株式会社 ヴィッツ

【ET2016 プレス発表】
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代理店販売開始!!

2016年11月16日

株式会社ヴィッツ
機能安全開発部
設計・技術開発室 兼 プロセス支援室 室長
水野 智仁

本発表の概要

株式会社 ヴィッツ

- 株式会社ヴィッツは、AbsInt社（ドイツ）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」**の代理店販売を開始しました。
- 本ツールチェーンは、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技術を提供します。
- これにより、**品質向上、検証コスト削減**を強力に支援することができます。

AbsInt社とツールの概要紹介

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とは】

- ツール群

ツール名	主な機能
Astrée	ランタイムエラー解析 コードメトリックの計算 各種コーディングルールチェック
CompCert	形式検証済みのコンパイラ
aiT WCET Analyzers	WCET解析
StackAnalyzer	ワーストケースのスタック使用量の解析
TimingProfiler	（開発初期の）WCET計測

- 開発元：AbsInt社（本社：ドイツ ザールブリュッケン）
- 販売実績：欧州、米国、ロシア、アジアなど
  - 大手自動車、航空宇宙メーカーで導入され、ツールの信頼性は証明済み

背景：従来の開発における課題

株式会社 ヴィッツ

- 近年、様々なシステムは、複雑化が爆発しており、人手による品質確保はますます困難を極めている
- 従来は膨大な動的試験を行っても、稀に不具合が発生することが、非常に大きな問題だった
  - 動的試験（膨大な時間とコストがかかる）
    - 複雑な組み合わせパターン
    - タイミングパターン

動的試験の問題点

正しいことを保証できない

- その解決策として、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言われてきた

形式手法による検証の利点と問題点

正しいことを保証できるが、高度な専門知識が必要なため、実用化されてこなかった

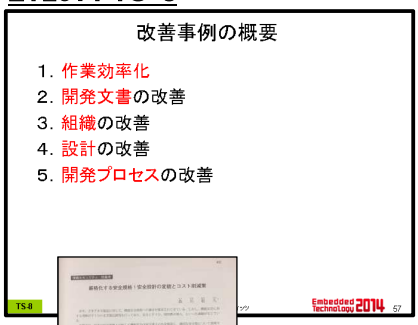
当社の高信頼性開発のコスト削減への取り組み

株式会社 ヴィッツ

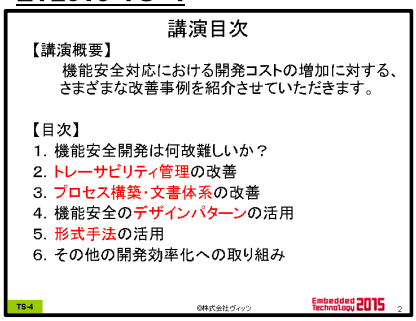
2006年：機能安全の研究開発活動を開始
2008年：機能安全コンサル事業を開始
2010年：日本初 IEC 61508 SIL3 ソフトウェア開発プロセス認証を取得
2012年：世界初 ISO 26262 ASIL-D ソフトウェア開発プロセス認証を取得
2012年：開発コスト削減に注力開始

【当社の開発コスト削減の主な紹介事例】

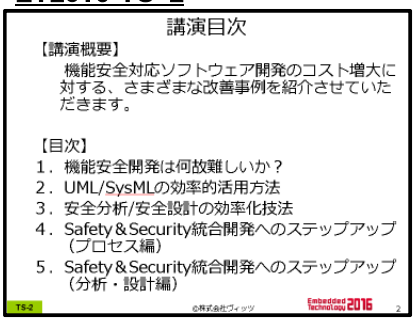
ET2014 TS-8



ET2015 TS-4



ET2016 TS-2



安全工学 Vol.54 No.6 (2015)
『厳格化する安全規格！
安全設計の変貌とコスト削減策』

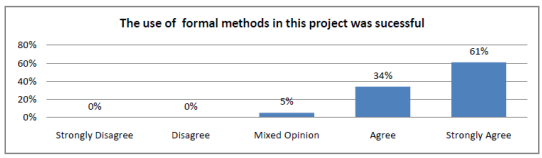
【課題】未だ全世界においても、「低コスト開発プロセス」の決定版は無く、多大な開発・検証費を要している

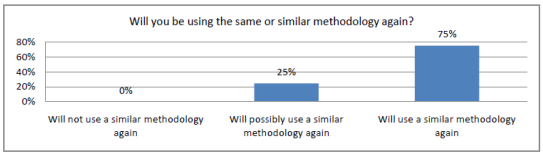
当社の形式手法活用実績＆普及活動

株式会社 ヴィッツ

【世間の形式手法の普及状況】

海外：導入数・継続率は高く**普及傾向**
日本：あまり**普及していない**

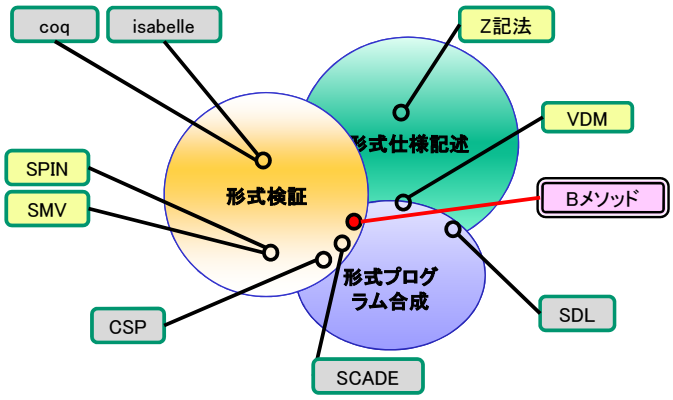




http://deploy-eprints.ecs.soton.ac.uk/161/2/fmsurvey%5B1%5D.pdf

【当社の形式手法の実績】

- 2006年より形式手法の研究・活用に着手。
- さまざまな形式手法の経験あり
- この内、最有力となる「Bメソッド」の普及に尽力



【課題】日本国内では、手法の利点よりも難しさが障壁に
普及には、学習などの事前準備コストゼロの簡単さが必要

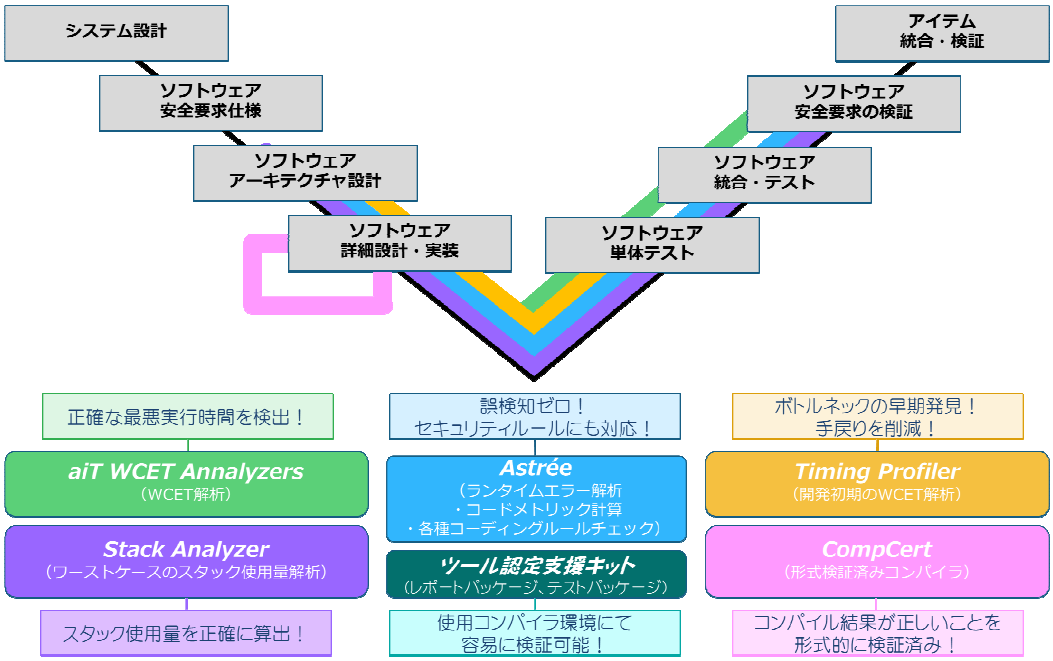
【当社のBメソッド活用支援】

- UML/SysML⇒Bメソッド変換ツール
- トレーニングコース（3週間）
- 活用ノウハウ集

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機能概要

株式会社 ヴィッツ

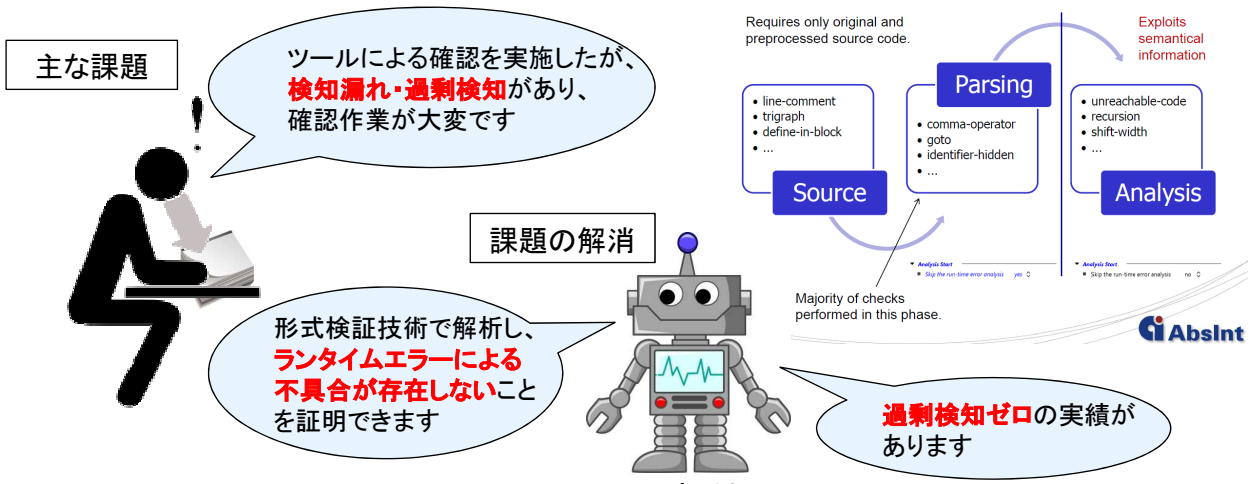
- ◆ 開発の上位工程から下位工程にわたって、検証作業を大幅に削減します。
- ◆ 機能安全で要求されるツール認定作業を低減します。



既存ツールの限界への改善策(1/3)

株式会社 ヴィッツ

従来のツールの主な課題	本ツールチェーンによる課題の解消
(A) 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	**① 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



既存ツールの限界への改善策(2/3)

株式会社 ヴィッツ

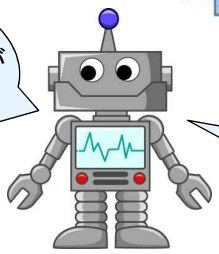
従来のツールの主な課題	本ツールチェーンによる課題の解消
(B) 正確値ではなく推測値で最悪実行時間を算出 • 複雑なキャッシュやパイプライン構造を持つプロセッサの最悪実行時間のシナリオ想定は、技術者の力量に依存 • 想定されるシナリオの証明、実施検証は困難	② 保証された最悪実行時間を算出 • キャッシュとパイプライン構造の形式モデルに基づき、CPUのクロックレベルで正確に最悪実行時間を算出 • 数学的にシナリオの正しさを証明することで、タイトな時間要件の設計にも使用が可能

主な課題

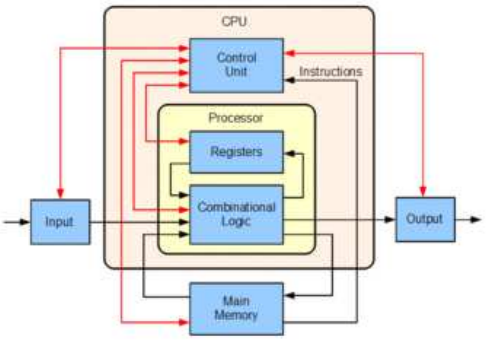
最悪実行時間(WCET)に至るシナリオは、おそらくこうだろう
(推測)
※確実に正しいとは言えません

課題の解消

形式モデルを使ってキャッシュとパイプラインがあるCPUでもWCETを解析できます



数学的に**WCETとシナリオの正しさを保証**できます

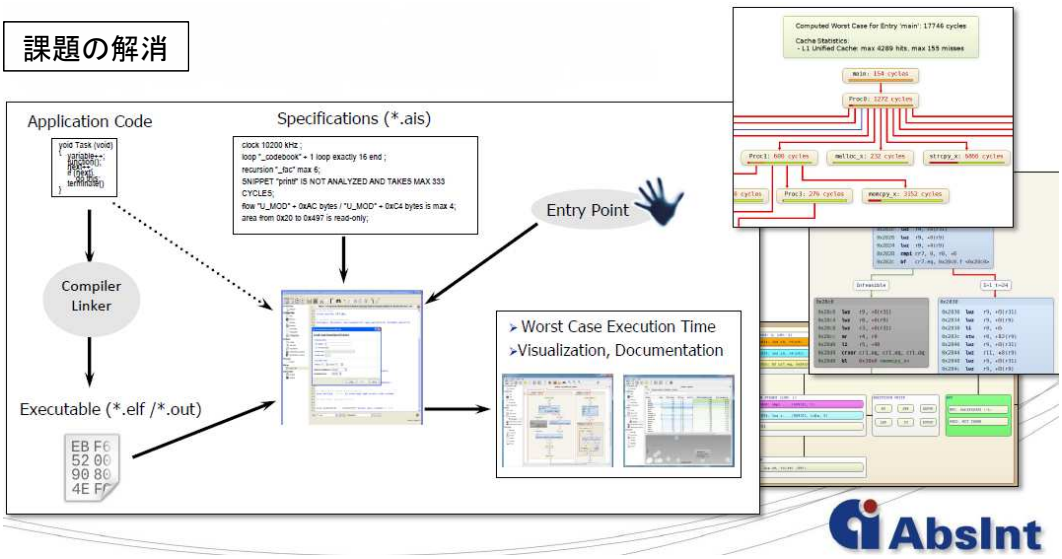


既存ツールの限界への改善策(3/3)

株式会社 ヴィッツ

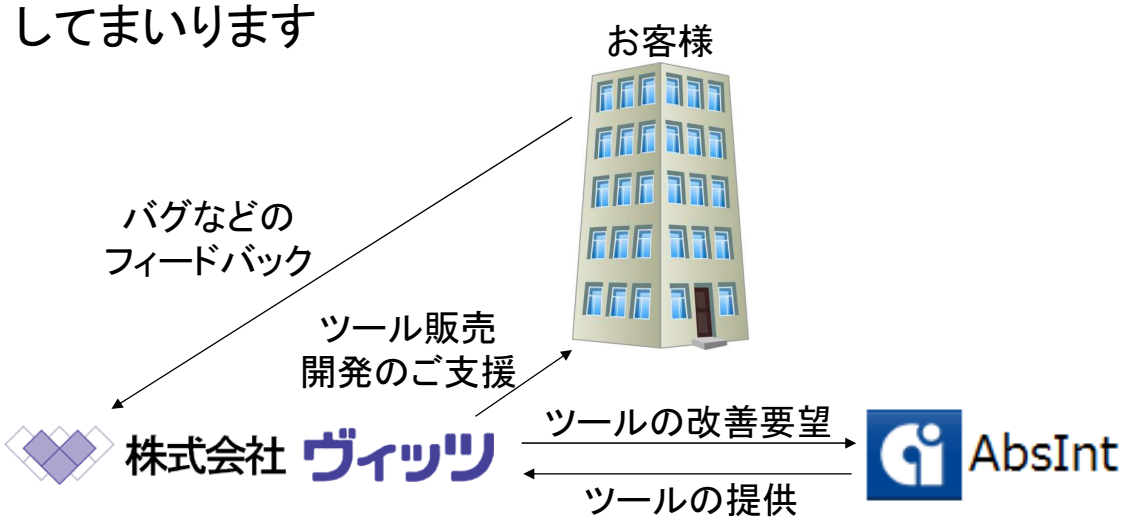
従来のツールの主な課題	本ツールチェーンによる課題の解消
(C) 高度な専門的知識がないと使いこなせない • 専門的な知識を習得したエンジニアでないと使用しにくいツールのため、導入ハードルが高い	③ 専門的知識がなくても容易に活用できる • **ソースコードまたはバイナリファイルを入力するだけの簡単な操作で、ほぼ自動的に解析し、結果を出力** • ビジュアルに優れた高いユーザビリティを提供

課題の解消



当社の今後の対応

- ◆ 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



補足資料

Astréeの機能概要①

株式会社 ヴィッツ

◆ Astréeは、潜在的なランタイムエラーを検知するツール

✓ 以下の潜在的なランタイムエラーを検知可能

- ゼロ除算
- 範囲外の配列インデックスへのアクセス
- 誤ったポインタ操作と参照（NULL、未初期化、宛先がないポインタ）
- 整数および浮動小数点演算オーバーフロー
- 未初期化の変数への読み込みアクセス
- データ競合
- 一貫性のないロック（ロック／アンロック問題）
- オペレーティング・システム・サービスへの無効な呼び出し
- ユーザー定義されたアサーション違反
- デッドコード

データ競合、一貫性のないロック（ロック／アンロック問題）、デッドロックは、他のツールでは完全に保証できない

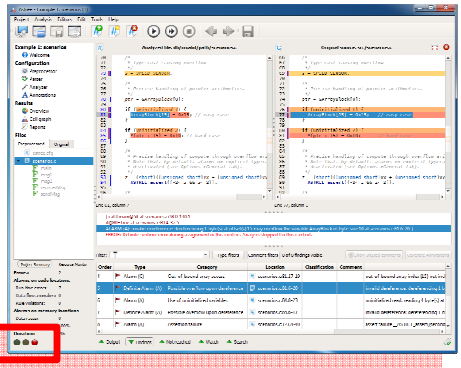
Astréeの機能概要②

株式会社 ヴィッツ

✓ 潜在的なランタイムエラーを深刻度別に分類して報告

- 形式手法に基づいた抽象解釈（abstract interpretation）によって、潜在的なランタイムエラーを100%検知し見逃さない
- 深刻度別に4段階で表示可能

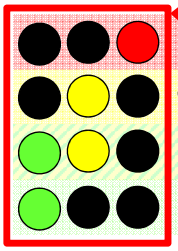
Cソースコードを読み込ませるだけで、ランタイムエラーを自動的に検出



深刻度

高

低



赤	エラーが存在する
黄	エラーは無いが、アラームAが少なくとも1つ存在する
緑and黄	エラーとアラームAは無いが、アラームCが少なくとも1つ存在する
緑	エラーとアラームは無い

アラームA:結果が予測できない潜在的なランタイムエラー
アラームC:結果が予測可能な潜在的なランタイムエラー
エラー:　プログラムの特定の状況、条件下で限定的に発生するアラームA
または 分析における致命的なエラー（例えば、入力ミスによる解析エラー）

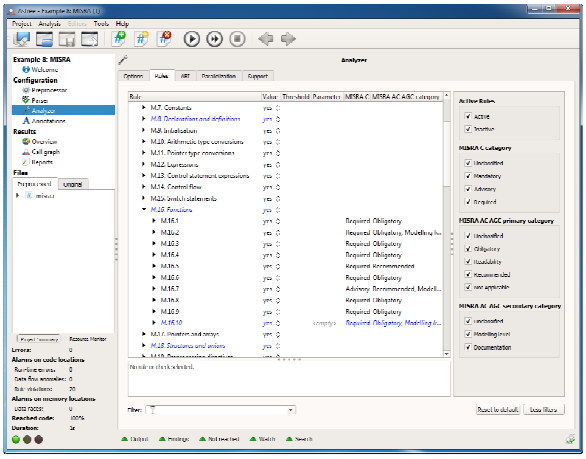
Copyright Witz Corporation 2016
2016/11/16 ET2016プレス発表

Astréeの機能概要③

株式会社 ヴィッツ

- ✓ **コーディングルールチェック静的解析ツールとして、各種コーディングルールに対応**
  - MISRA-C:2004、MISRA-C:2012 incl. Amendment1
  - CWE
  - SEI CERT C Coding Standard
  - ISO/IEC TS 17961:2013
  - （オプション）ユーザー独自のルール
- ✓ **機能安全開発における ツール認証に必要な情報を、ユーザ様にご提供可能（ツール認証キット）**
- ✓ **他社の同種ツールに比べて Matlabが不要で、単体で使用可能**

ユーザ独自のコーディングルール チェックもオプションで用意可能

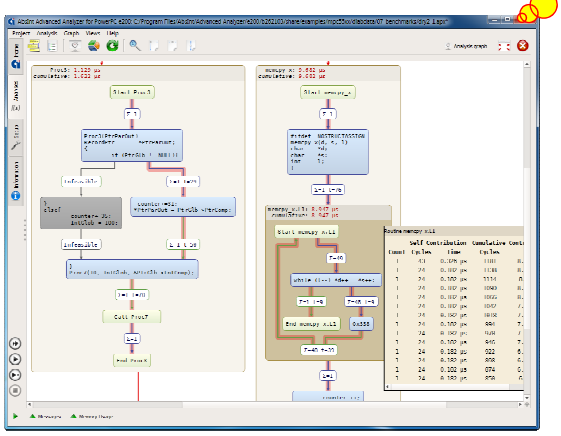


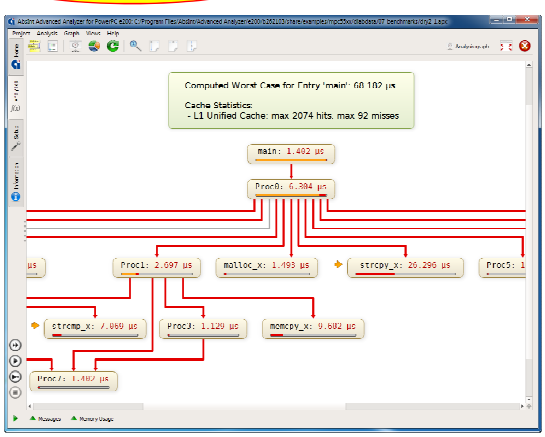
aiT WCET Analyzersの機能概要

株式会社 ヴィッツ

- ◆ **aiT WCET Analyzersは、形式モデルに基づいた完全に保証できる最悪実行時間を算出するツール**
  - ✓ ソースコードまたは実行可能コードを入力するだけで、自動的に最悪実行時間に至るシナリオを分析、結果を出力可能
  - ✓ 最悪実行時間に至るシナリオと入力は、数学的に正しいことを証明可能

技術者が最悪実行時間に至るシナリオを考える必要はありません。ツールが完全保障します

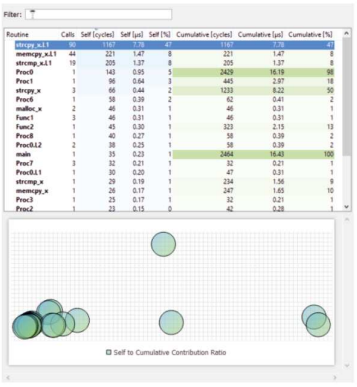


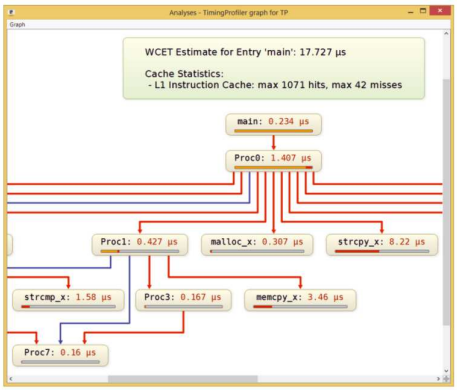


TimingProfilerの機能概要

株式会社 ヴィッツ

- **TimingProfilerは、コード開発中の動作タイミングを監視するツール**
  - ✓ 実機を使うことなく、開発の初期段階でタイミングの振る舞いを確認できるため、ボトルネックを早期発見でき、統合時の手戻りを減らすことが可能
  - ✓ aiTと比べて、最悪実行時間を保証するものではないが、効果的にタイミングを推定することが可能
  - ✓ グラフや表形式で関数ごとの時間情報を一覧を表示可能
  - ✓ 時間情報を持つコールグラフ、制御フローグラフを表示可能

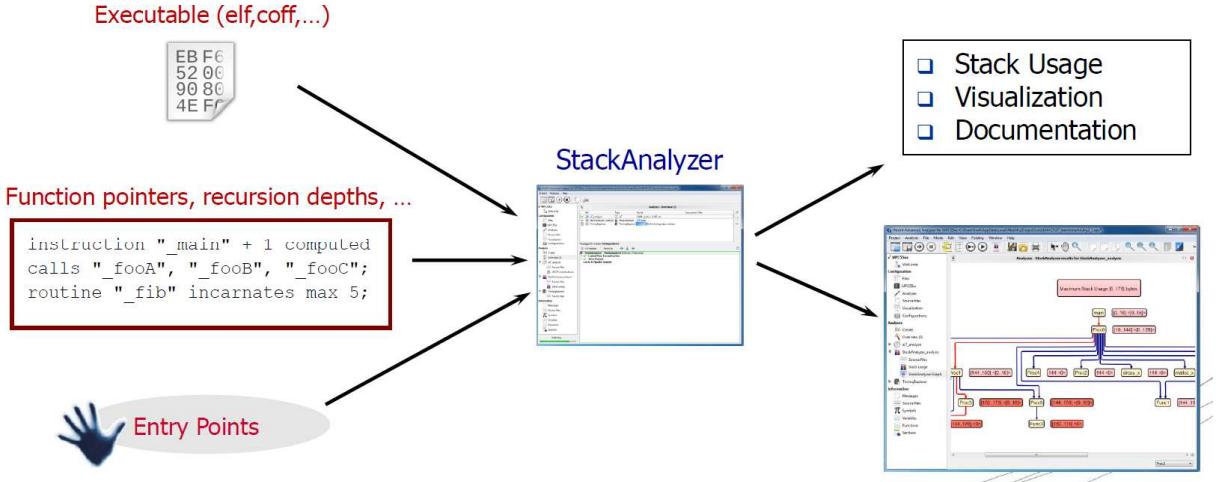




StackAnalyzerの機能概要

株式会社 ヴィッツ

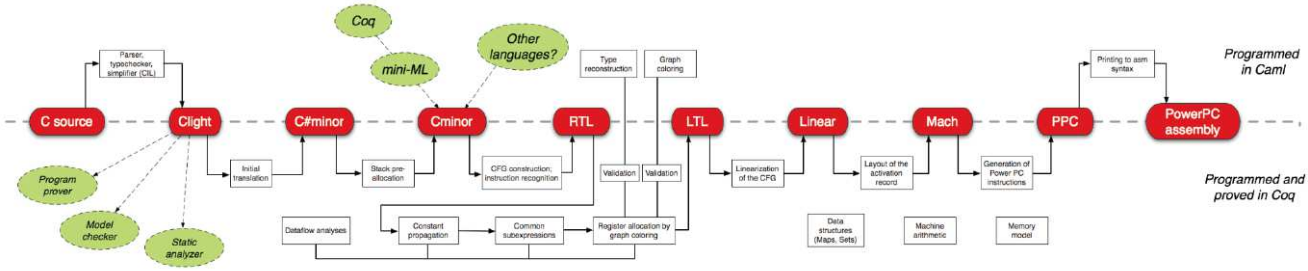
- **StackAnalyzerは、スタックオーバーフローが発生しないことを保障するツール**
  - ✓ 実行可能なバイナリファイルを入力として分析が可能(デバッグ情報、計測化の技法に依存することはない)
  - ✓ ループ、再帰、インラインアセンブリ、ライブラリ関数、Link Time Optimizationを考慮しているので、忠実にプログラムを解析可能
  - ✓ 安全規格に対するツール認証支援キットあり



CompCertの機能概要

株式会社 ヴィッツ

- **CompCertは、"machine-assisted mathematical proof"によって形式検証されたCコンパイラ**
  - ✓ 生成されたコードが、生成元のCソースプログラムのセマンティクス(意味論)と同じ振る舞いをすることを完全保証
  - ✓ CompCertが生成したコードは、最適化オプションを使っていないGCCよりも2倍ほど速い速度を実現している。(ただし、レベル3で最適化されたものよりは、20%ほど速度が遅い)



CompCert Phases