

適切な「ぼかし」で、ソフトウェア検証の複雑さに挑む ソフトウェアの要件の「ぼかし方」 に関する研究

小林 努(JST/NII)、猿渡 真之介(東大)、森田 大智(東大)、Paulius Stankaitis(英Newcastle大)、
Guillaume Dupont(仏ENSEEIH)、Yamine Aït Ameur (仏ENSEEIH)、石川 冬樹(NII)、蓮尾 一郎(NII)

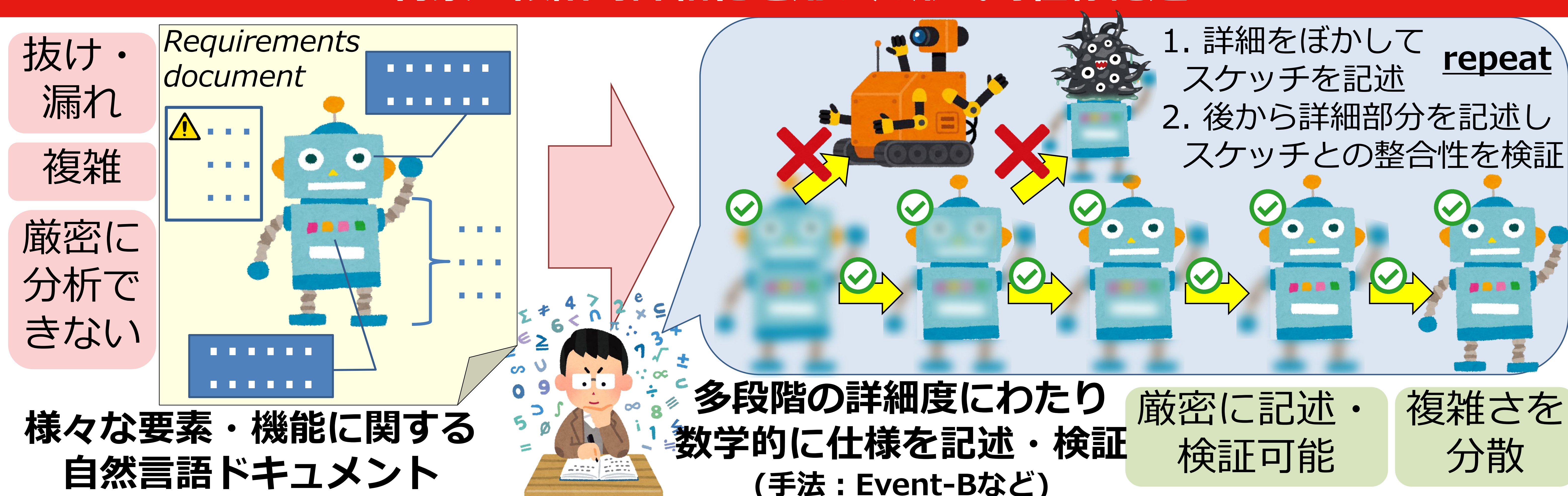
どんな研究？

信頼できるシステムを作るために、正しさを保ったままシステムを適切に何段階か「ぼかし」ながら数学的な検証を行う手法が注目されています。私たちは、ぼかし方の分析・変更を通じて厳密で柔軟な開発を可能にする他、「ぼかし」の仕組みを拡張し適用範囲を広げる研究を行っています。

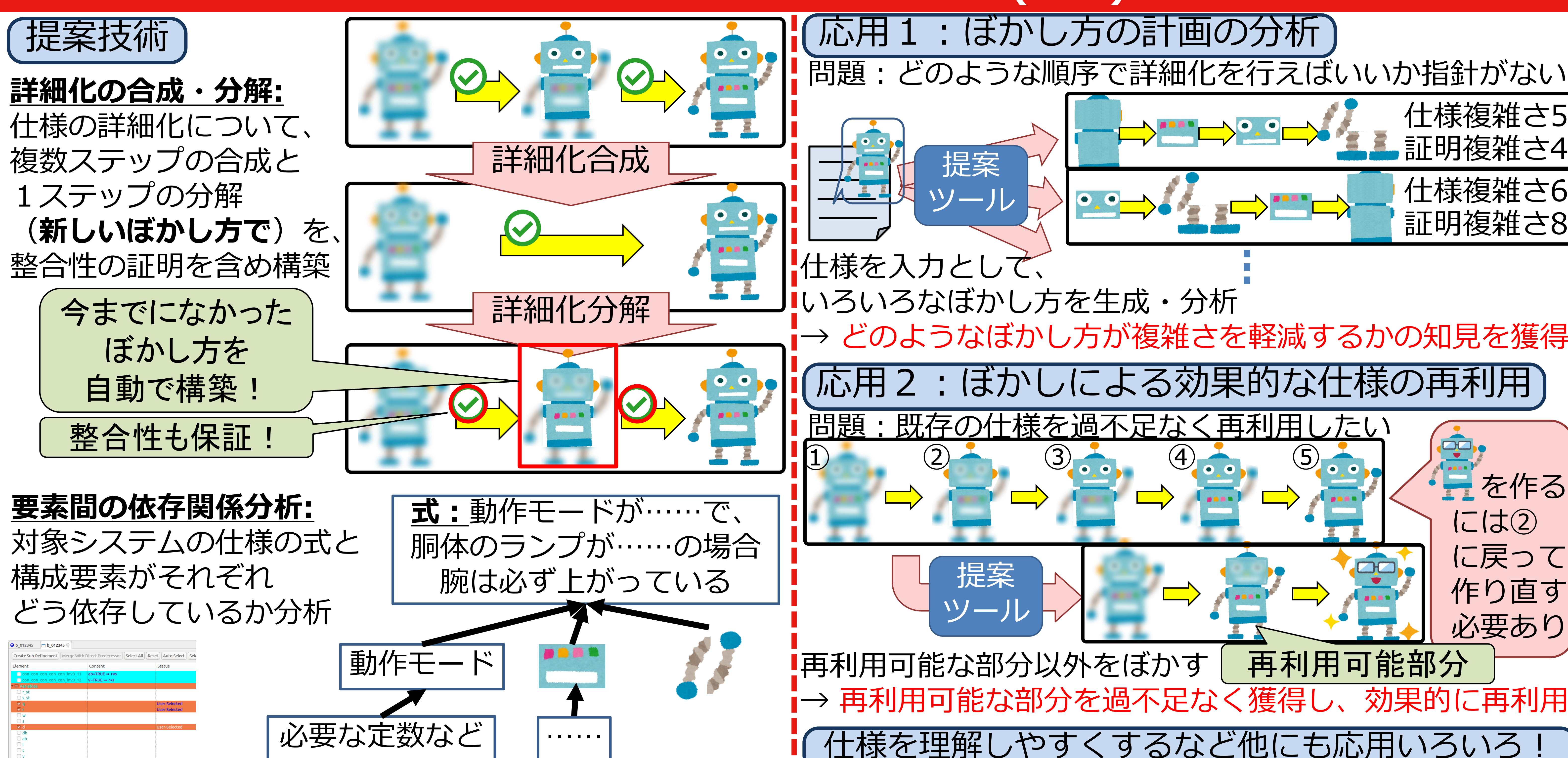
何がわかる？

見通しの良いソフトウェアシステムの検証方法の柔軟性と適用範囲を広げることで、私たちの身の周りの至るところにあるソフトウェアをより安全にすることができます。

背景：段階的詳細化を用いた形式的仕様記述



整合性を保つ詳細化の自動変更(小林)



Kobayashi & Ishikawa, Analysis on Strategies of Superposition Refinement of Event-B Specifications, ICFEM'18 (Best paper).
Kobayashi, Ishikawa, et al., Consistency-preserving refactoring of refinement structures in Event-B models, Formal Aspects Comput.

小林, 科学技術振興機構 ACT-I 「整合性を保持する形式仕様の自動抽象化システム「ソフトウェア顕微鏡」の開発」

小林, 科研費 研究活動スタート支援 「段階的詳細化の柔軟な変更および設計指針の確立」

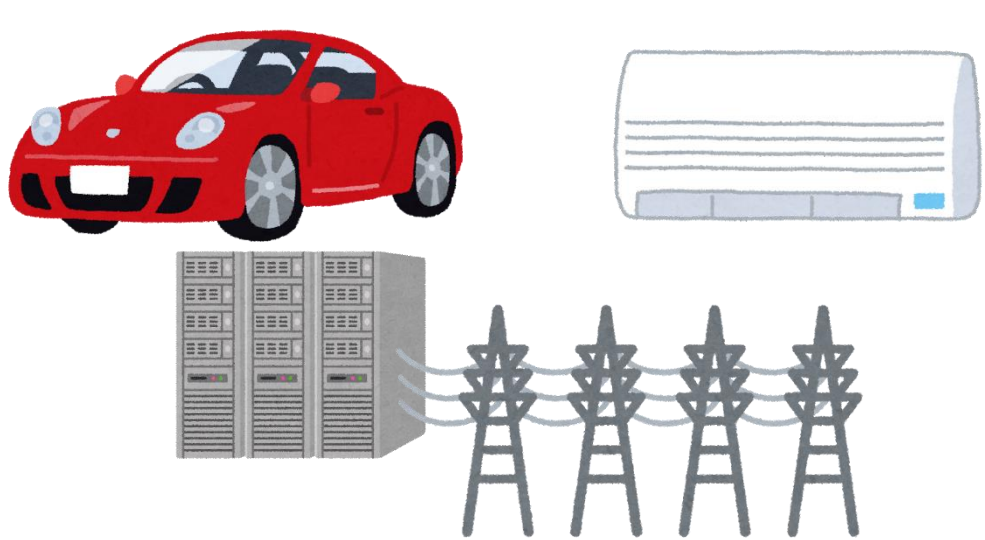
石川, 科研費 基盤研究 (B) 「保証付き多段階システムモデルの柔軟・継続的な洗練・進化」

ツール実装「Slice'n'Merge」
<http://research.nii.ac.jp/slicenmerge/>

段階的詳細化によるハイブリッドシステムのモデリングと検証(森田、Dupont)

背景：ハイブリッドシステム(HS)

センサネットワークなどで実世界をモニタリングしながら、機械をコンピューター制御することで、**実世界をコントロールするシステム**



動機と難しさ

私たちの身の回りの物理世界で動くソフトウェアシステムを安全にしたい……
→ HSも段階的に形式モデリング・検証したい！

しかしこんな問題が……

既存の段階的詳細化ツールはHSに必要な微分方程式などをサポートしていない
微分方程式を含む仕様の詳細化の検証はとても複雑で、現実的には困難

(Dupont) HSの仕様記述に必要な数学的概念ライブラリや記述パターンの整備

Event-Bの理論拡張機能を利用し、証明付ライブラリ構築

WHERE

grd1: $eq \in \text{DE}(S)$
grd2: $\text{Solvable}([t, +\infty[$

THEN

act1:

$v, p :$

$p' \in \mathbb{R}^+ \rightarrow \mathbb{R} \wedge v' \in \mathbb{R}^+ \rightarrow \mathbb{R} \wedge$

$[0, t[\triangleleft [v' p']^T = [0, t[\triangleleft [v p]^T \wedge$

$\text{solutionOf}([t, +\infty[, [t, +\infty[\triangleleft [v' p']^T, eq)$

$\forall t \in \mathbb{R}^+, \begin{cases} \dot{v}(t) = a \\ \dot{p}(t) = v(t) \end{cases}$
(仕様化したい数式)

HSの重要なパターンを仕様で扱いやすく！

コマンドによる変化

センシング

環境の振る舞い

コントローラ

操作

環境

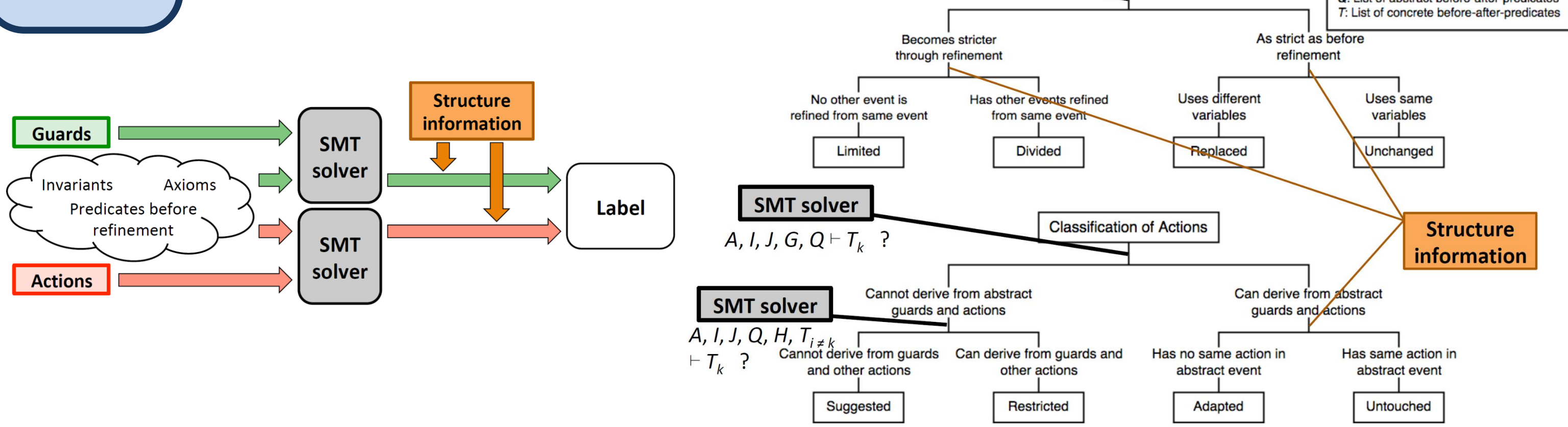
Dupont, Ait Ameur, et al., Proof-Based Approach to Hybrid Systems Development: Dynamic Logic and Event-B, ABZ'18.

仕様変更・再利用の可能性の可視化(猿渡)

動機

段階的詳細化で作られた仕様の抽象版と詳細版の関係は、(一般には)明示的ではない
……抽象版と具体版を両方作った後、両者が整合性を持っているか確認するため
→仕様を変更・再利用する時、どこに手を加えても整合性に問題がないか分かりづらい！

提案

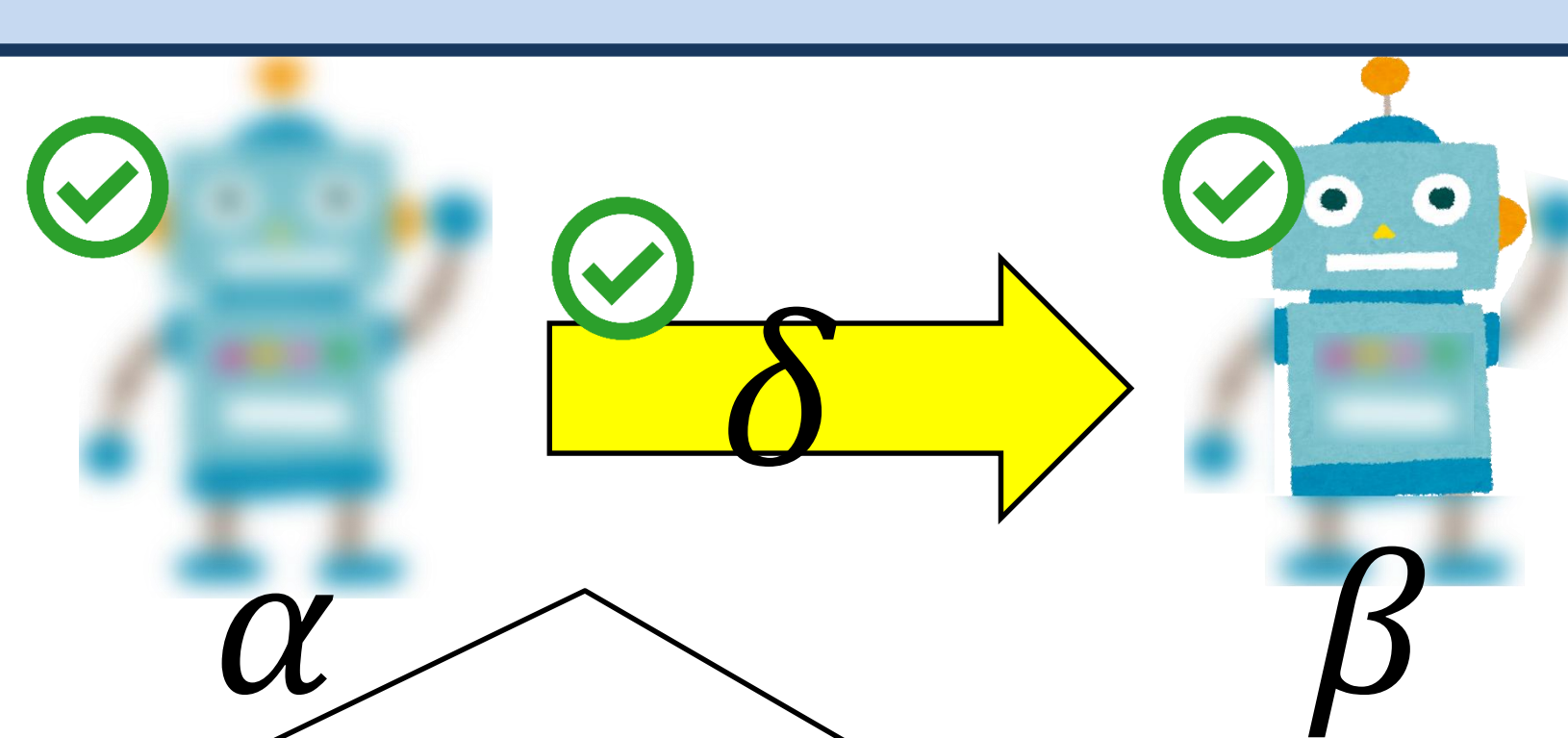


詳細化の特徴をソルバーツールを用いて解析、モデルの各部分にラベルを付けていく！
「ぼかし」の箇所や「ぼかし」具合を把握することでどのようにシステムが作られたかを理解

システムの整合性を崩さずに仕様を追加・変更する際のヒントに！
仕様の変更・再利用を促進し、より多くのソフトウェアを安全に！

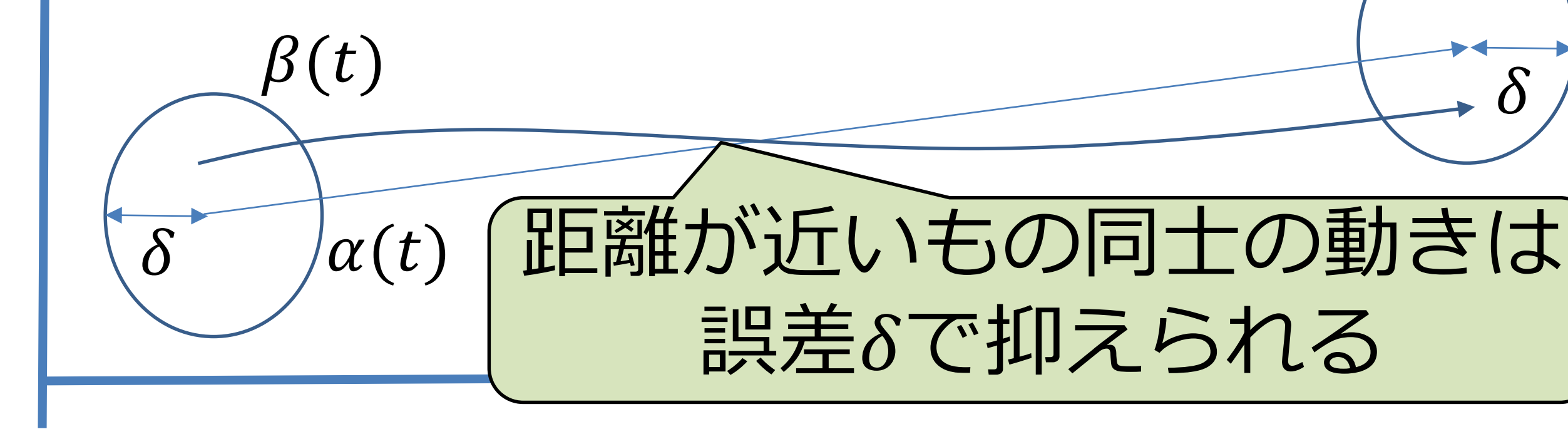
Saruwatari, Ishikawa, Kobayashi, et al., Change Impact Analysis for Refinement-based Formal Specification, IEICE Trans. Inf. & Syst. (in press)

(森田) 誤差を許容した詳細化機構の提案とそのための仕様記述手法の理論的拡張



(@蓮尾ERATO) ポスター[B-02]

制御理論の考え方を応用し、**誤差 δ を担保した詳細化**を採用

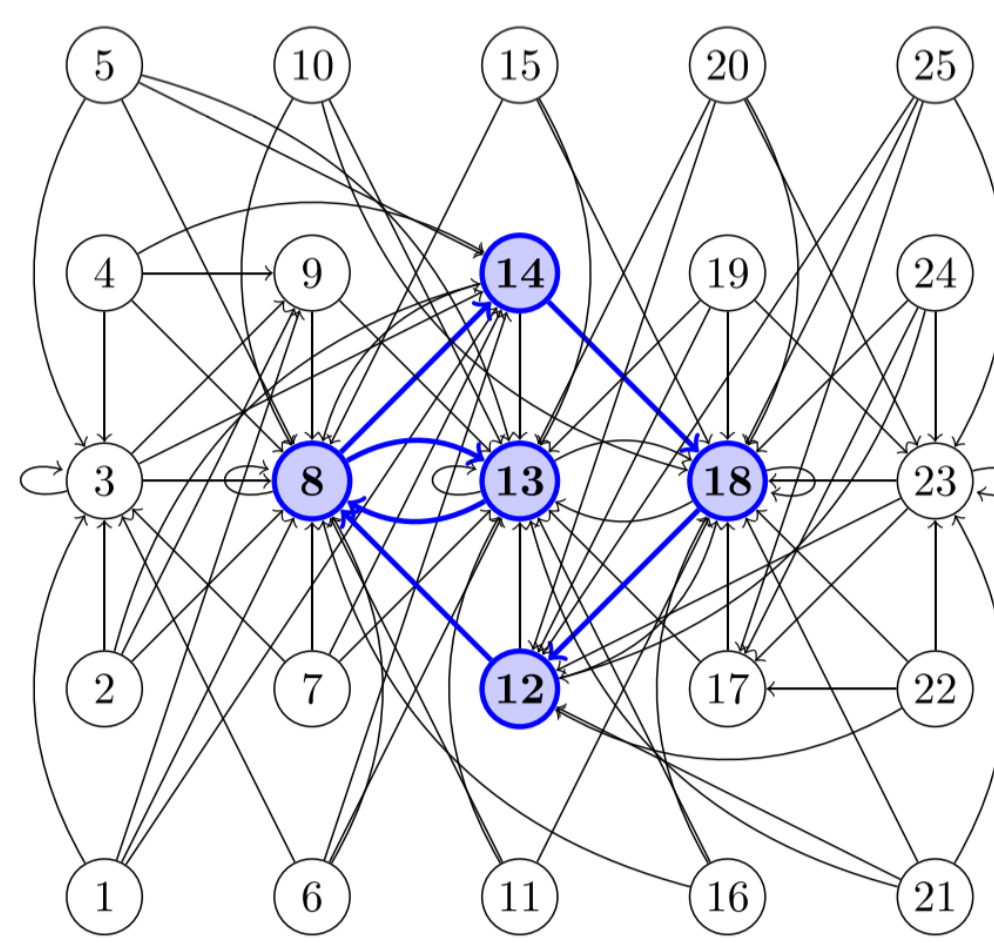


距離が近いもの同士の動きは誤差 δ で抑えられる

soundness theorem

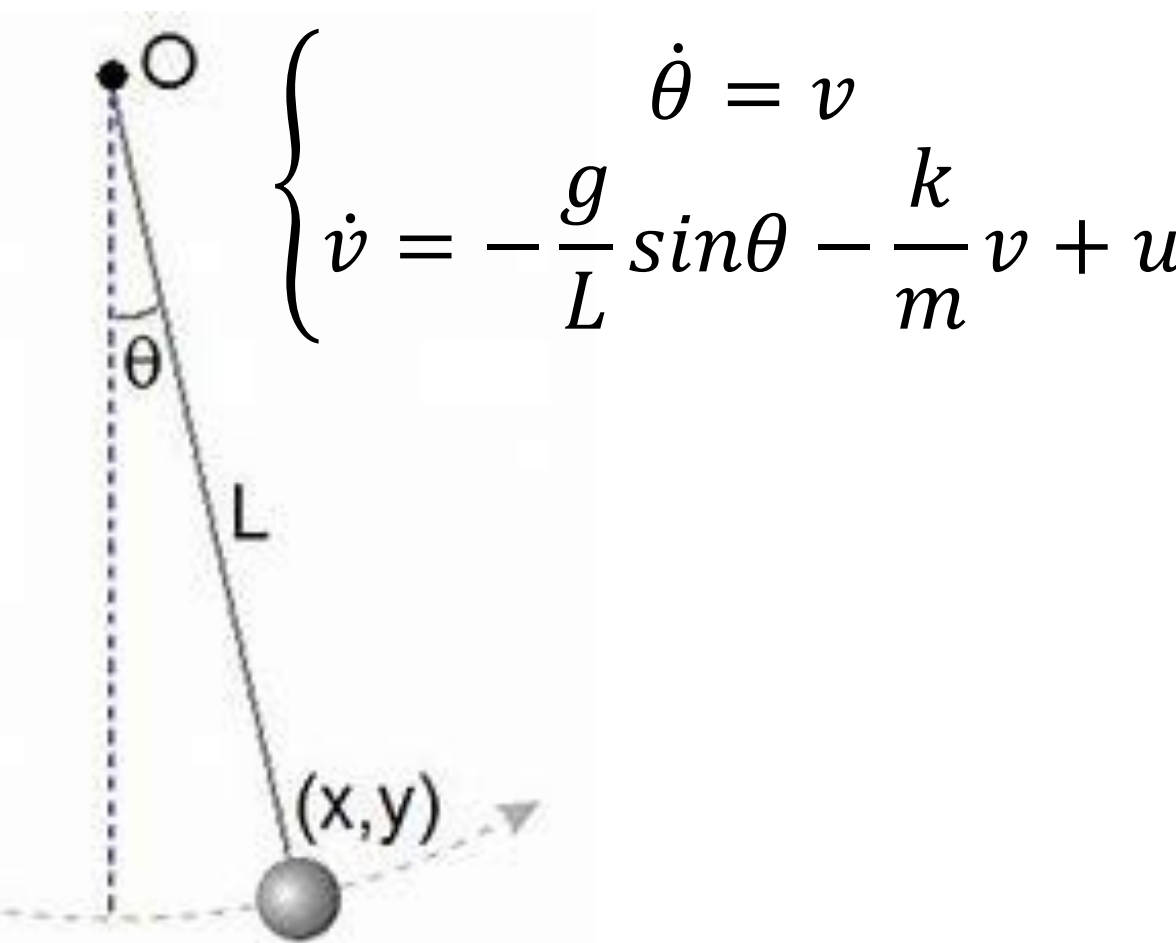
性質 ϕ を検証

例) 振り子の離散化



δ

性質 ϕ が誤差 δ で成立！

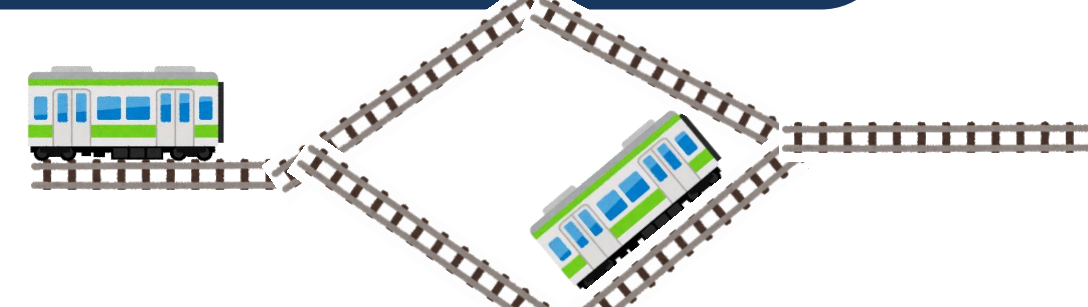


誤差を許容することにより、厳密さを保ちつつ現実的な検証が可能に！

先進的システムの検証(小林、Stankaitis)

(Stankaitis) 鉄道の分散運行プロトコル

多くの電車が同じ路線を共有する路線を安全にしたい！



- 各電車が通信して路線の各部分を重複しないように押さえる分散プロトコルを構築
- 段階的詳細化で仕様記述・検証
(路線の集合、路線、メッセージ、特殊リクエスト…を順に導入)
- 確率的挙動周りは確率モデル検査器によるシミュレーションで正しさを検証(停止性など)
- 確率的挙動も含め、鉄道の安全運行を保証！

Stankaitis, Ait Ameur, Kobayashi, Ishikawa, et al., A Refinement based Method for Developing Distributed Protocols, HASE'19.

(小林) 自動運転の安全アーキテクチャ(進行中)

自動運転ソフトを安全にしたい！

(@蓮尾ERATO) ポスター[B-02]

- 仕組みとしての安全性に加えて、各コンポーネントや動作も検証
- 一般的な枠組みを作りつつ個別の車の問題にも適用を目指す



機械学習工学(ポスタA-06)
機械学習ソフトウェアの信頼性をどう保証するか？

信頼性工学
安全にスイッチするには？
安全系に必要な性質は？

圏論
Event-Bなどの手法を一般化・拡張できないか？

通常系
性能◎ 信頼性○

安全系
性能△ 信頼性◎

テスト
形式仕様記述の困難な対象にテストをどう適用する？

ハイブリッドシステム
物理的挙動を微分方程式でモデル化・検証するには？

自動運転
安全アーキテクチャに必要な性質は？
どんな想定が必要？

多様な領域の方と協力し、鋭意研究開発中！

連絡先：小林 努／科学技術振興機構 ACT-I専任研究者

Email: t-kobayashi@nii.ac.jp

(兼：国立情報学研究所 アーキテクチャ
科学研究系 蓮尾研究室 特任研究員)

Web:

