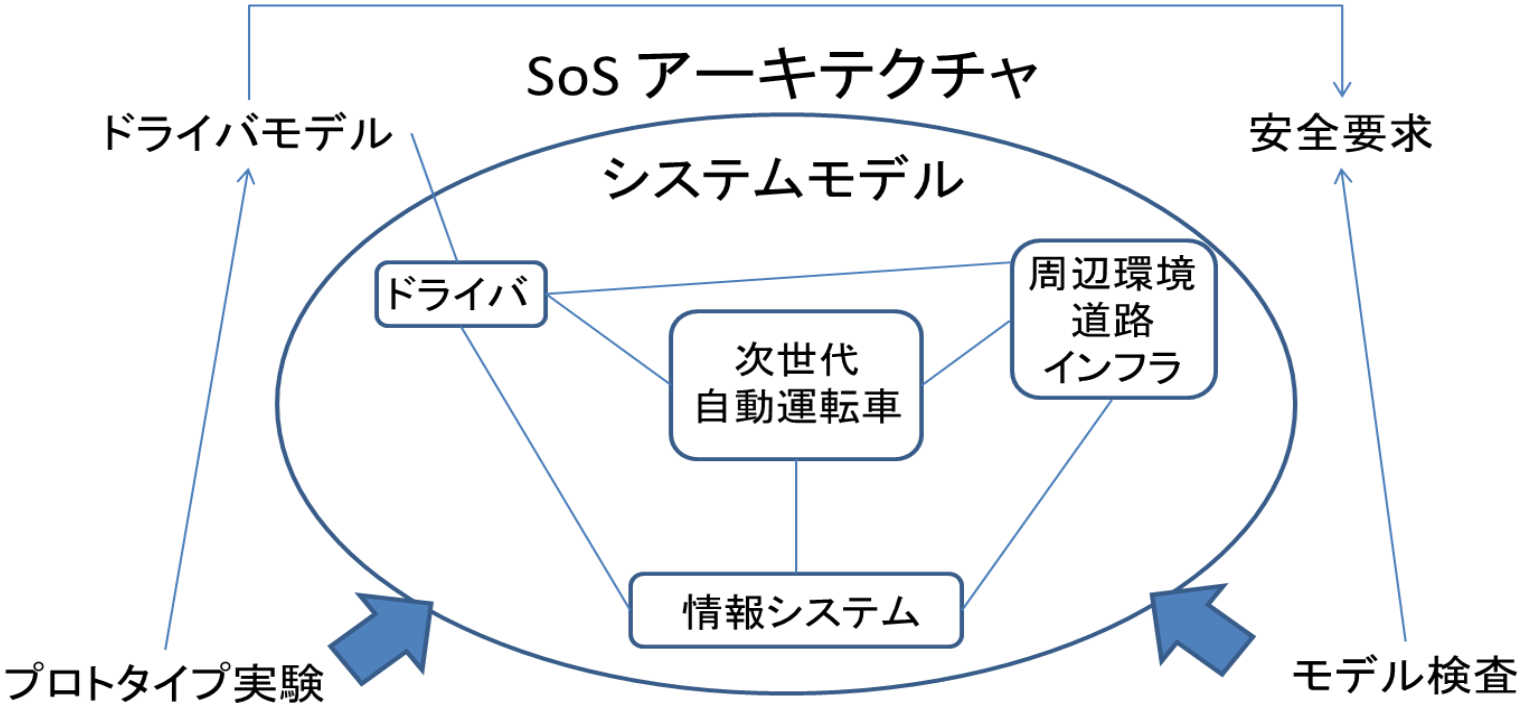
目次

1. 研究概要
2. 研究成果
3. 成果の活用見込み
4. 研究成果の発表、投稿、引用等
5. まとめ

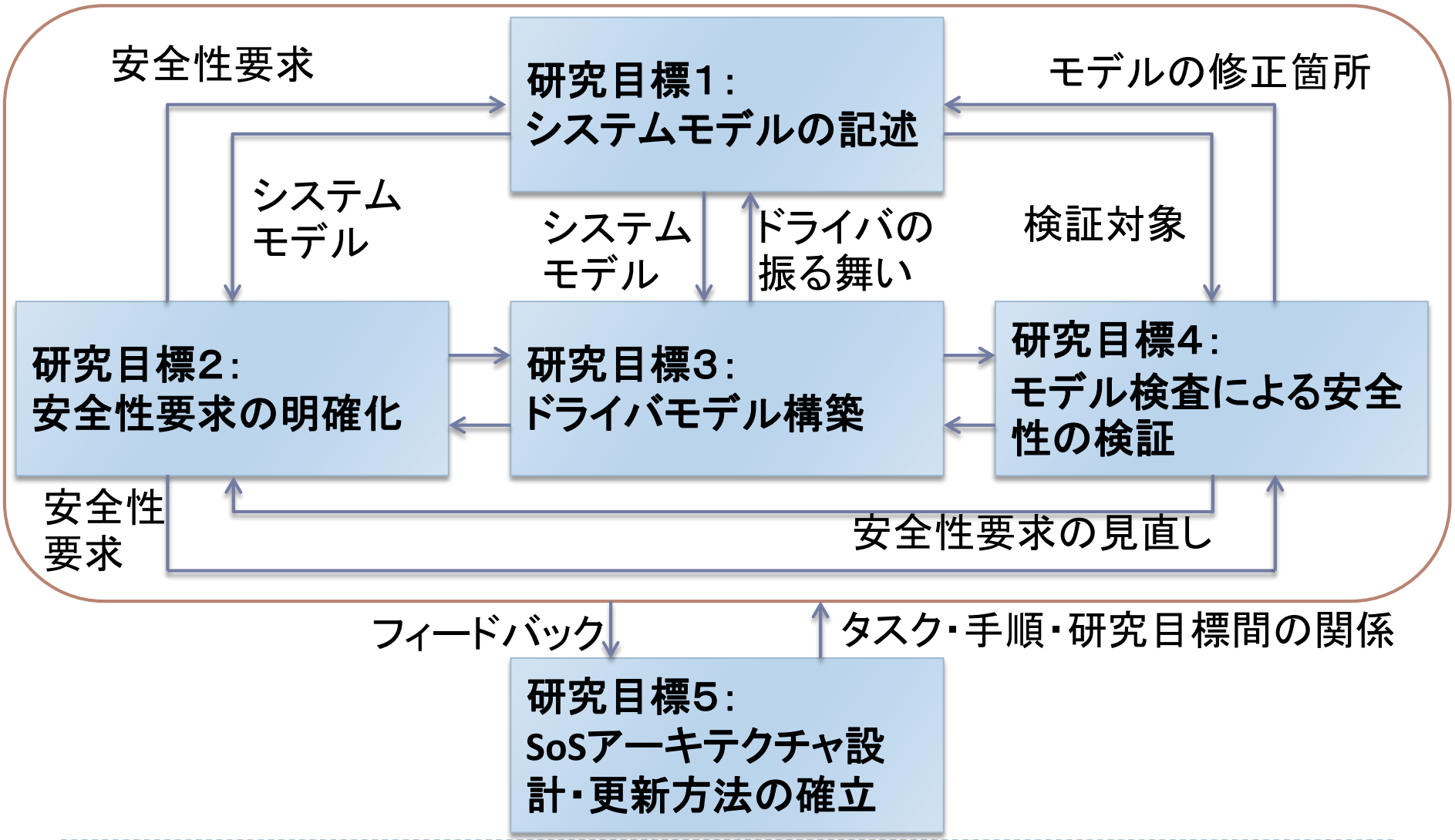
1．研究概要

次世代自動運転車の導入に向け、それを取り巻く交通インフラ、各種情報システムを含む周辺環境、ドライバなどをSystem of Systems（SoS）として捉えた上で、安全性を考慮したアーキテクチャを構築する。

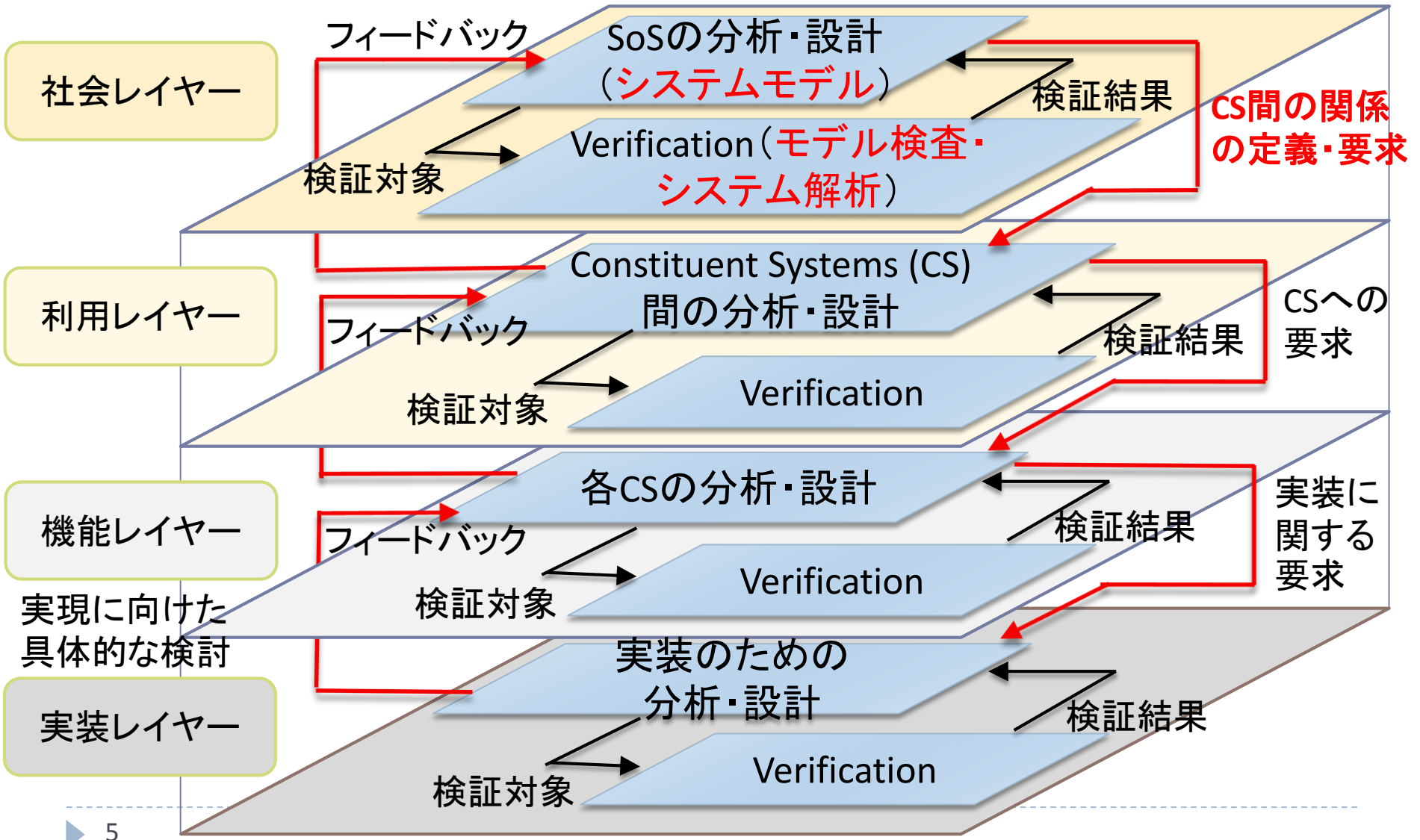
自動運転技術の研究のみでは、システムレベルでの安全性の確保は難しいため、安全なSoSアーキテクチャを構築することが課題と考える。



1. 研究概要:研究の進め方



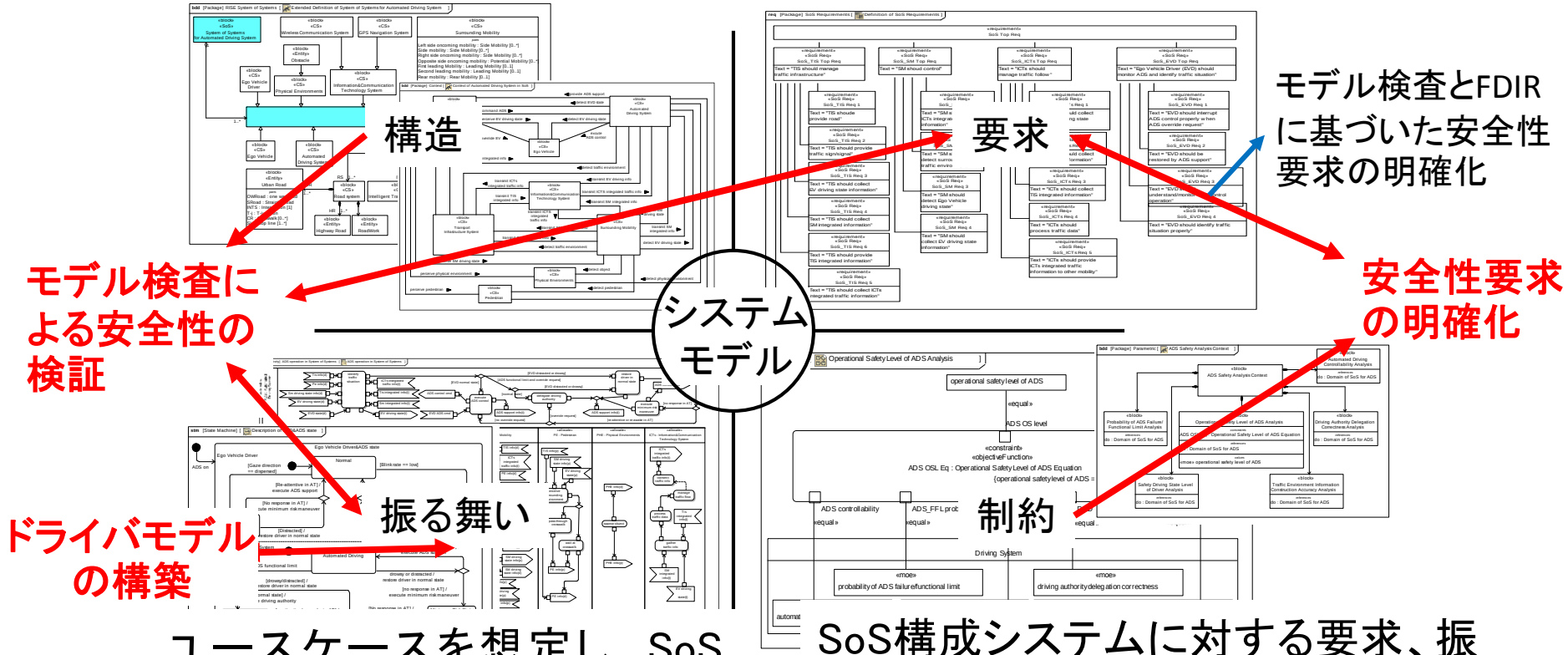
研究目標5:
2. 研究成果:SoSアーキテクチャ設計・更新方法



研究目標2:
2. 研究成果:SoSアーキテクチャ

SoS構成システムの構成とそれらの相互作用を用いたコンテキスト定義

SoS構成システムの振る舞いを検討し、各構成システムの要求を導出



ユースケースを想定し、SoS構成システム間の相互作用と自動運転システムとドライバの状態遷移を定義

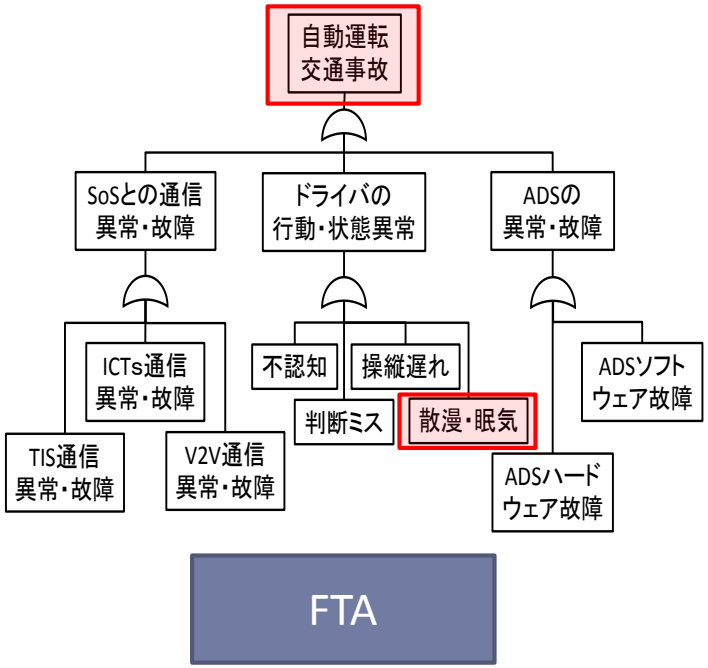
SoS構成システムに対する要求、振る舞い、構造を考慮した自動運転車の安全性を評価するパラメトリック制約を定義

2014年度ソフトウェア工学分野の先導的研究支援事業

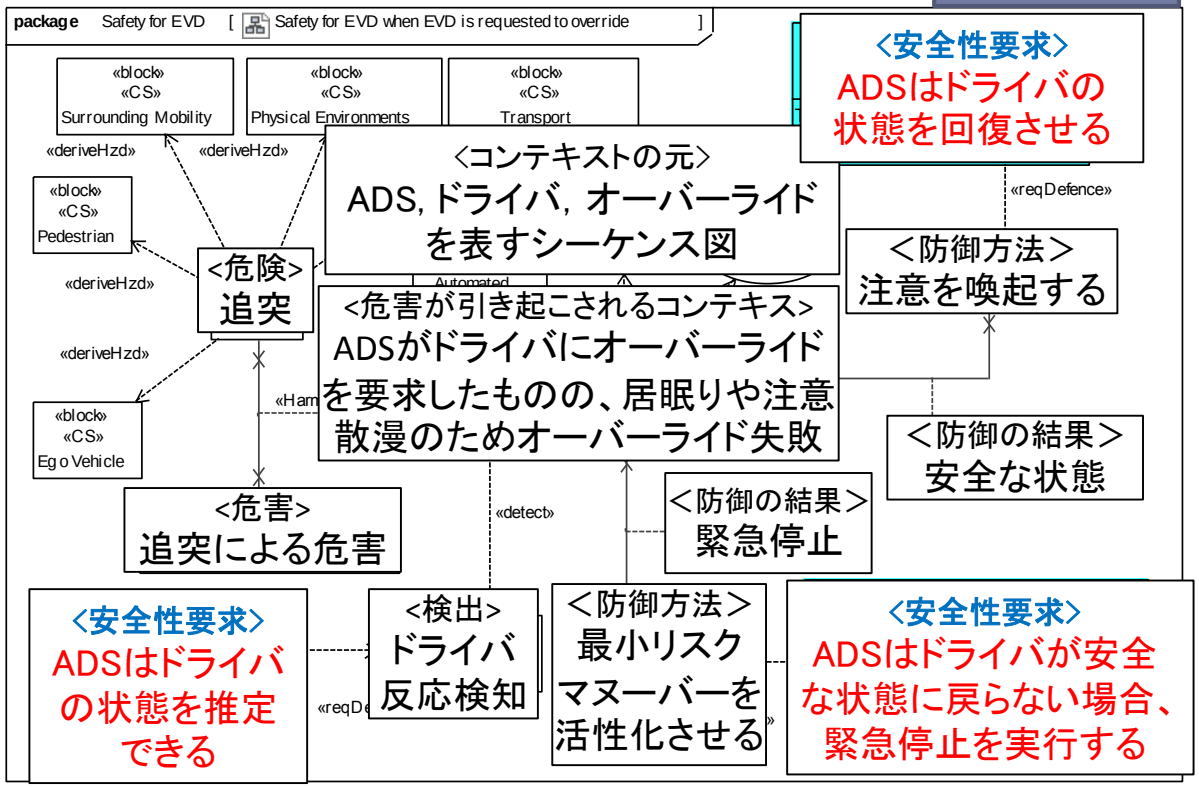
研究目標2:
2. 研究成果:安全性要求(1)

- FDIR(Fault Detection, Isolation and Recovery)に基づく安全性要求の明確化
  - 危険、危害、危険状況それぞれに対する安全対策をモデル化し、自動運転車のSoS構成システムに関する安全性要求を明らかにした。

SafeML



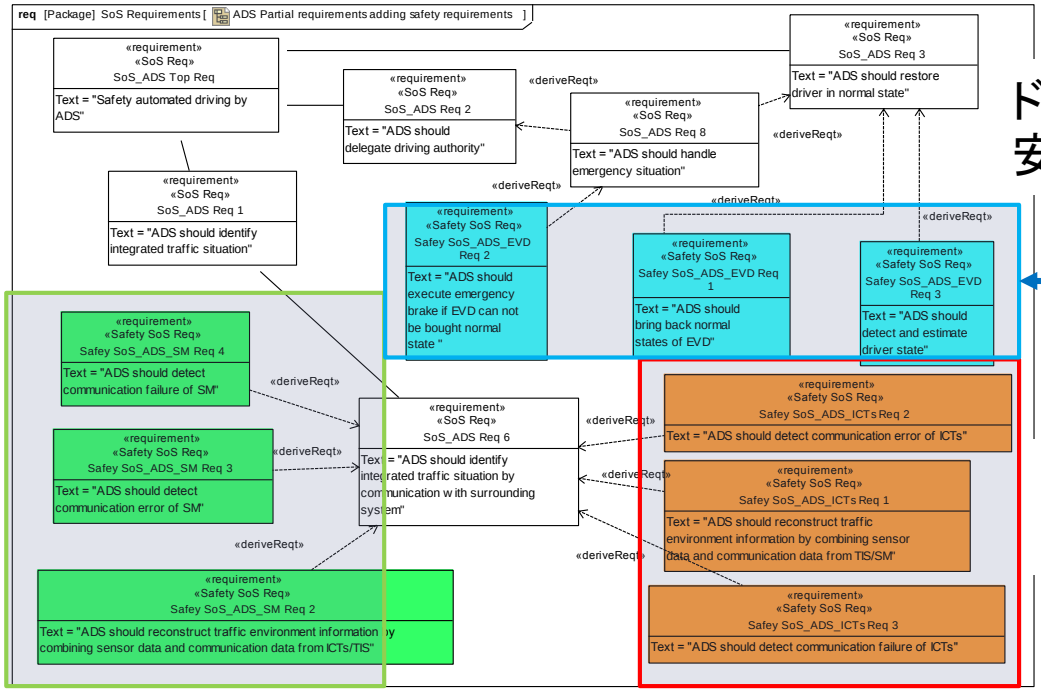
FTA



2014年度ソフトウェア工学分野の先導的研究支援事業

研究目標2:
2. 研究成果:安全性要求(2)

- FDIRに基づく安全性要求のSafeMLによる検討

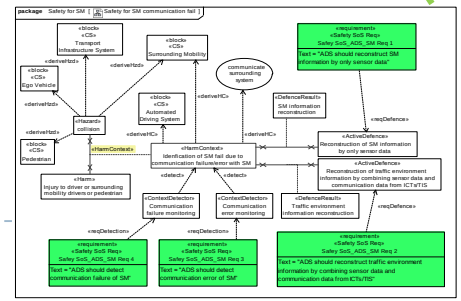


ドライバに対する安全性要求

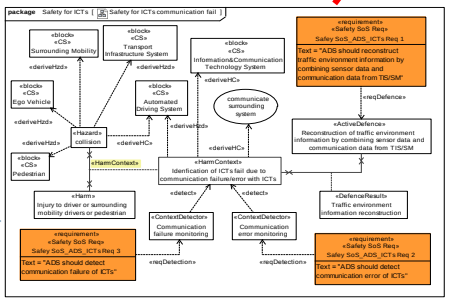
周辺モビリティに対する安全性要求

ICTs対する安全性要求

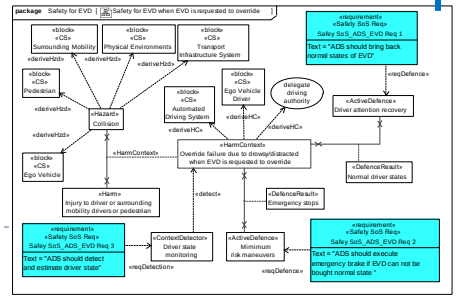
周辺モビリティとの通信異常



ICTsとの通信異常

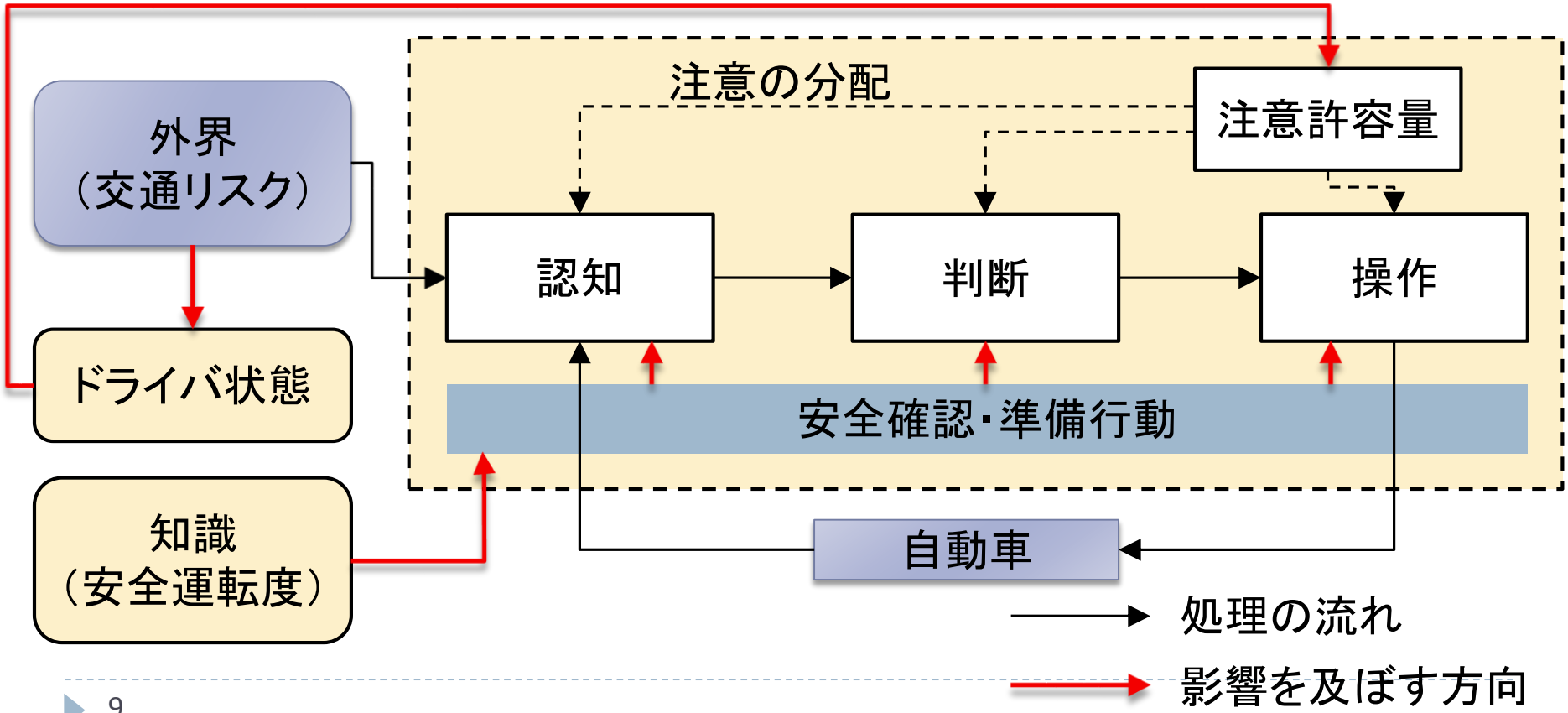


ドライバのオーバーライド



研究目標3:
2. 研究成果:ドライバモデル

- ドライバモデルには、運転行動に加え、ドライバの状態と安全運転度を含めている。⬅実験結果に基づく分析より
  - プロトタイプ実験(1年目)および公道走行実験(2年目)



2014年度ソフトウェア工学分野の先導的研究支援事業

研究目標4：
2．研究成果：SoSアーキテクチャの検証（1）

- SysMLで記述されたシステムモデルをCSP（Communicating Sequential Processes）モデルで記述し、モデル検査を実施
  - SoSの各構成システムを並行して動作するプロセスと見なす
  - ADSがドライバを不安全な状態から安全な状態に戻す際に、一定時間応答を待つことを表現するために、Timed-CSPのWait関数を利用
  - Wait関数を用いたドライバの安全運転度の考慮

システムモデル＆
ドライバモデル

アクティビティ図：各CSの振舞い
状態機械図：状態の遷移条件
ドライバモデル：安全運転度

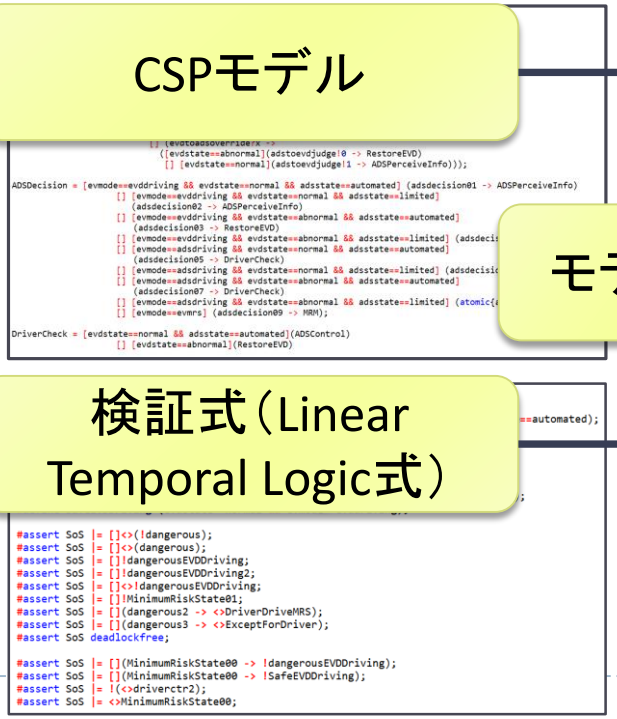
安全性要求　＆
CSPモデル作成時の検討

安全上、遷移すべきではない
状態の定義

CSPモデル

検証式（Linear
Temporal Logic式）

モデル検査



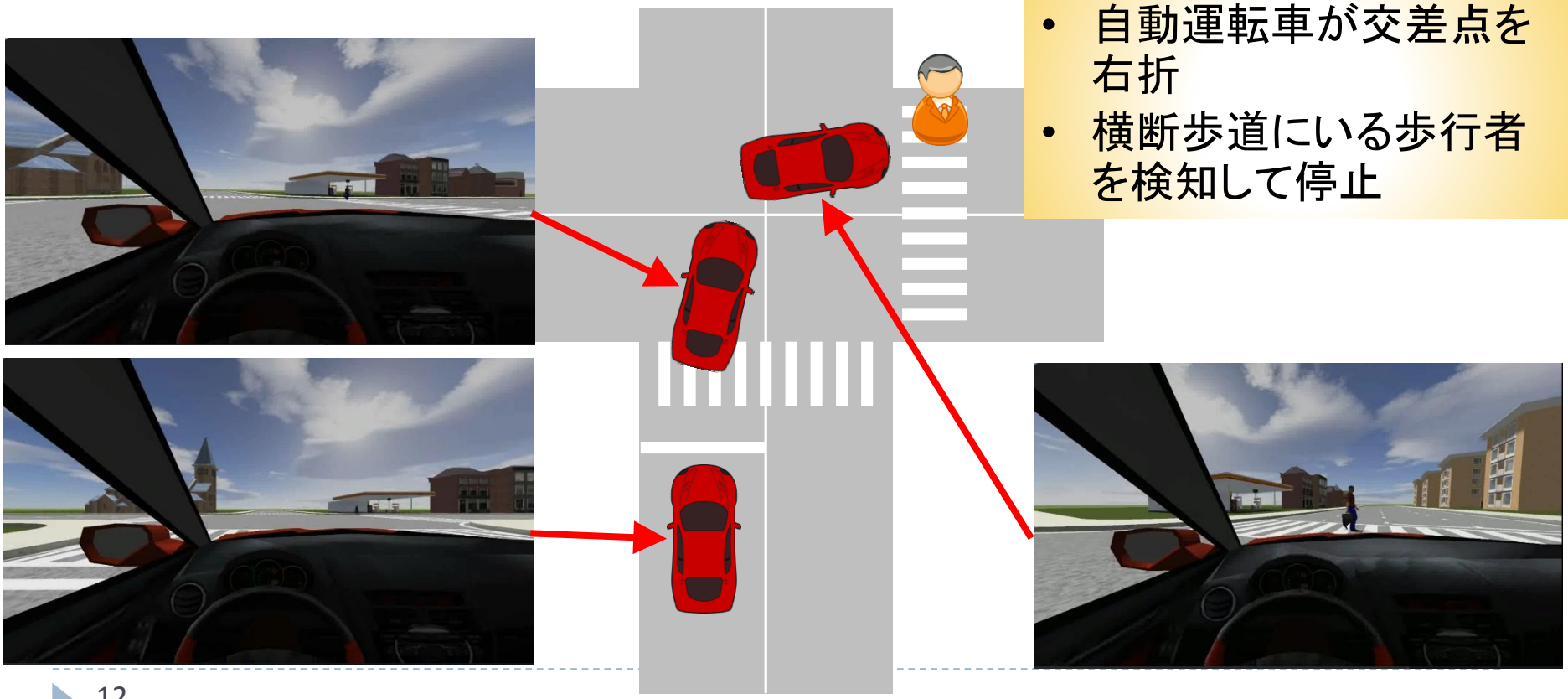
2014年度ソフトウェア工学分野の先導的研究支援事業

研究目標4：
2．研究成果：SoSアーキテクチャの検証（2）

- CSPモデルの検証結果の例
  - [検証内容]：”ADSの機能が限られた状態”かつ”ドライバが不安全な状態”かつ”MRSではない状態”となることはない。
  - [結果]：ドライバがオーバーライドし、マニュアル運転を開始後に、ドライバの状態が不安全になるという反例が示された。
    この反例より、マニュアル運転中は、ドライバ自身が安全を確保するという責任を負うべきであると考察した。
  - [検証内容]：”MRS”であり、かつ、”ドライバが正常な状態”であることはない。
  - [結果]：ドライバが不安全な状態にあるときは、ADSはドライバの状態を戻そうとする。その間にドライバが正常に戻っているにも関わらず、ドライバがADSに適切な応答をしないため、MRSに移行するという反例が示された。
    この反例は、ADSがドライバが正常にあると判断できない場合、ADSがMRSに移行して安全を優先する責任を果たしていることを示している。

研究目標3:
2. 研究成果:ドライバと車両挙動の相互作用の検証

- ドライバモデルに基づき、車両挙動とドライバの振る舞いとの相互作用を、動的シミュレーションを実施して解析した。
- 解析結果をもとに、ドライバモデルの振る舞い、および車両とドライバとのインタフェースを改善することができる。



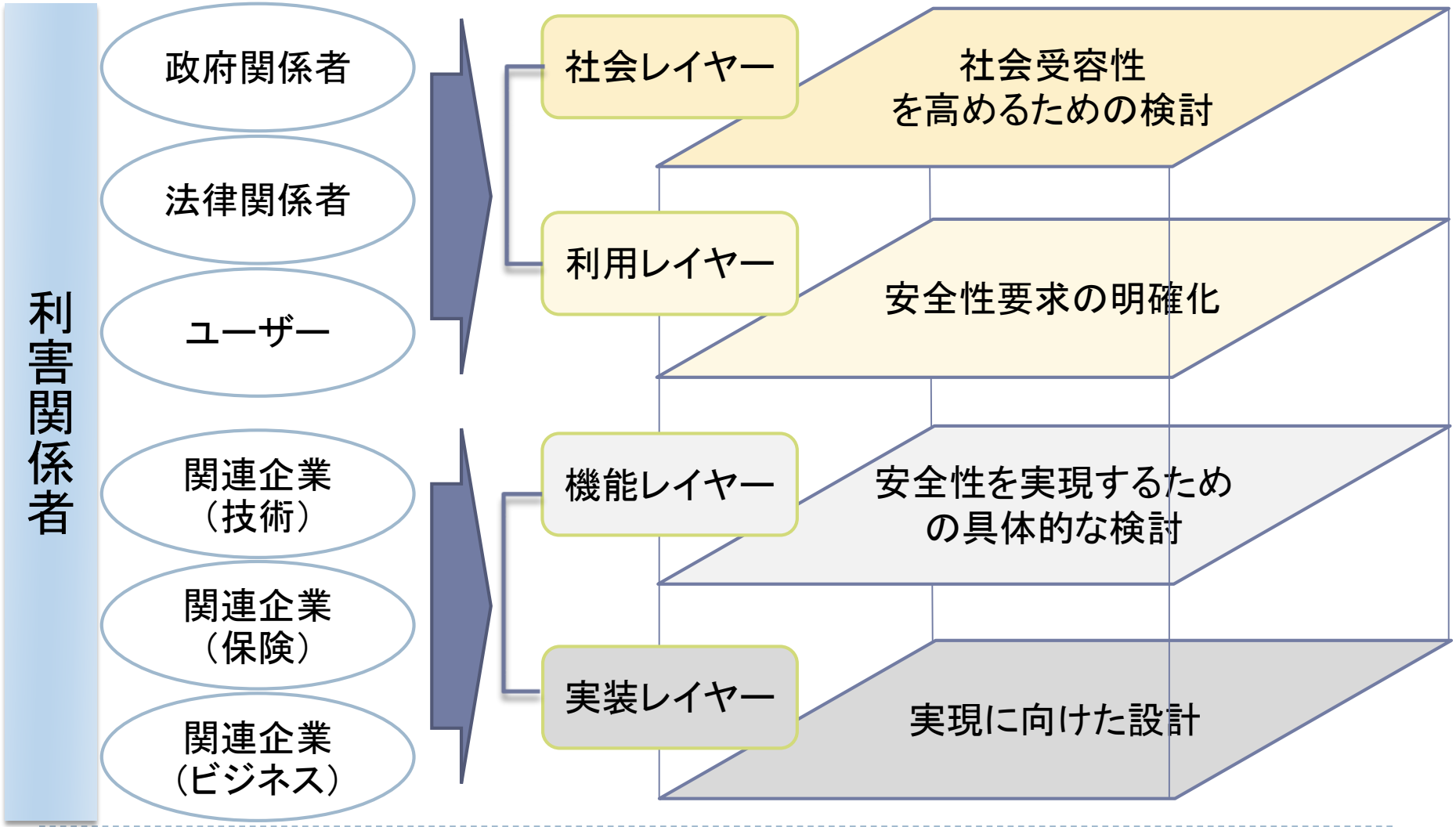
- 自動運転車が交差点を右折
- 横断歩道にいる歩行者を検知して停止

2014年度ソフトウェア工学分野の先導的研究支援事業

3. 成果の活用見込み(1)

- 自動運転車の普及が検討されているものの、それを取り巻く環境を含めたシステム(SoS)は、大規模・複雑であり、安全性に優れたシステム構築を行うためのアプローチは確立されていない。次世代自動運転車が安全に利用できるようにするための**SoSアーキテクチャを構築**することは関連企業に有効な情報となる。
- 今後、車車間通信システムや車間距離制御システムなど自動運転車に必要なシステムを統合する際にも、本アーキテクチャをもとに安全性やセキュリティに主眼を置きながらシステム統合の方法を議論することができると期待される。各関連企業は、このアーキテクチャに基づいて、次世代自動運転車用のソフトウェア開発・設計、周辺情報システムなどの開発・設計を行うことが可能となる。

3. 成果の活用見込み(2)


利害関係者
政府関係者
法律関係者
ユーザー
関連企業（技術）
関連企業（保険）
関連企業（ビジネス）
社会レイヤー
利用レイヤー
機能レイヤー
実装レイヤー
社会受容性を高めるための検討
安全性要求の明確化
安全性を実現するための具体的な検討
実現に向けた設計

4. 研究成果の発表、投稿、引用等

1. 記事
   - ① 西村秀和，自動車の安全を考える，小特集：自動車の安全と自動運転，安全工学会，Vol.54, No.3, pp.153-157, (2015)
2. 学会発表
   - ① 木下聡子, ユンソンギル, et al, 自動車の自動運転システムに対する安全性要求のアシュアランスケースによる分析, 日本機械学会2015年度年次大会, 2015年 9月
   - ② 木下聡子, ユンソンギル, et al, Analysis of a Driver and Automated Driving System Interaction Using a Communicating Sequential Process, First IEEE International Symposium on Systems Engineering, 2015年9月
   - ③ ユンソンギル, 北村憲康, et al, Design of an Automated Driving System to Ensure Delegation of Driving Authority with Ego Vehicle Driver, 9th Asia-Pacific Conference on Systems Engineering, 2015年10月
   - ④ 木下聡子, ユンソンギル, et al, Driver Functions Definition for System of Systems for Automated Vehicles, 9th Asia-Pacific Conference on Systems Engineering, 2015年10月（Best Paper Award受賞）

5. まとめ

- 自動運転車を取り巻くSoSに対して記述したシステムモデルに基づきモデル検査および安全分析を行い、そして実験データに基づきドライバモデルを明確にすることにより、SoSアーキテクチャを構築し、各構成システムに対する安全性要求を明確にした。また、SoSアーキテクチャを設計、更新するための方法を提案した。
- 今後は、自動運転車を取り巻くSoSのアーキテクチャに基づき、自動運転車を実現するための検討を自動運転関連企業などの利害関係者に広めていく。