2013 年 4 月 16 日
株式会社日立製作所
日立オートモティブシステムズ株式会社

形式手法を用いた自動車制御ソフトウェアの高信頼検査技術を開発

従来比で10倍規模の量産ソフトウェアに適用

株式会社日立製作所(執行役社長:中西 宏明／以下、日立)と日立オートモティブシステムズ株式会社(取締役会長兼 CEO:大沼 邦彦／以下、日立オートモティブシステムズ)はこのたび共同で、自動車制御システムの品質を向上させるための、形式手法を用いた高信頼ソフトウェア検査技術を開発しました。形式手法は、要求仕様と設計をそれぞれ数学的に記述し、両者の違いを比較することにより、設計が要求仕様を満たすかどうかを厳密に検査する技術です。設計の不具合を高い精度で検査できる一方、検査のための計算が膨大になることから大規模なソフトウェアへの適用が難しいという課題がありました。今回、検査支援ツールを開発することで、これまでに論文等で報告されている形式手法の適用範囲に比べ、約 10 倍規模となる量産ソフトウェア(350kLLOC*1)に適用できることを実証しました。日立オートモティブシステムは、2013 年度より製品開発に本技術を活用し、より高信頼な自動車制御ソフトウェアを開発していきます。

自動車制御ソフトウェアや、社会インフラシステムを支える組み込みソフトウェアには高い信頼性が要求されます。しかし近年、組み込みソフトウェアが大規模化・複雑化することにより、既存の設計・検査手法では、高品質なソフトウェアを開発することが難しくなっています。これを解決する技術の一つが形式手法です。形式手法は、数学的手法で厳密に意味付けられた言語を用いて情報システム(ソフトウェアの要求や設計等)を記述し、情報システムがユーザの要求等を満たしているか等を、論理的に推論するための仕組みを提供する手法です。2011 年 11 月に発行された自動車向け機能安全規格 ISO26262 においても適用が推奨されています。

形式手法の一つに、モデル検査があります。 入力に対する期待出力を設定して検査を行う従来の手法とは大きく異なり、モデル検査では、設計したソフトウェアの仕様や動作をモデル化し、ソフトウェアが動作したときに取りうる「状態」を計算機で網羅的に調べ上げることにより、設計時に予期していない動作が起こり得るかを検査時に判定できます。その一方で、大規模なソフトウェアをそのままモデル化すると状態数が膨大になり、計算機のリソースが不足して検査ができないという課題がありました。したがって、検査に必要な計算機リソースが少ないモデルを作る技術がモデル検査の実用化の鍵となっていました。

この課題を解決するために日立は、ソフトウェアのソースコードから検査モデルを自動生成する技術を開発し、本技術を用いた検査支援ツールを製作しました。検査支援ツールの特長は以下の通りです(図 1)。

1. 変数依存関係に着目したソースコード解析技術

ソースコードから設計者が検査したい点に関係する部分だけを抽出し、計算機が調べる必要のある検査モデルの状態数を削減します。ソースコードにおける変数のつながり(依存関係)を解析

し、検査したい部分だけを高精度に絞り込むことで、近年の大規模な自動車制御ソフトウェアに対しても適用可能としました。

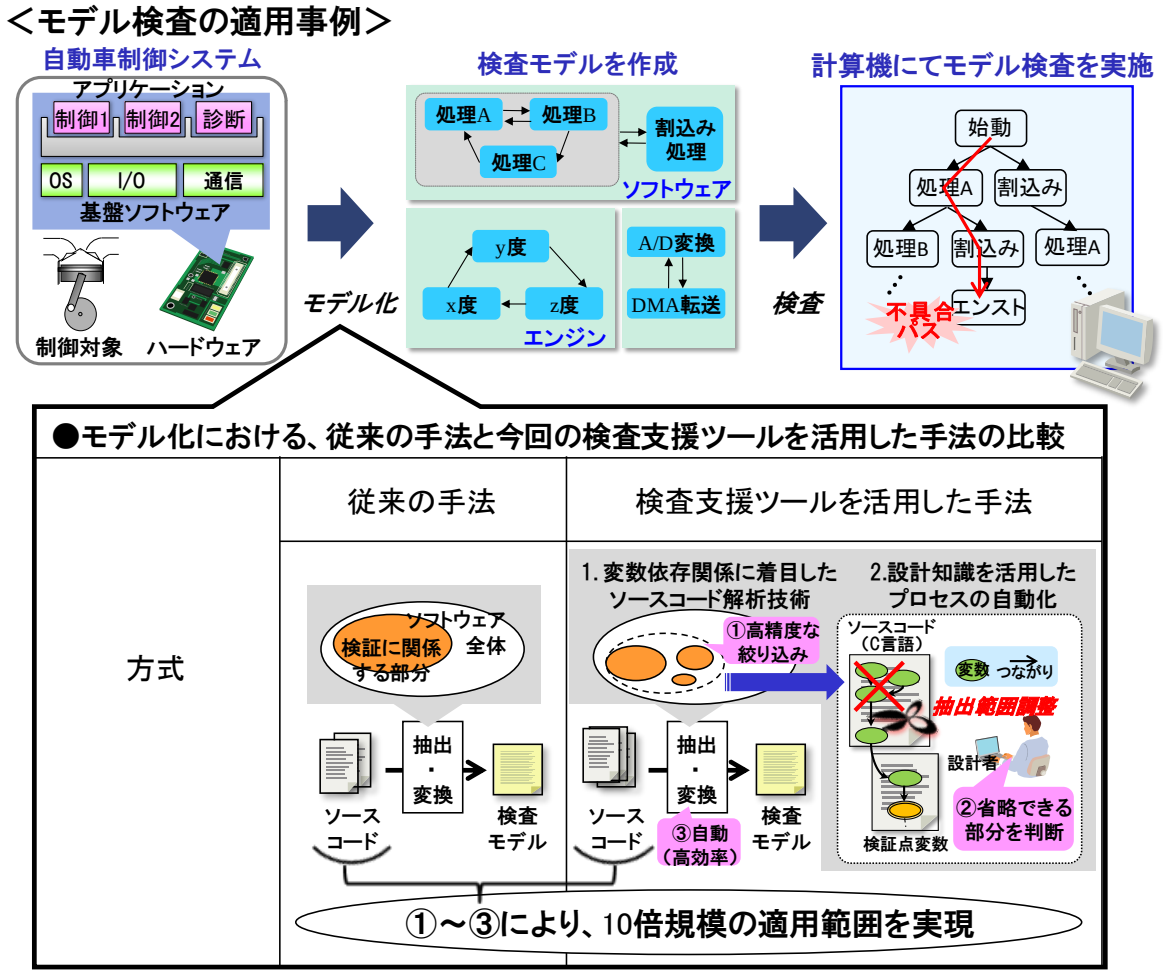
2. 設計知識を活用したプロセスの自動化

ソフトウェア開発者が設計知識を活用して検査点の選定や抽出範囲の調整を行い、それ以外のプロセスは自動化します。設計知識を活用することで、全自動でモデル化する手法に比べ、大規模で複雑なソフトウェアまで検査することができます。また、多くのプロセスを自動化することにより、全て手動でモデル化する手法に比べ、高い効率で検査モデルを生成することができます。

本結果により、高い信頼性で組み込みソフトウェアを検査できる形式手法を、量産レベルの大規模ソフトウェアに適用できる道を拓きました。日立オートモティブシステムズは、2013 年度より製品開発に本技術を活用し、より高信頼な自動車制御ソフトウェアを開発していきます。

本成果は、4 月 16 日から 18 日に米国・デトロイトで開催される SAE*2 2013 World Congress において発表予定です。

図 1 検査モデル作成手法の比較



■用語

*1 LLOC: Logical Line of Code (コメント等を除外したソースコードの行数)

*2 SAE: Society of Automotive Engineers (米国自動車技術会)

■照会先

株式会社日立製作所 日立研究所 企画室 [担当:滝澤]
〒319-1292 茨城県日立市大みか町七丁目 1 番 1 号
電話 0294-52-7508(直通)

以 上