



2020 年（令和 2 年）1 月 24 日

自動車システム設計の安全性を自動分析する手法を開発

～多様な設計・動作環境のデータから危険要因を抽出し知識として体系化～

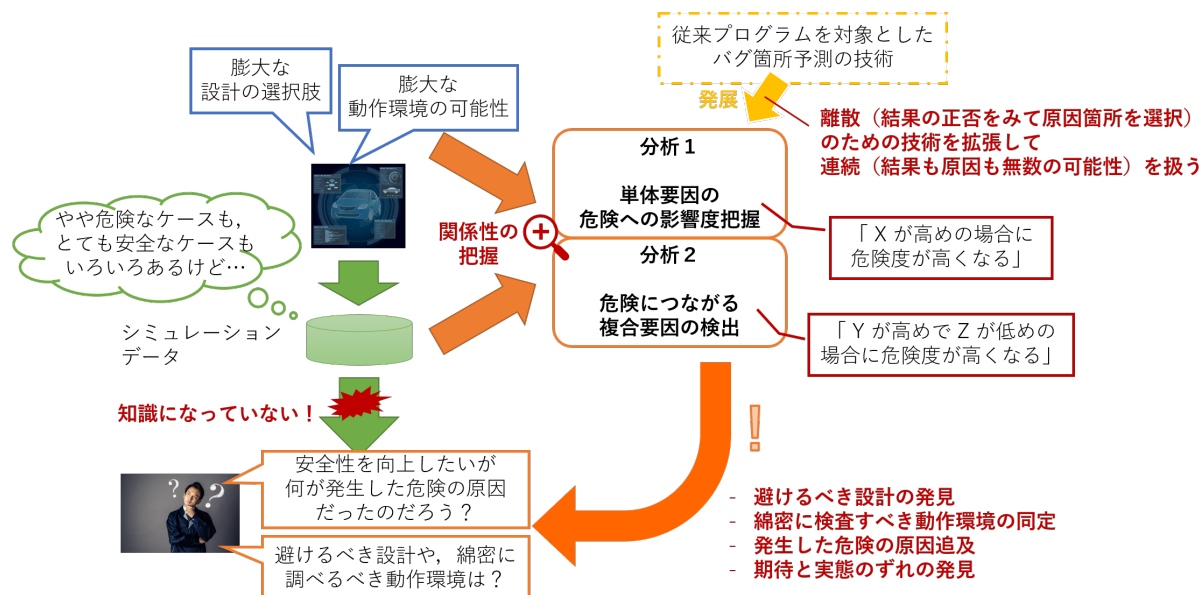
複雑ソフトウェアシステム工学のフラッグシップ国際会議 ICECCS 2019 で最優秀論文賞受賞

大学共同利用機関法人 情報・システム研究機構 国立情報学研究所（NII、所長：喜連川 優、東京都千代田区）のアーキテクチャ科学研究系准教授 石川 冬樹（いしかわ・ふゆき）の研究チームは、自動車システム設計の安全性を自動分析する手法を開発しました。

自動運転の開発が進む中、自動車システムの安全性分析においては、膨大な設計の選択肢、そして膨大な動作環境の可能性がどのように安全性に影響するかの評価が必要不可欠です。しかし、動作に大きな影響を与える 2 種類のパラメーター（設計パラメーター：馬力、ブレーキ力など、環境パラメーター：乾燥した路面や滑りやすい路面など）の組み合わせが膨大であるため、実際に大量のシミュレーションをしたとしても、得られたデータから知識を抽出して活用することが困難な状況となっています。

そこで、研究チームは、設計および環境パラメーターと全体的なシステムの安全性との関係を自動分析する手法を開発しました。それぞれのパラメーターが単独でどれだけ安全性に影響しているかを分析する手法と、パラメーターの相互作用がどう安全性に影響しているかを分析する手法の二段階から成り立っています。実際にシミュレーションデータに適用したところ、潜在的な危険に関連する重要なパラメーターと、パラメーターの相互作用パターンが特定できるとの結果が得られました。

本研究成果は、複雑ソフトウェアシステムに対する工学についてのフラッグシップ国際会議 ICECCS 2019^(*)にて最優秀論文賞を受賞しました。



＜図＞ 開発した「自動車システム設計の安全性を自動分析する手法」の全体概念図

【背景】

自動運転の開発が進む中、その安全性は非常に重要です。高度な運転機能の安全性を検証するためには、膨大な設計の選択肢、そして膨大な動作環境の可能性を考慮することが必要です。そのため設計および動作環境のパラメーターを変えながら、たくさんのシミュレーションを実行することがなされています。しかし、そこで蓄積された膨大なデータはそのままでは知識に仕立て上げられておらず活用できないため、体系化してシステムの安全性への洞察を深めたり、システムの設計を修正したり、今後のシステムの設計へ活用したりすることにはつながっていませんでした。

【研究手法・成果】

本研究では、大量のシミュレーションデータの解釈・整理・体系化を行い、システム安全性に関する知識を抽出する手法を考案しました。この手法では、二段階のアプローチによりシミュレーション結果を分析します。第一段階で、設計や動作環境に関する各パラメーター（単一要因）がどれだけ安全性に影響しているか（危険につながっているか）を分析します。そして、第二段階で、それらの組合せ（複合要因）が安全性に影響している場合があるかを分析します。

第一段階の分析では、従来のソフトウェアプログラムにおいてバグの存在箇所を予測するバグ箇所予測の技術にヒントを得て、新たな手法を提案しています。自動車システムにおいては、バグであることがはっきりわかる（離散的な）ソフトウェアプログラムとは異なり、結果の安全性も、原因となるパラメーター値も、連続的で無数の可能性があるものとなります。それらを「大まかにとらえる」ことが今回開発した手法の肝になっています。

第二段階の分析においても、無数の組合せの可能性から、安全性に影響しているパラメーター値の組合せを導きます。ここでもやはり、連続的で無数の可能性があるパラメーター値を「大まかにとらえ」、危険度とパラメーター値の組み合わせのそれぞれによる２段階のクラスタリング^(*)2)を行い、膨大な組み合わせの中から安全性への影響の観点から注意を払うべきものを抜き出します。

この二段階の分析結果を合わせることで、「X が高めで Y が低めの場合に危険度が高い（X が高めなだけではそうとは限らない）」といった知識を全自動で抽出し、開発者に提示することができるようになりました。これにより開発者は、避けるべき設計の選択肢や注意深く検査すべき動作環境を把握したり、危険なケースの原因追及をしたりできるようになります。また、分析結果を開発者の持つ知識や期待と照らし合わせることで、システムに対する理解不足や誤解、システムの意図通りでない動作に気がつくきっかけともなります。

【今後の展望】

本研究で得られた分析手法は、シミュレーションやテストのデータがあれば、自動車システムにおける安全性に限らずに活用できるものとなっています。今後は、運転経路の決定など自動運転の

他の機能や、ゲームのように膨大な可能性を扱う他のソフトウェアシステムなど、産業界の様々な事例に対する適用を行い、技術をさらに発展させて企業における問題解決に取り組んでいきたいと考えています。

石川 冬樹准教授からのコメント：

「自動運転に代表されるように、自律・スマートシステムのためのソフトウェア開発では、実世界における膨大な可能性、それに対応するための設計に関する膨大な選択肢と向き合う必要があります。本研究はこの潮流に対する一つの解であり、シミュレーションやテストのデータという、すでに存在するであろうものに適用できる、採り入れやすいものであると考えています。今回、企業からいただいた題材に基づいた研究が、学術的にも高く評価される成果につながり嬉しく思っています。今後も産業界の皆様との対話を通して、問題解決に寄与するような研究開発を行っていききたいと考えています。」

【研究プロジェクトについて】

本研究は科学技術振興機構（JST）戦略的創造研究推進事業（ERATO）の支援（JPMJER1603）のもとで ERATO 蓮尾メタ数理システムデザインプロジェクト^(*3)にて実施しました。また、マツダ株式会社の提供による物理制御モデルを題材として実施しました^(*4)。

【論文タイトルと著者】

タイトル： Assessing the Relation Between Hazards and Variability in Automotive Systems

著 者： Xiaoyi Zhang, Paolo Arcaini, Fuyuki Ishikawa

発表会議： 24th International Conference on Engineering of Complex Computer Systems (ICECCS 2019)

発 表 日： 2019 年 11 月 13 日（水）

※ICECCS 2019 において優秀論文賞を受賞しました（11 月 12 日授与発表）

〈メディアの皆様からのお問い合わせ先〉

大学共同利用機関法人 情報・システム研究機構 国立情報学研究所

総務部企画課 広報チーム

TEL:03-4212-2164 E-mail : media@nii.ac.jp

(*1) ICECCS 2019 : The 24th International Conference on Engineering of Complex Computer Systems。CORE と呼ばれる計算機科学系の国際会議ランキングにて A ランク。

(*2) クラスタリング:類似性の尺度により、標本パターンを似たものどうしで集めてグループに分けること。

(*3) ERATO 蓮尾メタ数理システムデザインプロジェクト：国立研究開発法人 科学技術振興機構（JST）の「戦略的創造研究推進事業 ERATO」に採択されている研究プロジェクトで、Society 5.0 の大きな柱と

なる CPS の品質保証手法の学術的研究を推進している。特に、CPS の典型例の一つとして注目される自動運転システムを重点応用対象として、その信頼性保証を支えるモデリング手法・形式検証手法・テスト手法、さらにこれらを含む実用的な V&V 技術の研究開発に取り組んでいる。このような大きなチャレンジでは、ソフトウェア・制御・AI といった多様な学術分野の協働が必要となるため、学術分野融合の基礎となる数理的（メタ）理論も重視して研究を推進する。略称は ERATO MMSSD。プロジェクト詳細は <http://www.jst.go.jp/erato/hasuo/ja/> 参照。

(*4) 本研究で考案したモデルは研究評価用のプロトタイプであり、特に、その品質は最終的な製品の品質には何ら関係ありません。