2018 年 1 月 15 日

報道関係各位

株式会社デンソーが長崎県立大学との自動車関連の研究プロジェクトで AdaCore 社 SPARK を採用

～「Freedom from Interference」を実証するためにフォーマルメソッドを適用～

AdaCore（エイダコア、本社：米国ニューヨーク州）は本日、　株式会社デンソー（以下デンソー）向け研究プロジェクト（Freedom from Interference、以下 FFI）実証するためフォーマルメソッドの適用」が成功裏に終了したと発表しました。

このプロジェクトは、デンソーと長崎県立大学との共同研究で、そのゴールは、安全性が決定的に重要な（クリティカルな）自動車用アプリケーションを、自動車の電気/電子機能安全についての国際規格「ISO 26262 Road vehicles – Functional safety」に沿って開発を簡素化することです。このプロジェクトは、レガシーな C 言語コードが多くを占める自動車システムにおいて、設計方法「VDM (Vienna Development Method) 」と実装言語「SPARK」を有効に使用できるか調査しました。

SPARK のソフトウェアコンポーネントは、ISO 26262 (FFI) の要求に従って、発生しうるレガシーC コードの妨害から保護されなければなりません。 デンソーは、SPARK Pro テクノロジで証明された AdaCore のフォーマルメソッドに関する専門的な知識と経験を評価し、AdaCore をパートナーとして選びました。

プロジェクトのフェーズ 1 では　AdaCore と長崎県立大学は　FFI の問題点についての調査を行いました。長崎県立大学のチームはフォーマルメソッドの使用について分析し、SPARK のアプローチによってシステムの安全性の検証作業を大幅に簡素化できると判断しました。

AdaCore は、SPARK 技術によって高い ASIL（Automotive Safety Integrity Level）を持つ（クリティカルな）コンポーネントそれ自体にエラーがないことを証明し検証作業を簡略化します。また AdaCore は ASIL が低い C コードに、SPARK の実行可能なコントラクト（事前条件と事後条件）を追加するガイドラインを作成しました。このコントラクトで、クリティカルではないコンポーネントの障害からクリティカルなコンポーネントを保護し、安全性を証明するのに役立ちます。

フェーズ１の終了後、デンソーは AdaCore と長崎県立大学がフェーズ２に進むことに合意しました。フェーズ２で AdaCore はソフトウェアアーキテクチャの安全解析のより一般的な問題に対してもフォーマルメソッドを適用可能か探りました。長崎県立大学では、VDM を使用して、障害の連鎖を検出/防止するための安全対策と安全機構を適用するための指針を策定しました。フェーズ２は 2017 年 10 月に完了しました。

「AdaCore の SPARK 技術は、フォーマルメソッドをクリティカルな自動車用ソフトウェアのための実用的なツールにします。デンソーの FFI プロジェクトで、その利点を実際に示す機会を与えていただいたことを嬉しく思っています。」と AdaCore の自動車市場製品担当マネージャー、ジュアン・カルロス・ベルネドは語っています。

「よくある質問は、C 言語のレガシーコードが多い既存システムにフォーマルメソッドが応用できるかについてです。我々のデンソーとの研究で、従来のテスト中心の検証手法に、SPARK を容易に統合でき、結果としてソフトウェアの信頼性、安全性、セキュリティに対して高いレベルの信頼性を獲得できます」。

「AdaCore 社はツールベンダーであるだけではなく、優れた研究パートナーでもあります。」とデンソー東京支社電子基盤先行開発室の東道担当課長は語っています。「このプロジェクトでは、デンソーから提示した研究課題や発想を素早く理解して、実りある議論を進めることができました。特にフェーズ２に向けての提案では、有力なオープンソースを活用するアイディアを提示していただきました。これは研究プロジェクトを効率良く進めるためだけではなく、今後の実用化への近道と期待できるものです。このように開発ツールに関する技術的な知見を背景に、AdaCore はバランスの良いソリューションを提示してくれています。」

「コンピュータ・システムならびにソフトウェアの開発のために、モデル指向形式手法の 1 つである VDM (Vienna Development Method)を使用しました。」と長崎県立大学の日下部茂教授は語っています。
「VDM モデルの構築と分析は、開発の初期段階から，システム仕様の不完全性とあいまいさを識別することに役立ちます。FFI の実現に向けて，このような既に確立されたソフトウェア向けの形式手法と、近年着目されている俯瞰的な観点のシステムエンジニアリングアプローチを組合わせる研究を行っていました。」

FFI (Freedom from Interference) について

自動車メーカーは、ソフトウェアの安全解析を行い、何らかの障害が発生しても安全関連機能を継続して実行することを証明しなければなりません。この解析の一部は、FFI オブジェクティブに適合しなければなりません。FFI は ISO 26262 によって求められており、安全上重要な機能と安全性にかかわらない機能が共存する場合、「２個またはそれ以上のエレメントでカスケード故障（障害の連鎖）が発生し、それが安全上の要求を阻害することがあってはならな

い」とされています。例えば、自動運転システムを制御するソフトウェアは安全性が最重要であり、ASIL が低いコンポーネント（例えばインフォテインメントなど）から保護されなければなりません。 FFI はこうした問題に対処する現実的なアプローチです。

SPARK Pro について

SPARK Pro はフォーマルメソッドを用いて完全性を検証する統合型の静的分析ツールスイートです。「SPARK 2014」言語をサポートし、GNAT Programming Studio (GPS)ならびに GNATbench IDE に統合された先進的な検証ツールを提供します。

SPARK Pro を使うことで、開発者はソフトウェアのアーキテクチャ・プロパティを形式化して定義でき、自動的にそれらを検証できます。それによって、ソフトウェアの完全性を広く保証できます。例えば、ランタイムエラーの防止、セキュリティポリシーの強制、機能の正確性（形式化して定義された仕様に準拠していること）などです。この自動検証は、ソフトウェアの障害が許容されないアプリケーションに特に適しています。 SPARK Pro は、コストと開発期間を削減するのを助け、フォーマルメソッドの使用によって数学的検証方法でソフトウェアライフサイクルの早い段階で問題を防ぎ、検出し、取り除きます。SPARK 言語とツールは、最も要求の高いセーフティ・クリティカルかつ高セキュリティのシステムで多くの採用実績があります。

AdaCore について

1994 年に設立された AdaCore は、ミッション・クリティカル、セーフティ・クリティカル、かつセキュリティ・クリティカルなシステムのためにソフトウェア開発・検証ツールを提供しています。次の 4 つが主力商品です。

- *GNAT Pro Ada* は、Ada の開発環境です。高い信頼性と保守性が求められるアプリケーションを、設計・実装・管理する為の完全なツールセットです。
- *CodePeer* は、先進的な静的分析ツールで、自動的に問題を検出して取り除く、Ada コードのレビュアーとバリデータを備えます。それらは開発中のソフトウェアにも、既存のソフトウェアにも適用できます。
- *SPARK Pro* は、検証環境です。フォーマルメソッドをベースとし、高信頼性システムの開発に適しています。

- *QGen* は、DO178C ツール資格を取得する等、安全性が重要な制御システム向けの、モデルベース開発ツールスイートです。カスタム可能なコード・ジェネレーター、Simulink®および Stateflow®モデルの静的な検証ツール、そしてモデルレベルのデバッガを提供します。

長年にわたり、AdaCore 製品のお客様は、セーフティ・クリティカルなアプリケーションを作り、保守し続けてきました。その分野は、商用航空機、自動車、鉄道、宇宙、軍事、航空交通管制制御、医療機器、財務サービスなどです。AdaCore の顧客は、世界的に幅広い分野で増えています。詳細については、http://www.adacore.com/customers/ （英語）をご覧ください。

AdaCore 製品はオープンソースで、開発エンジニア自身が専門的なオンラインサポートを提供しています。AdaCore は北米本社をニューヨークに、ヨーロッパ本社をパリに持ちます。
http://www.adacore.com

デンソーについて

デンソーは、自動車関連における先端技術、システムやコンポーネントの世界的なサプライヤーで、38 の国と地域で 15 万人以上の従業員を擁しています。
https://www.denso.com/jp/ja/

長崎県立大学について
長崎県立大学は 2016 年に情報システム学部を設置しました。この新学部は、情報システム学科と情報セキュリティ学科で構成され日本で初めて情報セキュリティを目的に設置されました。 この組み合わせは、安全とセキュリティに対する統合されたアプローチを促進すると期待されています。

【一般のお問い合わせ先】

アイティアクセス株式会社　（国内代理店）

E-MAIL：info@itaccess.co.jp

住所：〒222-8545 横浜市港北区新横浜 3-17- 6 電話：045-474- 9095

EU:
Emma Adby
AdaCore Marketing Operations Manager
+33 1 49 70 87 82

US:
Jessie Glockner
AdaCore Public Relations Representative
+1-646-532-2723