

報道関係各位

株式会社ジェイテクト、電動パワーステアリング・システム・サプライヤーが 安全性重視の自動車用ソフトウェア開発に SPARK Pro を採用

SPARK の形式手法が、安全重視の自動運転システム向け開発、検証コストを削減

AdaCore（エイダコア、本社：米国ニューヨーク州）は本日、株式会社ジェイテクト（以下 JTEKT）、自動車用電動パワーステアリング・システムの製造メーカーが、安全が重視されるパワーステアリング・システム・ソフトウェアの開発を支援するために、AdaCore の SPARK Pro ツールスイートと GNAT Pro Common Code Generator (CCG) を採用したことを発表しました。AdaCore のメンターシップ・プログラムを利用することにより、SPARK テクノロジーを短期間で導入することが可能となり、JTEKT は、SPARK 言語（Ada 言語サブセット）と形式手法を応用して、システムの C コードの単体テストと検証が容易となり、その正しさを証明する方法を実証しました。SPARK コードを C ソースコードに変換する CCG を使用することにより、SPARK の長所を活用しながら、JTEKT は開発済の C コードベースの設計資産の重要な安全特性を証明できるようになりました。

パワーステアリング・システムの制御ソフトウェアは、レーンキープアシストなどの自動運転システムと安全に通信する必要があります。誤作動により、生命を脅かしたり致命的な傷害が発生したりする可能性があるため、同システムは、ISO 26262 標準で定義されたハザードの最も厳格な自動車用安全度水準（ASIL）D に分類されます。



SPARK Pro は、Ada 言語サブセット対応のツールセットで、開発エンジニアは数学に基づいた厳格さで特定の脆弱性（バッファオーバーフロー、ゼロ除算、非初期化変数の参照等）がないことな

ど、ソースコードのプロパティを形式検証し、任意の表明（Assertion）を証明することができます。CCGを使用すると、Adaコンパイラが対応していないターゲットも含めて、SPARKアプリケーションをCコードにクロスコンパイルすることができます。SPARK ProとCCGはISO 26262およびIEC61508の機能安全規格への適合が認定されています。

「私たちは数年前から、信頼性への要求が高まる自動車ソフトウェアに対して、理論的に裏付けされた形式手法を研究している中で、SPARKを知ることができ喜ばしく思っております。」と、JTEKTの先行システム開発部上席主担当、米木真哉氏は語っています。「AdaCoreのツールは、セーフティ・クリティカルなソフトウェアテストの開発コストを低減し、安全かつ堅牢な量産コード開発に有効であると確信しています。」

「SPARKの形式手法を使用してCコードの正しさを証明することは、自動車の安全/セキュリティに関する最先端技術です。」と、AdaCoreの日本営業責任者であるジュアン・カルロス・ベルネド（Juan Carlos Bernedo）は語っています。「開発エンジニアにとって、自動車業界の最高レベルの保証基準を満足するソフトウェアを開発する上で、SPARKは費用対効果の高いソリューションの選択肢になりつつあります。JTEKTの事例は、Cコンパイラを提供するソフトウェア・プロバイダーが、SPARK言語とツールセットの導入、活用方法を示しています。」

ISO 26262 ならびに ASIL D について

ISO 26262は、自動車システムの機能安全規格であり、電気/電子/プログラマブル電子（"E / E / PE"）システムの一般的なIEC 61508規格の分野規格です。自動車の安全ライフサイクルのフェーズとそれに関連するアクティビティを定義し、リスクベースのアプローチを使用して、自動車用安全度水準（ASIL）と関連する要件を規定します。システムの機能分析は、機能不全が発生した場合の潜在的な危険と、生命ならびに資産への影響に焦点を当てています。ASILは、A（最低）からD（最高）で定義され、故障が曝露される確率、ドライバがハザードを回避できるか否か、ならびにハザードの発生の重大度が考慮されています。ASIL Dは、機能不全によって、生命に関わる、または致命的な傷害が発生する可能性を示します。そのため、安全性への目標が十分に達成されているかの保証が重要です。

株式会社ジェイテクトについて

株式会社ジェイテクトは、世界トップクラスの軸受メーカーである光洋精工株式会社と、世界をリードする技術を誇る工作機械メーカーである豊田工業株式会社が合併し、2006年に設立されました。株式会社ジェイテクトは、両社の最先端技術と製造への情熱を組み合わせ、自動車部品、ベアリング、工作機械の信頼できるシステムサプライヤーとして、社会に継続的に貢献する世界的に認められた製品と技術を顧客に提供しています。

AdaCore 社について

1994年に設立された AdaCore 社は、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向けにソフトウェア開発・検証ツールを提供しています。主力商品は次の4つです。

- ・ GNAT Pro は、Ada、C、C++に対応した統合化開発環境で、高い信頼性と保守性が要求されるアプリケーションを、設計、実装、管理する為のツールセットです。
- ・ CodePeer は、CWE 準拠の先進的な Ada コード用静的解析ツールで、ソフトウェアのエラーを検出し、レビューして検証する機能を備えています。また、CodePeer は、MITRE 社の Common Weakness Enumeration (CWE) で「最も危険なソフトウェアエラー上位 25」の検出が可能です。
- ・ SPARK Pro は、形式検証をベースに、高信頼性システムの開発に適した検証環境です。
- ・ QGen は、DO178C ツール資格を取得する等、セーフティが重要な制御システム向け、モデルベース開発ツールスイートで、Simulink[®]および Stateflow[®]モデルの静的な検証ツール、コード・ジェネレータ、さらにモデルレベルのデバッガを提供します。

長年にわたり、AdaCore 社製品のお客様は、セーフティ・クリティカルなアプリケーションを開発し、保守を継続してきました。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、医療機器、財務サービスなどです。AdaCore 社の顧客は、世界的に幅広い分野で増え続けています。詳細については、<https://www.adacore.com/industries> (英語) をご覧ください。

AdaCore 社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。同社の拠点は、ニューヨークならびにパリにあります。<http://www.adacore.com>

※本資料は、AdaCore 社のプレスリリースを意識したものです。正確な内容については、原文をご参照下さい。<https://www.adacore.com/press>

【お問い合わせ先】



アイティアアクセス株式会社（国内代理店）

E-MAIL : info@itaccess.co.jp

住所：〒222-0033 横浜市港北区新横浜 3-17- 6 電話：045-474- 9095

AdaCore US

Jessie Glockner

E: glockner@adacore.com

T: +1-646-532-2723

AdaCore EU

Juliana Silva

E: silva@adacore.com

T: +33-1-49-70-87-50

AdaCore UK

SingletonPR

E: abigail@singletonpr.com

T: +44 (0)1252 448 169

<http://www.adacore.com>

<http://twitter.com/AdaCoreCompany>