

産学連携事例

～自動車が危険に至るシナリオを時相論理で形式化～

NIIオープンハウス2024

- 上田 直樹
(Ueda Naoki)



- 三菱電機株式会社 情報技術総合研究所
情報ネットワークシステム技術部
トラステッドシステム技術グループ
- 組み込みシステム（主に自動車）向け
のモニタリング技術の開発に従事



三菱電機株式会社 情報技術総合研究所（神奈川県鎌倉市）

https://www.mitsubishielectric.co.jp/corporate/randd/laboratory/information_technology/index.html

共同研究の経緯

- 背景：高信頼システムでは、**システムが正常に動作し続けることが求められている**
ソフトウェアのバグはシステムの不具合発生の一因である
ソフトウェアのバグ発生の一因に**仕様に対する人の解釈の違い**が挙げられる
- 課題：① システムの仕様の形式言語で記述することで**人の解釈の違い（＝バグ発生要因）をなくす**
② 専門知識が必要となる形式言語の記述を支援し、**形式言語を容易に扱えるようにする**
- モチベーション：実製品に関する知識を持つ弊社が形式言語の専門家のNII蓮尾教授と協働し**技術開発を加速**



(i) 自動車



(ii) 人工衛星

【自然言語による仕様（自動車）】

自車と前方車との車間距離が常に一定以上
である（前方車との衝突の危険）



Aさん

現在の車速（km/h）
から15引いた値を車
間距離と定義



Bさん

前方車が通過した地点
から自車が通過するま
でに2秒かかる距離を
車間距離と定義

解釈の
違い

数式で定義



【形式化された仕様】

$$G\{ d \geq (v - 15) \}$$

車間距離 d は常に現在の
車速から15引いた値以上
である

厳密に定義できるようにはなったが、
意図通りに記述するためには専門知識が必要

共同研究での取り組み内容と成果

・ 取り組み内容

- ① ISO 34502*の交通外乱シナリオを題材に仕様を形式言語で記述する方式を検討
- ② 形式言語の記述をサポートするツールを開発し、記述が容易になったかどうかを評価

・ 成果

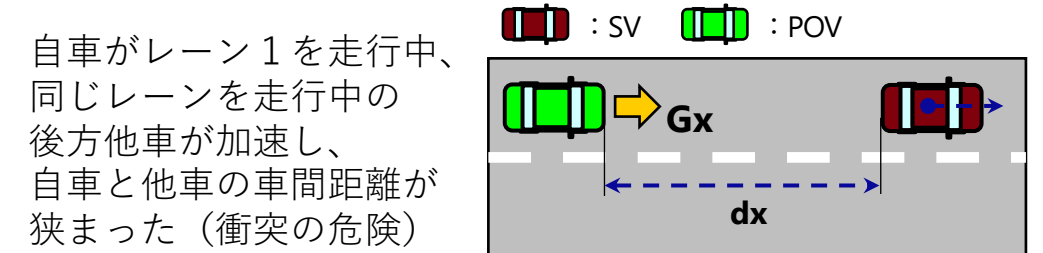
- ① 時間で変化する実数値の扱いに適した形式言語（Signal Temporal Logic）で交通外乱シナリオを数学的に表現でき、**仕様の曖昧さ排除を実現**
- ② 仕様の記述、グラフやアニメーションを用いた記述の検証、仕様の修正を1つのツール上で行うことで**形式化された仕様の理解支援に寄与**

タイトル：Temporal Logic Formalisation of ISO 34502 Critical Scenarios: Modular Construction with the RSS Safety Distance

著者：Jesse Reimann, Nico Mansion, James Haydon, Benjamin Bray, Agnishom Chattopadhyay, Sota Sato, Masaki Waga, Étienne André, Ichiro Hasuo, Naoki Ueda, Yosuke Yokoyama

発表会議：The 39th ACM/SIGAPP Symposium On Applied Computing

交通外乱シナリオ（ISO 34502*）の例

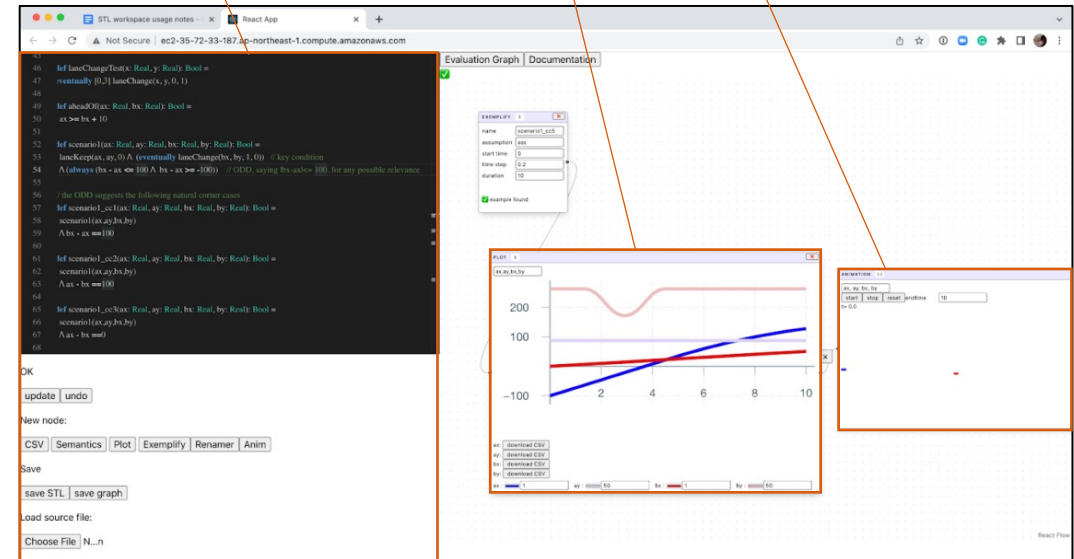


↓ ツールを用いて形式化

記述編集画面

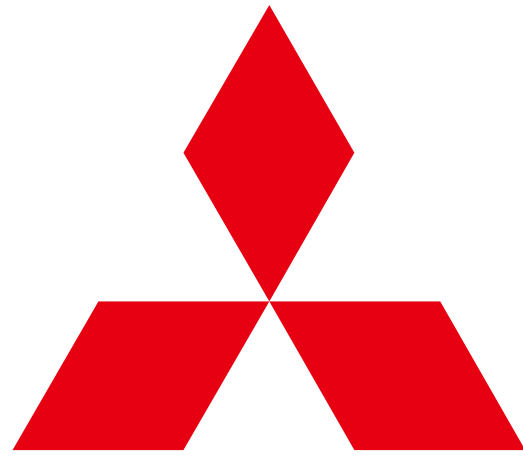
結果確認画面（グラフ）

結果確認画面（アニメ）



これまでの共同研究を振り返って

- 共同研究を行ってよかったこと
 - 弊社「形式言語を製品に応用したいが更なる理論的な知見が必要」というニーズと NII 蓮尾教授「豊富な専門知識を産業界に還元したい」という思いがうまく調和した結果、お互いにとって価値のある成果を得ることができた
- 今後
 - 形式言語の専門家ではなくとも形式言語が扱えるように記述方式の検討/改善に取り組む
 - 本成果の適用先拡大に向け、自動車以外のシステムへの適用を検討し、本技術のニーズを探っていく



**MITSUBISHI
ELECTRIC**

Changes for the Better