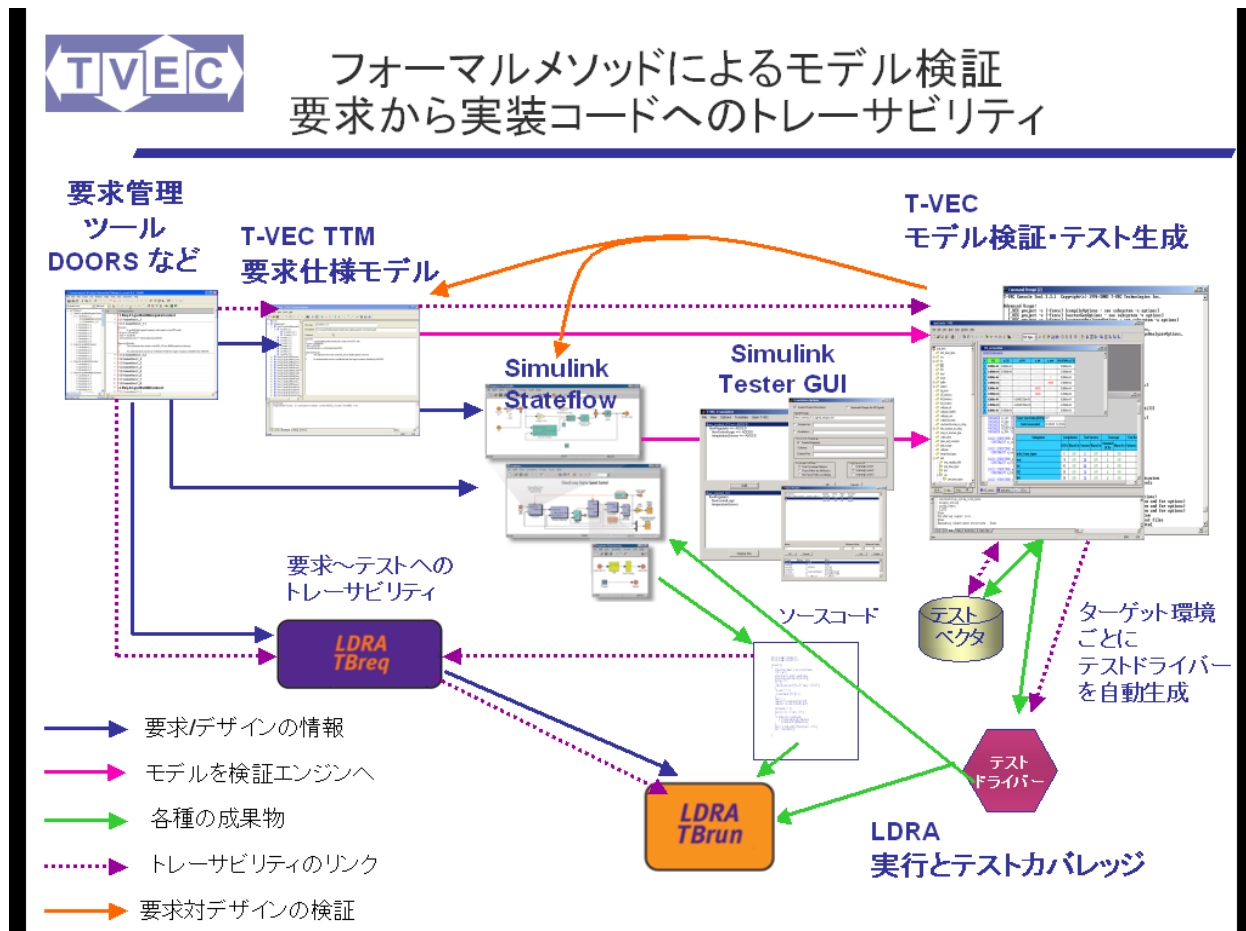




フォーマルメソッドによるモデル検証 要求から実装コードへのトレーサビリティ

要求モデル, デザインモデル等のツールにはモデル検査, シミュレーション, 自動ソースコード生成などをサポートするものは多く有りますが、開発の50%以上を占めるテストまで自動化するものは限られています。T-VECは, モデルを解析しその過程からテストベクタ(テスト入力と期待出力)を生成して, モデルに相対するコードへのテストドライバー生成・実行・結果判定まで行うモデルベースの検証ツールです。

“Lockheed Martin 社では Test Automation Framework (TAF) を採用し、要求仕様に基づいたテストを効率良く実現することに成功した。これは、JSF/F-35, F2, C5 等最新機種開発のみならず、T-50, F-16 などの既存ソフトウェアに対する機能追加にも有効である事が評価された。機能追加部分を T-VEC 社の表形式モデル化ツール(TTM)で記述し、TAF に高度に統合しうること確認した。Flight Control LAWS アプリケーションでは、6~12 回に及ぶリリースごとのテストを効率化し、テスト費用だけで6 億円以上の削減を得た。更に重要なのは、結果としてリリーススケジュールが短縮され、これ以上の効果が得られた事である。また、開発後半でないと言著にならないような(ゼロ割など)問題をデザインフェーズで明らかにすること、自動ソースコード生成ツール使用におけるエラーの早期検出など、開発後半では解決に相当なコストや時間、労力が割かれる問題に対する成果は我々の製品のソフトウェアにとっては億単位の成果になった”(2005年初頭)



T-VEC の特徴 :

T-VEC はフォーマルメソッドを利用したモデルベース検証ツールです。要求モデル (TTM) やデザインモデル (Simulink/Stateflow) を解析しモデル上の欠陥を抽出。解析の結果得られる入力値と期待値をテストベクタとして、ソースやオブジェクトコードがモデルと一致しているか、コードに欠陥が無いかを検証出来ることが特徴です。

他のフォーマルメソッド、モデル検査ツールに対する T-VEC の優位点は、

- *フローティング、ダブルなどにも対応 (インテジャー、ブーリアンなどのみでは無い)
- *リニア、ノンリニア式 共に対応
- *サブシステムごとに上流のコンストレインツを加味した入力での検証 (状態爆発しない)
- *テストベクタはシステム階層内のサブドメインごとに取り得る境界値を狙った入力値
- *検証結果の成果物として得られる入力値と期待値をテストベクタとして、ソースやオブジェクトコードがモデルと一致しているかの検証が出来る
- *要求モデル、デザインモデル (Simulink/Stateflow) の両方に対応している

以上の特徴をもって、大規模な組み込みシステムで実践的に採用されているモデル検証ツール (モデル検査のみではない) が T-VEC です。

テスト自動化のフレームワーク :

以下、図1に TAF の概略を示しそのコアである T-VEC について解説します。要求管理、デザインモデリング、テストカバレッジなどのツールに T-VEC テスト自動化ツール (モデル検証、テスト生成) を開発全工程に渡って統合しています。

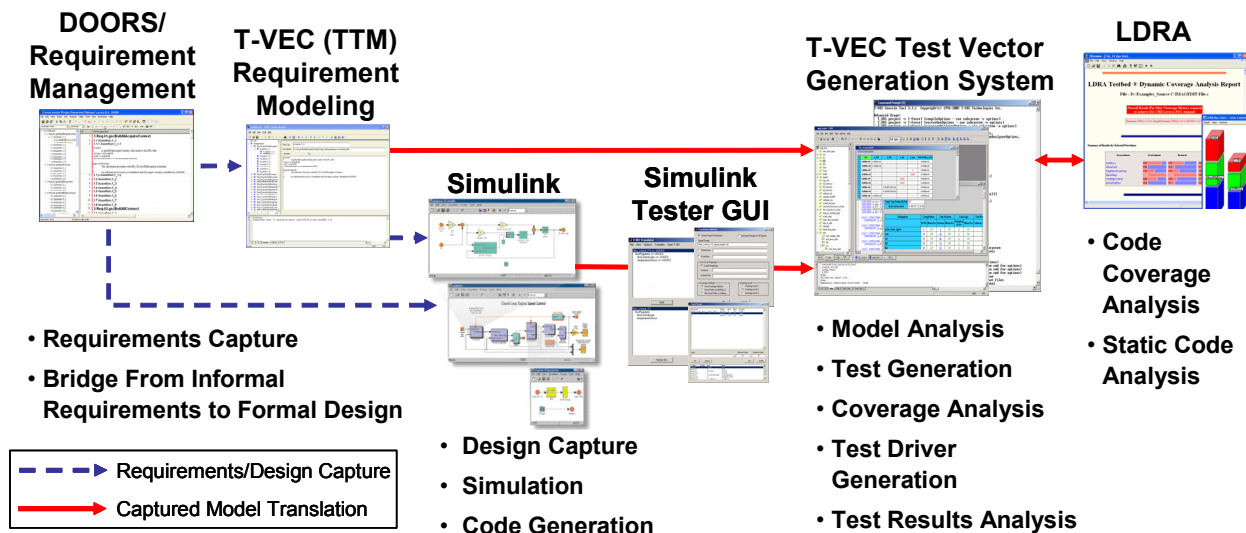


図1. T-VEC モデルレベルテスト自動化ツールと各種ツールの統合

T-VEC のコアであるテストベクタ生成システムは、TTM にモデル化された要求仕様やデザインモデル(Simulink/Stateflow)を、独自の階層的 Disjunctive Normal Form(DNF)に変換し、この形式に於ける各機能要求（入出力間の振舞い）の入力域に対するコンストレインツは Domain Conversion Path (DCP)として抽出されます。このパスに対し、テストベクタ生成システムは、上流の制約を受けて伝播されてくる入力範囲で期待出力との組合せを生成します。ここで、テストベクタを生成できない DCP は、モデル上の矛盾として検出されます。また、このテストベクタ生成機能は、フロート、ダブルなど各種データ型、リニア/ノンリニア式に対応しているため、矛盾無く生成されたテストベクタは、実システムに対する入力と期待値としてテストに用いられ、モデルに対するコードの一致性の検証が行うことができます。

またテストの動的コードカバレッジ解析 (LDRA 社 Testbed) により、モデルに存在していないコードを検証します。

TTM 要求仕様をフォーマルにモデル化するツール :

T-VEC Tabular Modeler (TTM)は、要求仕様を表形式の GUI を用いてフォーマルにモデル化するフロントエンドツールです。この要求モデルをテストベクタ生成システムでモデル検証し、要求仕様に基づいたテストベクタ生成、実行、結果判定を行います。この TTM は、DOORS®要求管理ツールと統合され要求項目とテストの完全なトレーサビリティを取る。テストで問題が発生すれば、テストベクタ、モデル、要求項目へとトレースバックして解析されます。DOORS に含まれていない要求項目も、TTM に直接モデル化することで同様に管理されます。

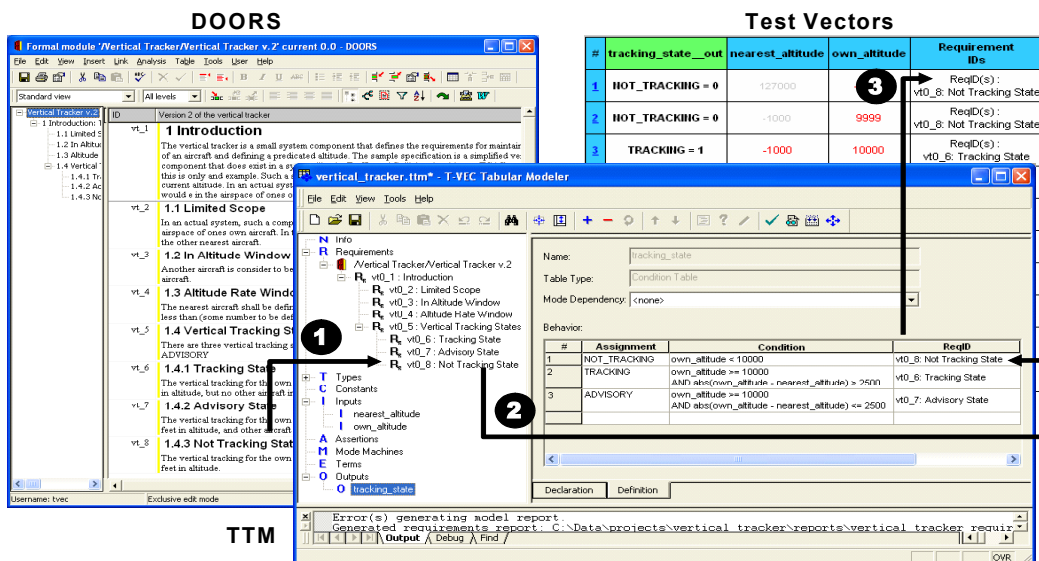


図 2. 要求項目と、要求モデル、テストベクタとのリンク

T-VEC Simulink® テスター :

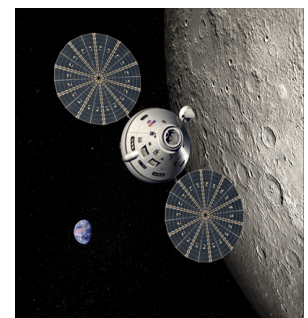
Simulink/Stateflow モデルをテストベクタ生成システムで検証し、テストベクタ生成、実行、結果判定を行います。モデルから自動生成されるソースコードに対するテストドライバーも自動生成されます。さらに、制御系システムで一般的なタイムディレイやインテグレータなどの動的振舞いに対応したテストシーケンスベクタも生成します。また、これらのテストも TTM と同様に要求項目とのトレーサビリティを取る為に統合されます。モデルから自動生成されるソースコードに対しては、MISRA スタンドアードチェックやデータフロー、実行フローの静的解析が LDRA 社ツールで行われ、動的なテストのカバレッジとグラフィカルに融合され評価されます。

T-VEC バックグラウンド :

T-VEC ツールのコアは1980年代後半に開発され FAA で求められる要求仕様ベースのテストで、その実用性が実証されています。例えばテストはコードレベルの MCDC カバレッジを達成することが LDRA 社 Testbed などにより確認され DO178B の認証取得にも役立てられています。最近では、United Kingdom's Ministry of Defence (MoD) により採用を推奨されました。航空宇宙以外でも、医用、通信、データベースセキュリティ機能や US NIST のスマートカードのモデル化と検証など多くの実績が有ります。T-VEC のメンバーは、現在 DO178C のモデルベース開発に於ける V&V に関するサブグループでも活躍しています。

T-VEC の全ての機能は手作業に頼った検証およびテスト (エラーを起こし易い) を全プロセスに於いて自動化し、開発期間や保守費用、タイム to マーケットを削減し、かつ製品の品質を向上します。またテストドライバーは殆どの言語 (C, C++, Java, Ada, Perl, PL/I, SQL) への実績が有り、独自言語やテスト環境への柔軟な対応も可能であり、幅広いアプリケーション領域で採用されている実践的な形式的手法・検証ツールです。

次期有人宇宙船 CEV (Project Orion) の主契約企業であるロッキードマーチン社は、このプロジェクトに T-VEC の TTM 要求仕様モデルと Simulink のモデル検証機能をサブコントラクターも含めて採用することを表明している。



ツールのデモンストレーションを行っています。

ご興味いただける場合は、お手数ですが下記までご依頼頂けると幸いです。



富士設備工業株式会社 電子機器事業部
〒591-8025 大阪府堺市北区長曾根町1928-1
Tel: 072-252-2128 www.fuji-setsu.co.jp