AdaCore

AdaCore 社 Ada 言語、SPARK 言語、C 言語対応ツールチェーン
ISO 26262 ならびに IEC 61508 安全規格認定を取得

AdaCore（エイダコア、本社：米国ニューヨーク発）は、2020 年 2 月 18 日 Ada 言語、SPARK 言語、C 言語向けの 3 つのソフトウェア開発/検証ツールが ISO 26262 および IEC 61508 の機能安全規格の下で認定されたことを発表しました。AdaCore 社は、航空、宇宙、鉄道などのセーフティ・クリティカルな分野で認証に関わる経験が 20 年以上あります。 自動車および工業安全規格の認定プロセスを完了することにより、同社の高信頼性技術が、自動車産業の厳しいソフトウェア保証要件を満たすことができることを示しました。認定を受けた 3 つの開発/検証ツールを次に説明します。

- GNAT Pro は、Ada および C プログラミング言語をサポートするツールチェーンで、複数の言語に対応できる堅牢かつ柔軟性が高い開発環境です。 GNAT Pro には、スタックサイズの計算、コーディング規格の検証、カスタマイズ/拡張可能な IDE などの開発検証ツールが統合されています。

- Common Code Generator（CCG）は、SPARK 言語（Ada 言語のサブセット）を C コードへコンパイルします。 CCG を使用すると、Ada および SPARK アプリケーションを、Ada コンパイラが対応していないターゲットを含め、C コードにクロスコンパイルします。

- SPARK Pro は、Ada 言語サブセット対応のツールセットで、開発エンジニアが特定の脆弱性（バッファオーバーフロー、ゼロ除算、非初期化変数の参照）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、個々の機能表明（Assertion）を証明することができます。

GNAT Pro コンパイラならびに CCG は、ISO 26262 TCL3 と IEC 61508 T3 認定を取得し、SPARK Pro 検証ツールは、TCL3 および T2 認定を取得しました。 3 つの製品は、世界的に権威のあるテュフズード（TÜV SÜD）が認定し、国内および国際基準を満たしていることが確認されました。 テュフズード（TÜV SÜD）の認定マークは、品質、安全性、持続性の証であるシンボルとして広く認知、尊重されています。

「この数年、費用対効果の高いツールや方法論への需要が自動車や他の産業分野で高まっています。」と AdaCore 社の事業開発責任者であるクェンティン・オシエム（Quentin Ochem）は述べています。 「Ada 言語や SPARK 言語は、信頼性の高いソフトウェアを必要とする開発エンジニアにとって、C 言語の代替手段として浮上し、安全認証の取得完了によって、同言語の導入を検討している企業の後押しとなっています。」

ISO 26262 と IEC 61508 に関して

ISO 26262 は、自動車システムの機能安全規格で、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 規格の派生物です。 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、自動車の安全度水準（ASIL）と関連する要件を決定します。 システムの機能の分析は、障害が発生した場合の潜在的な危険と、人体などへの影響に焦点を当てています。ASIL の範囲は、A（最低）から D（最高）であり、故障が曝露する確率、ドライバが対応するハザードを改善できるかどうか、およびハザードの発生の重大度を考慮しています。

ISO 26262 は、生産性ならびに正確さの両方の観点から自動化の利点で、ツール認定の要件を指定しています。　ツール認定方法は次の 4 つを定義しています。

- ツール使用に対する信頼性の向上
- ツール開発プロセスの評価
- ソフトウェアツールの検証
- 安全規格に準拠した開発

ツール認定は、Tool Confidence Level（TCL）に基づいており、1（最低）から 3（最高）の範囲で規定されています。ツールの TCL は、ツールまたはその出力のエラーが安全に関する問題を引き起こす可能性があるかどうか（「ツールの影響」）、ならびに、そのエラーを防止/検出する可能性（「ツールエラー検出」）によって決定されます。 TCL1 のツール認定は不要で、 TCL2 および TCL3 ツールには認定が必要です。システムの ASIL により、どの認定方法が最も推奨されるかが決定されます。 ツール認定資料には、ソフトウェアツール認定計画、ソフトウェアツール文書、ソフトウェアツール分類分析（関連する TCL を確立）、およびソフトウェアツール認定レポートが含まれています。

IEC 61508 は、E / E / PE システムにおける機能安全の国際規格であり、ISO 26262 などの特定分野固有の規格の「基盤」です。この規格は、安全ライフサイクル（に必要なエンジニアリングプロセス）、機能安全および安全水準、または SIL（リスク回避のレベル）の概念に基づいています。SIL の範囲は、SIL1（リスク回避の最低要件）から SIL4（最高）です。SIL は、要求に応じた障害の確率の観点から定義されます。 例えば SIL4 の場合、連続操作の 1 時間あたりの危険な故障の確率は 10-9 から 10-8 の間です。

ソフトウェア関連の要件は、ソフトウェアの開発/検証の手法と対策の項目とともに、IEC 61508 のパート 3 で定義され、要件は SIL に基づいています。 この規格では、3 つのツール認定カテゴリを指定しています。

- T1 : ツールは、実行ファイルとなるコードを検証したり、出力を生成したりするために使用されません。（例：テキストエディタ）
- T2 : ツールは、実行ファイルとなるコードのエラーを検出できないかもしれない（コーディング標準チェッカなどの検証ツール）し、コード生成しません。
- T3：ツールは、実行ファイルとなるコードの出力を生成できます。（コンパイラなど）

T2 または T3 に分類されたツールには明確な仕様書が必要です。T3 では、ツールがその仕様書に準拠している証拠を（妥当性検証、テストケースに基づいて）示す必要があります。

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、レビューならびに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、http:// 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訳したものです。正確な内容については、原文をご参照下さい。

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

AdaCore US:
Jessie Glockner
glockner@adacore.com
+1-646-532-2723

AdaCore EU:
Pamela Trevino
trevino@adacore.com
+33 1 49 70 87 93

http://www.adacore.com

http://twitter.com/AdaCoreCompany