2016 年 9 月 26 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

自動車制御システムの安全要件を自動検証する技術を開発

安全・信頼性を保持し、従来の 1/10 の時間で検証

株式会社日立製作所（執行役社長兼 CEO:東原 敏昭／以下、日立）と日立オートモティブシステムズ株式会社（社長執行役員&CEO:関 秀明／以下、日立オートモティブシステムズ）はこのたび共同で、自動車メーカーや自動車部品メーカーが制御システムの設計開発において作成する安全要件について、従来は設計者により異なることがあった要件の記述*1 を記号で簡略化し統一することで、安全要件の検証を行う際に要件に漏れがないことをコンピューターにより自動検証する技術を開発しました。本技術の採用により、安全要件の検証に要する時間を 1/10*2 に短縮することが可能となります。

日立と日立オートモティブシステムズは、自動車制御システムの安全・信頼性を保持しながら、作業効率の向上を図るとともに、自動車メーカーの自動運転車両の開発にも貢献していきます。

自動運転システムをはじめとした自動車制御システムの複雑化や大規模化の拡大に伴い、機能不全のリスクがますます高まっています。自動車制御システムの制御機能に不具合が起こると、ドライバーや同乗者だけでなく歩行者を含む周辺全体に危険が及ぶため、機能不全のリスクを十分に低減した自動車制御システムの開発を行うことが、国際標準規格 ISO 26262（機能安全規格）で定められています。

自動車制御システムの開発において始めに定義を行う要件には、主機能（自動運転システムなど）に関する要件と、主機能を構成する制御システムに不具合が起きた時にも安全を確保するための安全要件の二つの主な要件があります（図 1）。ISO 26262 に対応するためには、安全要件を漏れなく要件定義書に記述し、第三者認証機関や自動車メーカーなどに示す必要があります。

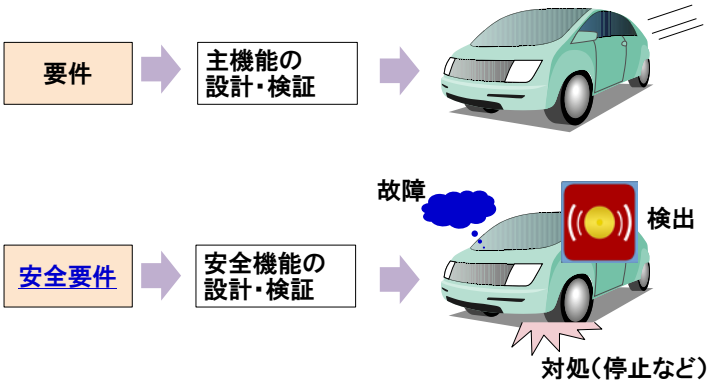

図 1 安全要件の位置付け

安全要件の記述には従来、日本語や英語といった言語が用いられてきました。しかし、一つの言葉や単語に複数の意味や解釈があるため、曖昧かつ不統一な表現をしやすい上、安全要件の記述に

漏れが発生するおそれもあり、専門知識を有した設計者でも、安全要件の内容確認や検証作業に多くの時間がかかっていました。

今回、日立と日立オートモティブシステムズではこれらの課題を解決するために、安全要件を記号化（論理式で記述）することで曖昧さをなくし、漏れがないことを自動検証する技術を開発しました。本技術は、国立大学法人北陸先端科学技術大学院大学（学長:浅野　哲夫）先端科学技術研究科セキュリティ・ネットワーク領域青木研究室の協力を得て開発したものです。

1. 安全要件に曖昧さをなくし、漏れがないことを自動検証する技術

安全要件を従来の自然言語から、数学的に厳密な論理式(命題論理*3)で定義することで、検証ツールに入力する内容を明確化します（図 2 ポイント①）。また、要件の内容を単純な式で書ける構文としたことで、設計者の安全要件の読み書きを容易にします。安全要件は、システムで保持したい安全について概略を上位要件として記してから、下位要件として、その安全を実現するために動作するECU*4、センサー、アクチュエーター（出力を遮断するスイッチなどの駆動部品）、通信、ソフトウェアの構成や処理について詳細に記していきます*5。このため、詳細化を進めると要件の数も増えていきます。検証ツールでは、制御システムの機能を指す上位要件と、その機能を実現する細かな下位要件を自動で検証し、漏れがないかを判定します。

2. 検証済の要件を再利用して、新たな要件を自動生成する技術

安全要件は、類似システム間や同じ製品システム内の構成部品間で、記載内容が類似することがあります。そのため、検証ツールで漏れがないことが示された論理式の一部を共通パターンとして再利用します（図 2 ポイント②）。これにより、例えばセンサーA の異常検出を、同じ条件下で利用するセンサーB でも行う場合、センサーA で作成したパターンにセンサーB のパラメーターを入力することで、新しい要件の論理式を自動生成します。検証済みのパターンを再利用することで、新しい要件に漏れがなく、また要件を新たに書き出す必要もないため、作業効率も向上します。

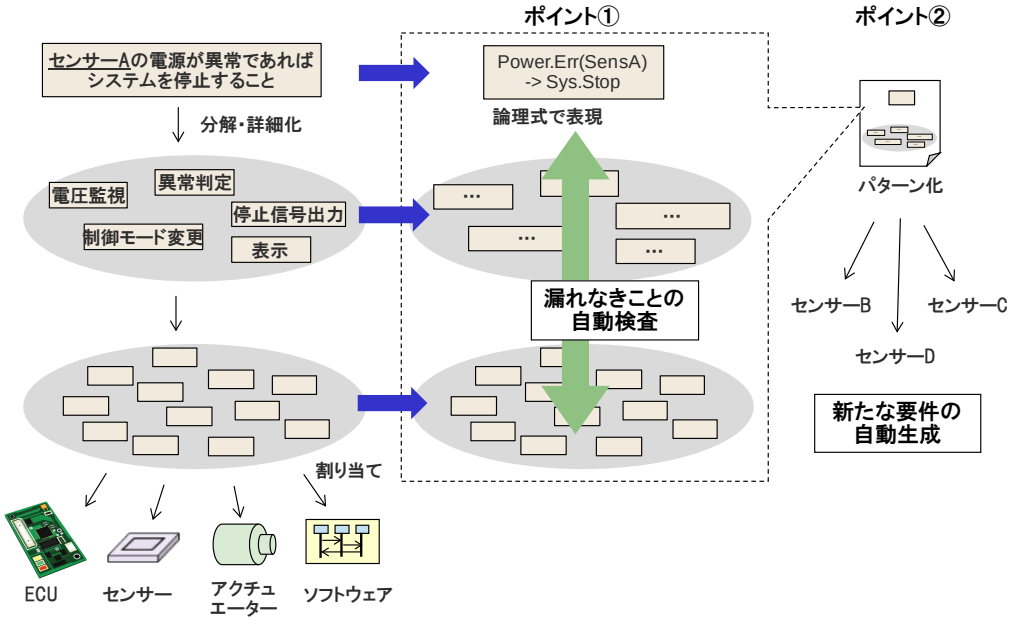

図 2　開発技術のポイント

自動車制御システムの一つである電動パワーステアリング*6 の制御システムに本技術を適用した結果、要件定義書に現れる全ての安全要件を記述・検証できることを確認しました。さらに、従来の英語での記述に対して記述量を 30%削減し、約 60 分かかっていた目視による検証時間もコンピューターによる自動検証により約 6 分に短縮できることを確認しました。なお、本技術は第三者試験認証機関であるテュフズードに、機能安全規格 ISO 26262 への対応の点で有効性を認められています*7。

日立と日立オートモティブシステムズは、自動車制御システムの安全・信頼性を高効率で保持する本技術の適用拡大や普及を通じて、加速する自動車産業の進展に貢献していきます。

*1 システムやソフトウェア開発の初期段階で、利用者がそのシステムなどに求めていることや、システムなどが成立するのに必要なことを明確にしていく作業を要件定義といい、従来日本語や英語等の自然言語により記述していた。要件定義書はそれらを文書化したもの。
*2 当社調べ。従来の目視による検証時間との比較。
*3 命題論理:表現の正しさを推論する数理論理学の一つ。
*4 Electronic Control Unit, 電子制御ユニット。
*5 前提とする安全の仕組みが適切であり、安全要件はその仕組みを表現している必要があります。
*6 電動パワーステアリング:モーターなどを用いて電気由来の力で運転者の操舵を補助する機構。
*7 2016 年 8 月にテュフズードジャパン株式会社よりフィージビリティレポートを受領しています。

■照会先

株式会社日立製作所 研究開発グループ 研究管理部［担当:鈴木、黒澤］
〒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