2021 年（令和 3 年）5 月 26 日

計測誤差があるセンサーを使っても安全に動くように制御ソフトウェアを自動で変換する手法を開発

～「誤差はないものとする」理想上の設計で現実を安全に～

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特任研究員 小林 努（こばやし・つとむ）、同研究系准教授 蓮尾 一郎（はすお・いちろう）らの研究チームは、科学技術振興機構（ＪＳＴ、理事長：濵口 道成、東京都千代田区）の戦略的創造研究推進事業 ERATO蓮尾メタ数理システムデザインプロジェクト(*1)（ERATO MMSD、研究総括：NII アーキテクチャ科学研究系准教授・蓮尾 一郎）のもと、制御システムのセンサーに計測誤差があっても、安全に動くように制御ソフトウェアのモデルを自動で変換する手法を開発しました。この手法を使うと、ソフトウェアのモデルを自動変換するとともに、出力された制御ソフトウェアが耐えられる誤差の限界を示す数式を得ることができます。本手法は、自動運転をはじめとした外部環境とやり取りする様々な制御システムに対して活用でき、多様な利用環境や計測手段に対応するシステムへの応用が期待されます。

本研究成果は、第 13 回 NASA フォーマルメソッド・シンポジウムで 2021 年 5 月 26 日（水）にオンライン発表されます。

【背景】

近年、活用が期待され、役割の重要性が増しているドローンや自動運転などの制御システムは、適切に動作し、事故を起さないよう高い安全性が求められます。高い安全性を実現するには、数学的な手法を使って、システムをモデル化し、安全性を証明する手法が有効です。

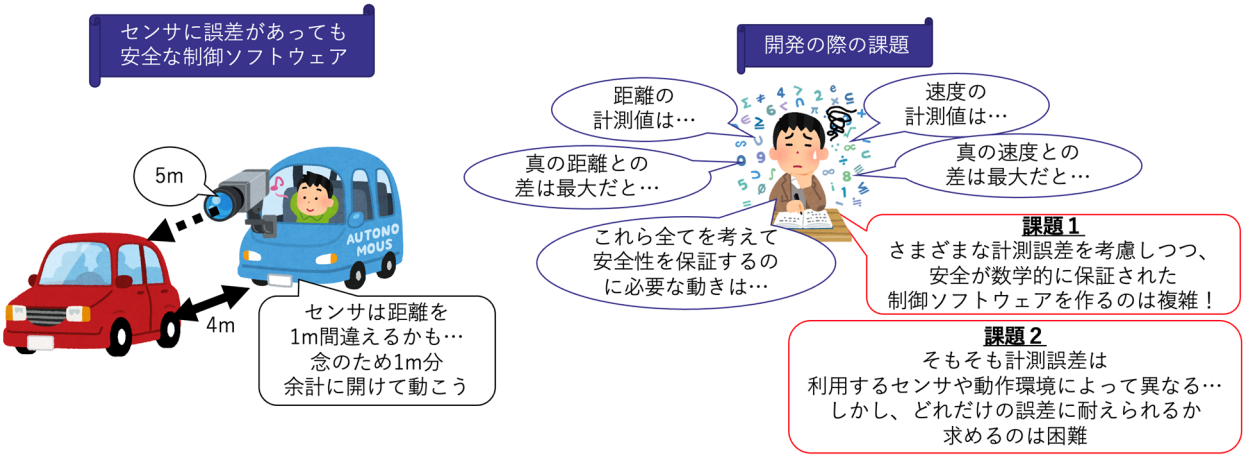
制御システムに含まれる制御ソフトウェアはセンサーで計測した制御対象の状態をもとに適切な動作を決定します。しかし、現実には真の値と異なる値が計測される（計測誤差がある）ため、計測値が真の値と等しい前提で決定された制御ソフトウェアの動作は安全性を損ないかねません。そのため、このような制御ソフトウェアを開発する際には、計測誤差を考慮して設計する必要があります。例えば、他の車の位置を計測する際に最大 1m 間違える可能性がある場合には、基本的に 1m の安全マージンを持った動作をする制御ソフトウェアとする必要があります（図 1 左）。

しかし、センサーの計測誤差を考慮した、真に安全な制御ソフトウェアの設計はとても複雑になります。なぜなら、計測する対象それぞれについて真の値と計測値の両方を扱ったうえで、制御ソフトウェアのあらゆる動作において安全性が保証されると数学的に証明するには複雑さが伴うためです（図 1 右：課題 1）。さらに、制御システムの計測にどのような誤差があり得るかを確実に知ることは、設計の段階（開発の早い段階）では困難です。例えば、計測誤差は制御システムが動作する環境（霧が出るか否かなど）によって異なります。そのため、はじめから計測誤差を具体的に見込んで制御ソフトウェア

国立研究開発法人 科学技術振興機構（JST）
広報課
〒102-8666 東京都千代田区四番町 5 番地 3
TEL：03-5214-8404 FAX：03-5214-8432
E-Mail：jstkoho@jst.go.jp

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
〒101-8430 東京都千代田区一ツ橋 2-1-2
直通：03-4212-2164 FAX：03-4212-2150
E-Mail：media@nii.ac.jp

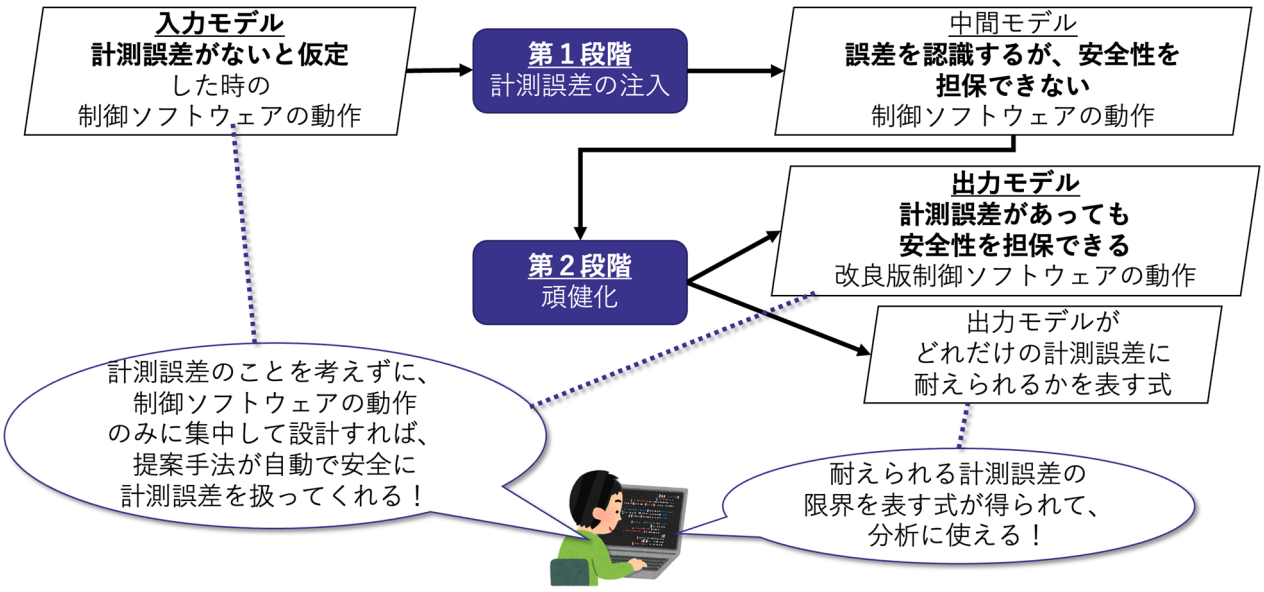
の設計に組み込むのではなく計測誤差がないことを前提に作り、その制御ソフトウェアが「どの程度の誤差に耐えられるか」を計算できると、制御システム全体を柔軟に設計できます。そうすれば、実際にシステムに搭載するセンサーを後から検討できるなどのメリットがあるからです。ところが、この「どの程度の誤差に耐えられるか」を表す数式を獲得することは難しい問題でした（図１右：課題２）。



<図１>安全な制御ソフトウェアの例（左）と計測誤差を含む制御システムの課題（右）

【研究手法・成果】

本研究では、与えられた制御ソフトウェアがセンサーの計測誤差を考慮せずに設計されたものであっても、計測誤差を考慮して安全に動作する制御ソフトウェアに自動で変換する手法を開発しました（図2）。



<図２>開発した手法の全体像。入力モデルを２段階で変換し、出力モデルとそのモデルが耐えられる誤差の限界を示す数式を得ることができる。

この手法では、２段階のアプローチで変換を行います。第１段階（計測誤差の注入）で、入力として与えられた制御ソフトウェアのモデルを、「誤差の存在を認識し、誤差のある計測値に基づいて動作す

るが、元の制御ソフトウェアと同じ動作をするため安全性を担保できない制御ソフトウェア」のモデルに変換します。そして、第２段階（頑健化）で、第１段階で得られた誤差を認識するが安全性が担保できない制御ソフトウェアのモデルを、「誤差のある計測値に基づいて元のソフトウェアとは違って適切に動作し、安全性を担保できる制御ソフトウェア」のモデルに変換します。そして、この変換後のモデルにより表される制御ソフトウェアが耐えられる誤差の限界も数式として出力します（図２）。

具体的には、第１段階（計測誤差の注入）では、制御ソフトウェアのモデルに、誤差を含んだ計測値に対応する変数を新しく導入します。また、入力として与えられた誤差を考慮しない制御ソフトウェアは、動作を決定する際に制御対象の真の値を参照できるかのような非現実的な記述がされているのに対し、第１段階の処理では、制御対象の値を、現実を反映した（真の値ではない）計測値として参照するような記述に変更します。第１段階の処理の後では、制御ソフトウェアは計測値をもとに動作しますが、動作は元の制御ソフトウェアと全く同じなため、一般に安全性は保証できません。例えば、自動運転車が、4m 前にいる別の車との距離を 5m と間違えて動いた結果追突する、といったことが起こります。

第２段階（頑健化）では、まず、制御ソフトウェアが想定している制御対象の状態に応じた場合分けを、誤差を考慮して行います。例えば、自車の前に車がいる状況で、ブレーキをかけるべき距離なのか、そのままの速度で走行して良い距離なのか、誤差があるせいで判断しかねる場合があります。そこで、本手法ではこのような場合を特別に扱うために、どのような「判断しかねる」状況があり得るかを算出します。さらに、動作を適切に変更することで、制御ソフトウェアが安全性を担保できるようにします。ここでは、計測値から算出した真の値のあらゆる可能性を考慮し、真の値がどのような値であっても安全であるような動作を算出します。

この手法で変換された制御ソフトウェアは、計測誤差があっても安全であるような動作が記述されたものです。しかし、計測誤差があまりにも大きい場合のように、そもそも安全な動作を取ることが理論上不可能な場合もあります。極端な例をあげると、他の車の位置を最大 100km 間違えるセンサーを使っている場合、ほとんどの環境で確実に安全な動作を取ることは不可能です。従って、「得られた制御ソフトウェアが耐えられる誤差の限界はどこか？」という問題が生じます。本手法では、この耐えられる誤差の限界も数式として出力します。これにより、制御システムに搭載可能なセンサーの選定や、制御ソフトウェアを他のコンポーネントと組み合わせた際の誤差に関する分析を体系的に行うことが容易になります。

これらの手法により、計測誤差がある場合でも安全に動作する制御システムの設計が体系的で、かつ容易になるほか、様々な計測誤差に対して制御ソフトウェア動作の柔軟な分析・対応が容易になり、様々な制御システムに囲まれた我々の社会の安全性向上に貢献できます。

【今後の展望】

ここまで自動運転を例に説明してきましたが、本手法は、外部環境とやり取りする様々な制御システムに対して活用できます。今後は、手法をさらに一般化していき、数値の誤差に限らず、物体認識システムが一定の確率で対象を正しくない物体として認識してしまう場合など、多様なシステムの安全性に寄与できるようにすることを目指します。

小林特任研究員からのコメント：

「多くのソフトウェアシステムは外部環境とやり取りを行うことで人の役に立つものであり、これらのシステムとその安全性が今後ますます重要になっていくことは間違いありません。本研究は、環境とのやり取りについて回る「理想と現実の差」を引き受け、開発者が誤差の細部に惑わされずに制御ソフトウェアの本質的な部分に集中できるようにすることで、現実での安全性を数学的に保証する開発を促進するものであり、有用であると共に今後の大きな発展も期待できるものであると考えています。今後も産業界での適用を見据え、数学的で厳密な手法をより現実に使いやすくする研究開発を行ってい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 戦略的創造研究推進事業 ERATO 蓮尾メタ数理システムデザインプロジェクト（JPMJER1603）の一環で行われました。

【論文タイトルと著者】

タイトル：Robustifying Controller Specifications of Cyber-Physical Systems Against Perceptual Uncertainty

著　　者：Tsutomu Kobayashi, Rick Salay, Ichiro Hasuo, Krzysztof Czarnecki, Fuyuki Ishikawa, Shin-ya Katsumata

発表会議：The 13th NASA Formal Methods Symposium

発 表 日：2021 年 5 月 26 日（水）口頭発表予定（米国東部時間）

〈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

国立研究開発法人 科学技術振興機構（JST）
広報課
TEL：03-5214-8404　E-mail：jstkoho@jst.go.jp

〈JST の事業に関すること〉

国立研究開発法人 科学技術振興機構（JST）
研究プロジェクト推進部　内田信裕
TEL：03-3512-3528　E-mail：eratowww@jst.go.jp

(*1) 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、さらにこれらを包括する実用的な 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 MMSD。プロジェクト詳細は https://www.jst.go.jp/erato/hasuo/ja/参照。