

SuperTestとの併用でソースコードの100%バグフリーを保証する TrustInSoft

パリとサンフランシスコにオフィスを置き、国際的な航空・通信・産業用IoT・自動車業界にサービスを提供するソフトウェア開発ツール会社TrustInSoftは、Solid Sands社のコンパイラテスト・検証スイートSuperTestの典型的な顧客ではありません。同社の主力製品TrustInSoft Analyzerは高度なソースコードアナライザで、コンパイルする前にC/C++プログラムの正当性を検証するものです。コンパイラの開発や検証に特段関与していない企業であるTrustInSoft社がどのような目的でSuperTestを使用しているのかというと、ツールチェーンにおいてソースコードからバイナリにいたるまでISO 26262機能安全の認証が必要となるからです。

TrustInSoftのソースコードアナライザは、C/C++プログラムの数学的に厳密なモデルを作成して、プログラムの入力パラメータとターゲットアーキテクチャの情報とを合わせ、プログラムに未定義の動作がなく、機能要件に適合していることを100%の精度で検証します。

「形式手法を使用することにより、C/C++プログラムの動作について数学的に明確な解、つまりバグがないことの数学的な保証、を導くことができます。あるプログラムに対してTrustInSoft Analyzerが『問題ない』と言えば、どのような入力ベクトルを使っても、そのプログラムに違反が見つかることはありません」とTrustInSoftの共同設立者で最高技術責任者のBenjamin Monate氏は言います。

コンパイルに関してTrustInSoft Analyzerが必要とする情報は、GCCライクのターゲットであるかどうか、32ビットアーキテクチャ用か64ビットアーキテクチャ用のものかなど、コンパイラについて最小限のものだけです。

「解析のためには何もコンパイルしません。アナライザをパラメータ化するためにコンパイラに関連する情報が必要になりますが、コンパイラは最終的に呼び出されたときに期待通りに動作するものと想定しています。そこでC/C++規格を正しく実装しているコンパイラを選択するかどうかは、お客様に任されているのです」とMonate氏は言い、続けます。「もちろん、お客様はSuperTestのようなテストスイートを使って、コンパイラが正しく動作することを検証しなければなりません。コンパイラがソースコードを間違っただけで翻訳すれば、当社がソースコード上で数学的に証明した性質が実行ファイルに転移されることが保証できないからです。たとえコンパイラが完全に規格準拠であっても、未定義の動作を含むコードをコンパイルすると、意味がなく、重大かつ予測不能な安全性・セキュリティの問題を含みうる実行ファイルが生成されることに注意してください。そこに、TrustInSoft AnalyzerとSuperTestを使用することが必要となる理由があります」

ソースコードと実行ファイルが同じセマンティクスを持つことを保証するために最も重要なことは、アナライザとコンパイラがC/C++言語を該当する規格で定義されたとおり正確に解釈することです。TrustInSoft社にとってSuperTestはTrustInSoft Analyzerの規格準拠性をチェックするために使うツールの一つです。

「当社のツールは数学的な保証を与えるソリューションを提供する

ものですので、アナライザ自体の開発法は非常に厳格なものでなければならず、厳密に検証することが必要です。そして自動車市場向けには、特にISO 26262の認証が必要でした。当社には自社で開発した広範なテストスイートがありますが、ISO 26262に必要なエビデンスを提供する上で重要なのは、自動車エレクトロニクス業界ですでに広く認知されている独立したテストスイートを使用することでした。それが、SuperTestを選んだ理由です」とMonate氏は言います。



同社ではTrustInSoft AnalyzerがC/C++言語のセマンティクスを正しく解釈していることを確認するためにSuperTestを使用しているのです。

「規格の細かい部分でTrustInSoft Analyzerがまだ完全にはサポートしていない項目をSuperTestによって特定し、それらを実装・認証しています。Solid Sands社と当社のエンジニアとでC/C++規格の解釈について些細な食い違いを確認することもでき、今後も続けていきたい非常にやりがいのあるコラボレーションでした」とMonate氏は言い、さらに「当社にとって本当に重要なことは、SuperTestのおかげで、規格のカバレッジマトリックスを抽出できたこと、そして、完全に独立で、あらゆる可能性を隅々までチェックするよう綿密に設計されたテストスイートに基づいて、自社ツールの品質の証しとして、コードについて間違ったことは決して言わない、と示したことです」と言います。

ツールチェーンでソースからバイナリまでISO 26262認証を必要とするセーフティクリティカルシステムのソフトウェア開発者にとって、TrustInSoft AnalyzerとSuperTestを併用してソースコードを検証し、正しいコンパイルを保証することは、継続的インテグレーション環境にシームレスに適合する強力なソリューションです。

TrustInSoft AnalyzerとSuperTestの詳細については、www.trustin-soft.comとwww.soldsands.nlをご覧ください。



TrustInSoft社の主力製品はTrustInSoft Analyzerです。TrustInSoft Analyzerにより、ソフトウェア開発者とテスターはソースコードにバグがないことを数学的に保証でき、形式手法を備えた高度なソースコード解析によってソフトウェアテストの労力を大きく削減できます。TrustInSoftは、形式手法を産業用に誰もが使えるものになっています。現場でのバグ発見による影響が重大である企業のために、TrustInSoft AnalyzerはC/C++プログラム用の使いやすく網羅的な静的解析ツールを提供し、バッファオーバーフローや未初期化メモリ、ゼロ除算、解放済みメモリの使用などといった、問題を引き起こす「未定義の動作」のバグすべてを特定します。

数学的解析によってすべてのバグが検出され、誤検知はほとんどないため、開発者は修正すべき真の問題に集中し続けることができます。そのようなバグがコードに存在しないことを数学的に保証することで、ソフトウェア開発者やテスターは、それらによるソフトウェアのクラッシュやランタイムエラーが発生しないこと、ハッカーが利用してソフトウェアを制御されたり、秘密データにアクセスされたりできないことを確信できます。TrustInSoft Analyzerを使用している企業では、ソフトウェア検証の労力が4倍減少、バグ検出時間が40倍削減されたと特筆しています。



Solid Sandsは、北米、ヨーロッパ、アジアにおけるコンパイラとライブラリのテストおよび認証テクノロジーの大手プロバイダーです。私たちの使命は、Cの品質を向上させることです。これは、C/C++コンパイラ、ライブラリ、および分析ツールの品質を向上させ、それらを安全かつ確実に使用できるようにすることによって実現されます。当社のテストスイートの品質レベルにより、当社はソフトウェアテストと認定の最前線に立ち、お客様がISO準拠と機能安全規格の要件を達成できるように支援します。

2014年に設立されたSolid Sandsは、オランダのアムステルダムに本社を置いています。世界中のパートナーとともに、半導体、IP、セキュリティ業界の革新的な企業だけでなく、自動車、ロボット工学、鉄道、医療などの安全性が重要な企業にもサービスを提供しています。

当社のSuperTestコンパイラテストおよび検証スイートは、完全な検証環境を提供し、お客様がISO言語規格、および機能安全規格で要求されるソフトウェア品質レベルを達成できるようにします。一方、当社のSuperGuardライブラリ安全性認定スイートは、標準ライブラリ用の要件ベースのテストスイートであり、言語規格から導出された要件と個々のライブラリテストとの間の完全なトレーサビリティを備えています。

SOLID SANDS

from Amsterdam is the one-stop shop for
C and C++ compiler and library testing,
validation and safety services.

Postbus 7897 | 1008 AB AMSTERDAM | The Netherlands | www.solid Sands.nl