2016 年 11 月 16 日

報道関係各位

株式会社ヴィッツ

ソフトウェアの実行時不具合を根絶する形式検証ツールチェーン 販売開始
～自動車や航空宇宙で求められる高信頼性設計品質をサポート～

株式会社 ヴィッツ（本社：愛知県名古屋市、代表取締役社長：服部 博行）は、AbsInt 社（本社：ドイツ ザールブリュッケン）が開発する「ソフトウェアの実行時不具合を根絶する形式検証ツールチェーン」の日本国内唯一の販売代理店として販売・サポートを開始いたします。

本製品は、従来の動的試験やシミュレーションによる検証の代わりに、論理的に正しさを立証する画期的なツールです。これにより、高信頼性を必要とするシステム開発において、常に検証結果を信用することができ、検証コストを大幅削減できます。また、ISO 26262 や DO-178C などの機能安全規格への適合性の立証にも有効です。欧州の大手自動車メーカーや航空宇宙メーカーにも本格導入され、高い評価を得ております。

１．背景

近年、様々な産業製品に用いられる組込みシステムは高度に複雑化しており、品質の確保が著しく困難になっています。複雑な組み合わせパターンやタイミングパターンについて膨大な時間をかけて人間が動的試験を実施する開発体制では、不具合が無いことを保証することはできておらず、高信頼性を求められるシステムにおいても稀に不具合が発生するリスクがありました。

従来、このような問題に対しては、形式検証によって“不具合が存在しないこと”を証明する方法が有効だと考えられてきました。しかし、形式検証の導入には高度な専門知識が必要であり、あまり実用化されておりませんでした。

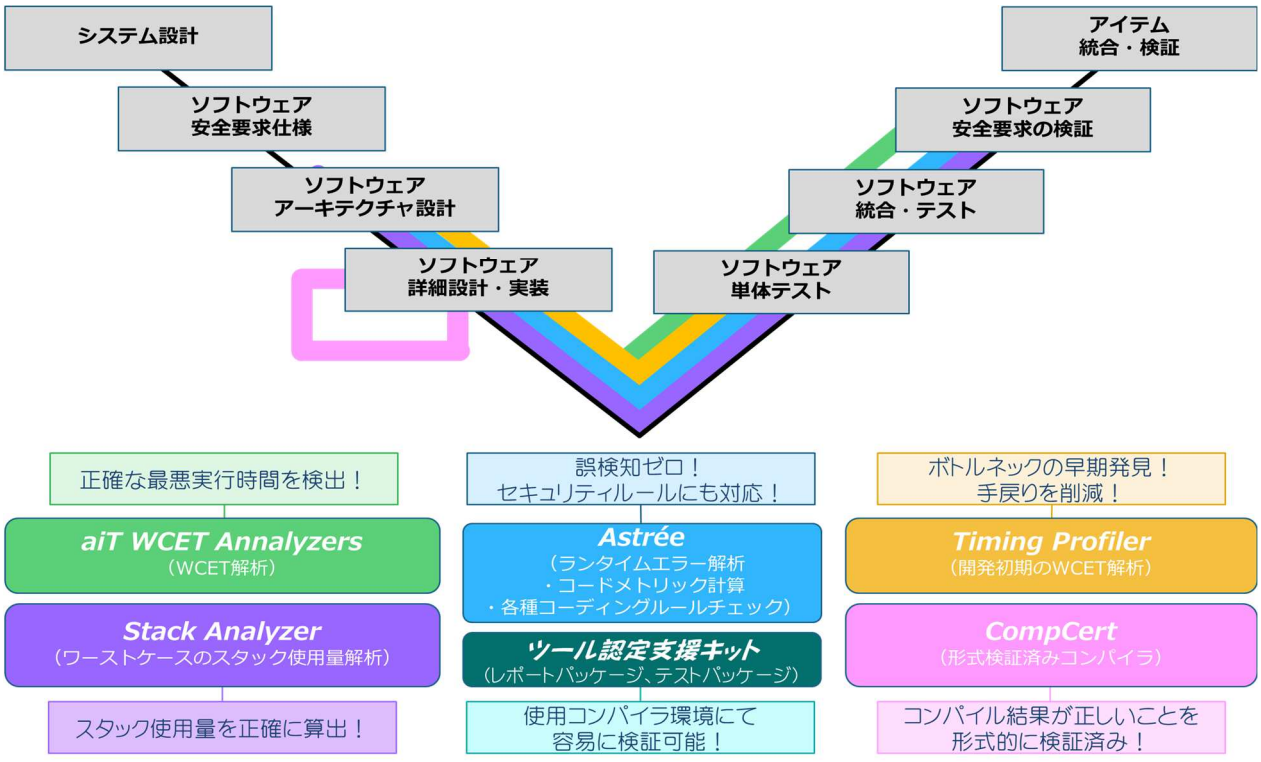
２．本製品による課題の解消

システム開発において、非機能要件に関連する不具合等は発見しにくく、完全に防げないのが現状であり、品質の低下や検証コストの増加を招く大きな要因となっております。長年にわたり高信頼性システムの開発を支援してきた当社では、従来のツールでは解決しづらい課題として、以下の表の問題点が存在すると考えます。これらの課題に対し、本製品を用いることで、ユーザーは形式検証技術による容易な課題解消が可能となります。

従来のツールの課題点	本製品の特長
ランタイムエラーの検知漏れ・過剰検知 ・不具合の可能性は検知できるが、全ての不具合の検知までは保証していないため、追加の動的検証が必要 ・正常処理に対しても、不具合の可能性として過剰に検知することがあり、これらに対しても確認作業が必要	**ランタイムエラーを正確かつ確実に検知** ・形式検証技術を用いた解析によって論理矛盾が無いことを証明することで、不具合を正確に、漏れなく検知 ※某航空機メーカーの飛行制御ソフトウェアの解析において、過剰検知ゼロの実績あり
正確値ではなく推測値で最悪実行時間を算出 ・複雑なキャッシュやパイプライン構造を持つプロセッサの最悪実行時間のシナリオ想定は、技術者の力量に依存 ・想定されるシナリオの証明、実施検証は困難	**保証された最悪実行時間を算出** ・キャッシュとパイプライン構造の形式モデルに基づき、CPU のクロックレベルで正確に最悪実行時間を算出 ・数学的にシナリオの正しさを証明することで、タイトな時間要件の設計にも使用が可能
高度な専門的知識がないと使いこなせない ・専門的な知識を習得したエンジニアでないと使用しにくいツールのため、導入ハードルが高い	**専門的知識がなくても容易に活用できる** ・ソースコードまたはバイナリファイルを入力するだけの簡単な操作で、ほぼ自動的に解析し、結果を出力 ・ビジュアルに優れた高いユーザビリティを提供

3．本製品の構成と特徴

本製品は、開発の上位工程から下位工程にわたって、検証作業を大幅に削減します。バイナリファイルを自動解析した結果を元に、高度なビジュアル表示によって、修正作業も効率化します。機能安全で要求されるツール認定作業を低減するキットも提供しています。



４．今後の展開について

当社は、本製品の販売だけではなく、お客様の既存の開発プロセスとの融合を支援してまいります。また、機能安全やセキュリティ開発に関する要求事項や、日本企業の開発に適した機能などを、AbsInt 社に要望することにより、日本企業にとってより使いやすいツールに改善してまいります。

アイシン・コムクルーズ株式会社　走行安全・VIT 技術部　部長　鬼頭正広　氏のコメント

現在の自動車の開発では、タイミングの問題などで稀にしか発生しない不具合を防ぐために膨大な検証を実施していますが、それでも完全に取り除くことは極めて困難です。AbsInt 社のツールは、画期的な形式検証技術により、不具合を確実に検出できることに加え、誤検出がないため、検証費用を大幅に低減できるところに大きな魅力を感じます。かねてより機能安全を得意とするヴィッツがツール活用の支援を提供することにより、国内企業の品質と生産性の向上の更なる後押しとなることを期待します。

AbsInt 社（本社：ドイツザールブリュッケン）CEO Dr. Christian Ferdinand 氏のコメント

So far our tools have been widely used in the European market due to their powerfulness and rigorousness based on the formal technologies. We've searched for the right partner to represent us in Japan, and we are delighted to have found an excellent partner with WITZ.

WITZ has a lot of experience and achievements in the fields of real-time embedded systems, functional safety, and formal method. This gives us an outstanding chance to offer our most advanced program analysis tools and verified compilers to Japanese customers.

（私達のツールは、形式手法記述をベースにした強力で厳格なツールであり、ヨーロッパでは広く使われております。これまで私達は、日本で一緒になって活動してくれる素晴らしいパートナーを探していました。今回、ヴィッツという素晴らしいパートナーと出会うことができ、とても嬉しく思っています。

ヴィッツは、リアルタイム組込みシステム・機能安全・形式手法の分野で多くの経験と成功を収めてきました。これは、私達の最も先進的なプログラム分析ツールや検証されたコンパイラを、日本の皆様に提供する素晴らしい機会を与えてくれることでしょう。）

【お問い合わせ先】

本発表に関するお問い合わせは、以下にお願いします。

株式会社ヴィッツ
総務部：脇田、佐藤（技術的内容：機能安全開発部　森川）
TEL: (052) 220-1218