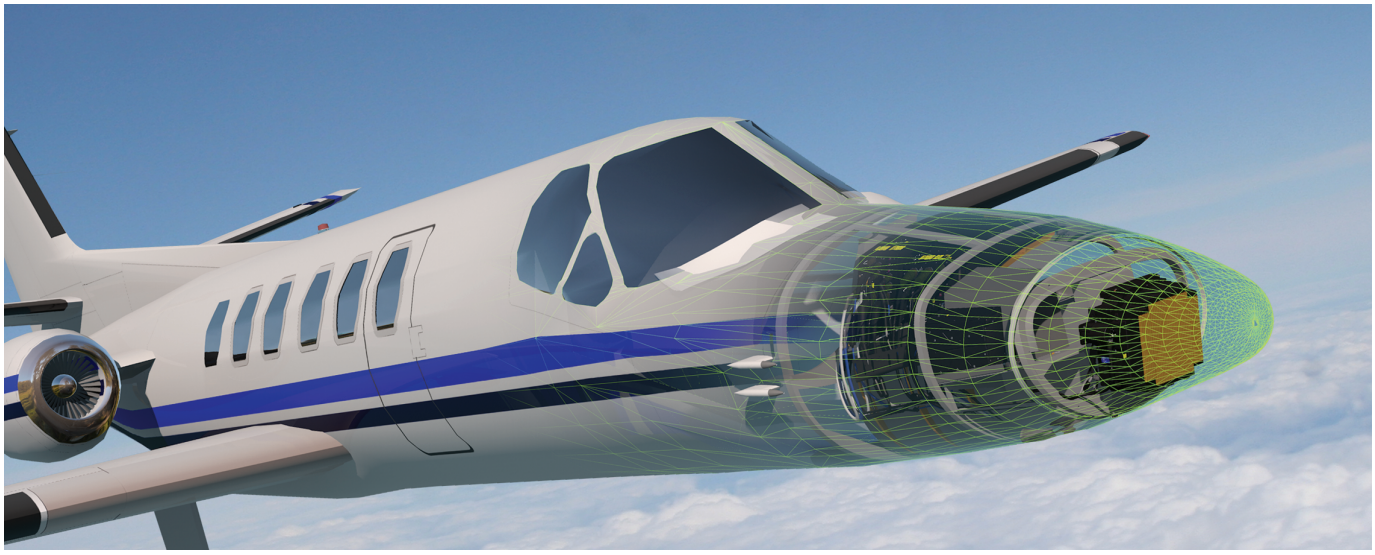
PRQA Programming Research

Case Study

静的解析 -- 手書きコードと自動生成コード



静的コード解析の用途を手書きコードの欠陥検出だけに限定する必要はありません。PRQAは、長年の顧客であるセレックスES社と共に、彼らのQA·C++ソースコード解析ソリューションとIBM Rational Rhapsodyシステムモデリング環境(自動生成コード)を統合し、コード品質の改善、開発時間の短縮、そしてはるかに効果的で堅牢なソフトウェア開発作業フローを実現しました。

1. 手書きコード

フィンメッカニカグループ傘下のセレックスES社は、イギリスBasildonでQA·Cの展開を開始した2001年からPRQAの静的解析ソリューションを利用しています。

その4年後、セレックスES社はベストプラクティスを目指し、ギャップとオポチュニティを識別して生産性を高めるために、ツールチェーン全体の大規模な再評価を開始しました。商用のコード解析ツールの厳格な評価において、以下の重要な要件が提示されました。

- 欠陥と危険な言語の用法を検出すること
- (MISRAベースのコーディング規約に対する)コーディング規約への準拠を確実に判定すること
- ツールの誤検出(ノイズ)を最小限に留めること
- スタイルチェックを行えること (例: 第三者がコードを使用しやすくするための命名規約および物理的なレイアウト)
- ファントムインスペクション　(ツールにより開発者から他の開発者の欠陥が見えるようにし、ベストプラクティスの適用を促進すること)
- メトリクスレポート (コードの改善を支援するための分析手段を提供すること)

Selex ES
A Finmeccanica Company

要約

- 航空宇宙産業および軍需産業
- 2001年以来QA·C/QA·C++を広く採用し、手書きコードの解析において非常に効率的であることを実証済み
- MISRAベースのコーディング規約(MISRAルールのサブセットに加えて会社独自の拡張規約を使用)
- 重要な戦略的イニシアチブとして認識されている"Rhapsodyおよび自動生成コード"と"QA·C/QA·C++"の連携は現在、独自に自動生成コードの品質を検証するための効果的で実践的な方法を提供する

コーディングベストプラクティスおよびコーディング規約

セレックスES社は、堅牢なコードの開発におけるコーディング規約の重要性を認識し、会社独自の拡張規約に加えてMISRAルールのサブセットを選択しました。この規約は元々自動車産業のために作成されましたが、このルールセットは世界トップレベルのコーディング専門家による研究の産物であり、他の多くの産業に対しても等しく(そして幅広く)適しており、特にミッションクリティカルかつセーフティークリティカルなソリューションを展開しているものに対して適しています。セレックスES社に関して言えば、MISRAガイドラインはコーディング規約のアプリケーション固有および会社固有セットの理想的な出発点として機能しました。

またセレックスES社は、以下の表で示されるようにソフトウェア開発プロセスの異なる段階における異なる利害関係者の成果物のニーズを考慮しました。

フェーズ	目的	役割
設計＆実装	進行中のサニティーチェックの提供 未熟なエンジニアの支援 欠陥リークを最小限に抑える	開発者
テスト	動的テスト前に生成されたコードの自動検査の提供	テスター
承認	作業成果物/SCR(ソフトウェア変更要求)完了のために必須	設計権限者
リリース	成果物のベースラインのために必須	QA

そしてこの評価を踏まえた結果、2007年にQA•C/QA•C++を会社全体で採用する決定をしました、そしてこのツールはエディンバラ、ルートンそしてイタリアの他のセレックスES社サイトに続けて展開されました。センサー・データ・プロセッシング・ソリューションのソフトウェアエンジニアリング責任者であるIan Anderson氏は、**「この決定は容易でした、QA•C/QA•C++は私たちの開発チームでは既に広く採用されており、非常に効率的に提供される手書きコードの自動解析については既に実証済みでしたから。」**と語りました。

それ以降の数年間で、セレックスES社のピアレビューの重点はかなり変化しています。詳細に渡るコードのウォークスルーの必要性を取り除き、レビューアはコードが設計通りに動くかどうかに集中できるようになりました。その結果として、レビューアの知識や能力に頼るマニュアルコードレビューよりもはるかに一貫性があり効率的になりました。また、セレックスES社では、QA•C/QA•C++がコードの品質を向上し、単体テストに達する前に多くの欠陥を取り除いたことで、動的テストがより早く、より簡単に実施できるようになり、その結果、手戻りの発生を最小限に抑えられるようになりました。さらに、コードはスタイルに一貫性を持たせることで、はるかに管理しやすくなりました。

2. モデル駆動開発

セレックスES社の重要な戦略的イニシアチブの1つは、IBM Rational Rhapsodyに基づくモデル駆動設計(MDD)の採用を増やすことでした。開発プロセス全体の迅速化と同様に、プロジェクトを跨る自動生成コードの再利用を重要な目的の一つとして挙げています。

セレックスES社は、UMLモデルから得られた自動生成コードが標準的なプロジェクトにおけるコードベースの60-80%を占めることを発見しました。残りの20-40%はコードインサートを用いて、手書きで記述する必要があり(通常、C++を使用)、この２種類のコードが、両者を組み合わせたモデルから生成される１つの共通コードベース内に混在します。

図1aと1bはモデル内のコードと生成されたコードの関係性を示しています:

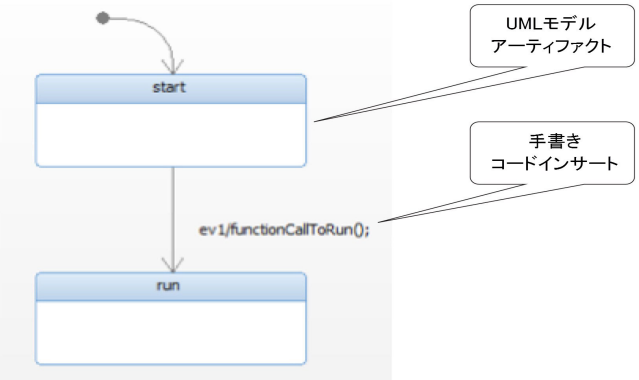


図 1a: モデル内状態図

```
IOxfReactive::TakeEventStatus class_1::rootState_processEvent() {
    IOxfReactive::TakeEventStatus res = eventNotConsumed;
    switch (rootState_active) {
        // State start
        case start:
        {
            if(IS_EVENT_TYPE_OF(ev1_Default_id))
                {
                    //#[ transition 1
                    functionCallToRun();
                    //#]
                    rootState_subState = run;
                    rootState_active = run;
                    res = eventConsumed;
                }

        }
        break;
```

モデルアーティファクトから得られたコード

コードインサート

図 1b: モデルから生成されたステート･マシン･コード

Rhapsodyのモデル生成コードは広範囲に及ぶ産業に適用できます、そしてこれは15年以上にわたり約40のライブプロジェクトで使用され、セレックスES社ではこのコードの堅牢性により高いレベルの信頼性を確立しています。

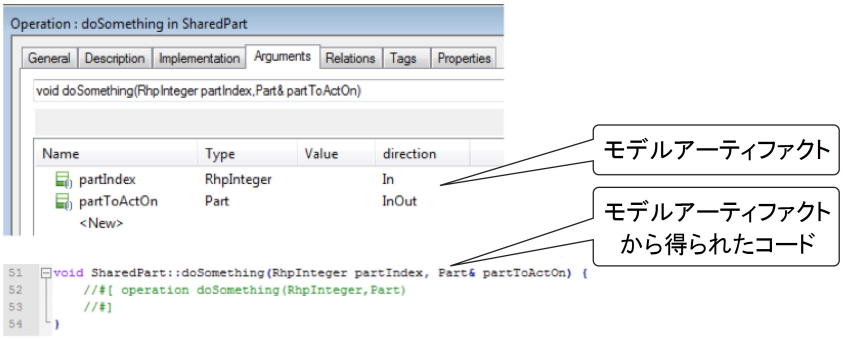
当初、手書きコードの検査では個別の検証が必要でしたが、これにはスケーラビリティ、速度、解析の一貫性、および全体的なリソースの面で大規模な問題が生じました。QA•C/QA•C++は、既に手書きコードに対する非常に効率的な検証ソリューションをセレックスES社に提供していました。ここでの挑戦はRhapsody環境において、これを十分に活用する方法を見つけることでした。この問題の要点は、2種類のコードを区別することでした:

a) UMLモデルアーティファクトから得た自動生成コード:

このタイプのコードにおけるセレックスES社のアプローチは「オブジェクト指向」です。テストの焦点は。機能性に向けられました。また、その大部分はカバレッジ測定を用いた要件ベースまたは設計ベースのテストに注がれました。このアプローチを支えるのは、次の3つの要素です。モデル生成コードは、モデル変換およびコード作成プロセス固有の制限があるため、言語の使用においてより厳重な制約があります。また、レガシーコードの考察に類似しますが、自動生成コードは過去の使用法を通じて現場で既に実証されています。したがって実際の使用から得た高い信頼性のある検証を提供します。最後に、開発者はモデル生成コードを変更できません、モデル自体の変更のみ可能です。

b) 手書きコードインサートと開発者が管理可能なモデルアーティファクトから得た自動生成コード:

コードインサートは本質的には手書きで作成されたコードです。Rhapsodyがモデルアーティファクトから自動生成したコードと連携します。開発者が管理可能なモデルアーティファクトには、Rhapsody　GUIでの制御が可能な関数プロトタイプであるといった側面があります。この両者とも、ベストプラクティスとコーディング規約との準拠を確実に判定するため、他のあらゆる手書き生成コードと同様に十分な精査が行われなければなりません。このコードの修正は開発者の責任となるため、静的コード解析がソフトウェア開発作業フローにシームレスに適合しなければなりません。



Rhapsody及びQA•C/QA•C++

PRQAとセレックスES社との共同ワークショップで、RhapsodyとQA•C/QA•C++の連携に必要な数多くの重要な要素を発見しました、その概要は:

- 開発者が自己責任範囲内のコード、すなわち手書きコード及びコードに類似したモデルアーティファクト（例: 関数パラメータータイプ）に対する配慮を認識し、それに集中できるようにします。つまり、QA•C/QA•C++がモデルアーティファクトから自動生成されるコードに対して検出される静的コード解析の診断結果を識別し、抑止できなければなりません。
- Rhapsodyベースのソフトウェア開発作業フローにシームレスに適合させた形でQA•C/QA•C++を使用できるようにする。具体的には:
  - 全てのQA•C/QA•C++の機能が動作する
  - Rhapsody IDEからの静的コード解析を容易に実施できる
  - 個々のコード変更に効果的に集中し、分析できるようにする

この成果として、RhapsodyとQA•C/QA•C++の連携が実現し、その後すべてのセレックスES社Rhapsodyプロジェクトに展開されました。

より技術的なレベルでの連携

セレックスES社は、マイクロソフトMSVC++コンパイラおよびGNUとDIABコンパイラを有するWind River VxWorks RTOSを使用しています。これらの連携では、全てのアプリケーションが問題なく動作します。セレックスES社では'IDE'としてRhapsodyを使用するため、コードインサートは直接Rhapsodyに入力され、モデルファイルとして保存・設定されます。手書きコードを含むソースファイルはありません。エンジニアはモデルだけで作業を行います、自動生成されたC++ファイルはオブジェクトコードのように実行モジュールに組み込まれるアーティファクトの一つに過ぎません。セレックスES社はモデル駆動開発を採用しています。モデルがレポジトリで保存される必要のある唯一の項目です。必要なコードはすべてモデルから自動生成することができます。

Rhapsodyでモデルを作成した後に、Rhapsodyから実行される連携処理により、自動生成されたC++ファイルと必要な解析設定を含むQA・C++プロジェクトが生成されます。QA•C++　GUIは自動的にプロジェクトを起動・ロードして解析の準備を整えます。開発者は解析するファイルを選択でき、解析によってコードの問題点を記した診断結果を得ることができます。

QA•C++は1300以上の診断メッセージを備えており、MISRAルールでグループ分けされます (MISRAを使用していない場合は、重要度によって９レベルにグループ分けされます)。

解析後のメッセージはメッセージブラウザに表示されます。メッセージブラウザでは、メッセージが重要度に応じてグループに分けされるため、重要度の低い問題 (例: コードレイアウト) の中から最重要問題 (例: 未定義の動作) を検出しやすくなっています。各ファイル、各メッセージまたはグループごとに診断結果を確認できます。診断結果は、診断対象のソースコードと診断結果のメッセージを合わせた形で提示されます。診断結果のメッセージは、HTML形式のヘルプを含みます。

モデルアーティファクトに関する診断結果は初期設定では表示されません(非表示状態になっています)が、任意で表示可能です。その他全ての診断結果のレビューでは、開発者がRhapsody IDE内でコードインサートを修正して問題を解決できます。Rhapsodyで再生成し、QA•C++で再解析を行うと、モデル修正によって問題が取り除かれ、他の問題にもさらされていないことが即座に確認できます。

まとめ

セレックスES社では10年以上にわたり、手書きコードの自動解析にQA•C/QA•C++を使用しています。

モデルベース設計の戦略的採用により、彼らはQA•C/QA•C++の実証済の利点がRhapsody環境で確実に継続して活用されることを強く望んでいました。これに対するソリューションとして、自動生成コード内の2つの異なるカテゴリ(手書きインサートからのコードとUMLモデルアーティファクトからのコード)の便宜を図る必要があるという事実を認識しました。PRQAがセレックスES社へ提供した連携ソリューションは:

- 開発者の自己責任範囲であり、直接編集できる手書きのコードインサートを認識し、集中できるようにすること
- QA•C/QA•C++の解析がRhapsodyベースのソフトウェア開発作業フローにシームレスに適合できるようにすること

「Rhapsodyと自動生成コードの採用はセレックスES社にとって重要かつ戦略的なイニシアチブでした。」とIan Anderson氏は語りました、「QA•CとQA•C++は私たちの開発チームでは既に広く採用されており、手書き生成コードの解析については非常に効率的であることが既に実証済みでした。この連携は我々にとって非常に重要であり、PRQAは自動生成コードの品質を個別に検証するための効率的かつ実践的な方法を提供してくれました。」

Selex ES
A Finmeccanica Company

セレックスES社(フィンメッカニカ社傘下)は、防衛、航空宇宙、宇宙、セキュリティ、高信頼性監視、ネットワークマネージメント、情報セキュリティおよびミッションエッセンシャルサービスにおけるエレクトロニックおよび情報ソリューションの国際的なリーダーです。

様々な分野や領域において数多くの経験を持つハイテクシステムおよびセンサーの世界的リーダーとして、セレックスES社は最上級のソリューションを必要とするお客様のあらゆるニーズに対応できます。

航空宇宙および防衛エレクトロニクスの分野において、セレックスES社は戦術的ISTARシステム、C4Iインフラストラクチャ、電子軍事機器、状況認識のためのミッションクリティカルシステム、自己防衛、広域監視、情報配信の設計および開発の経験があります。

セレックスES社は、セキュリティ、ルートマネジメント、ミッションクリティカルサービスセクターに対応したものと同等のテクノロジーとスキルを提供します。これには航空および海上交通の制御とモニタリング、グリーンアンドブルーボーダーの監視および防衛、堅牢なサイバーセキュリティー、通信ネットワークの保護、複雑なインフラストラクチャ管理のための「スマート」ソリューションの配置、「システムのためのシステム」が含まれます'。

イタリアとイギリスにおける主要国内業務および本社と並行し、セレックスES社はアメリカ、ドイツ、トルコ、ルーマニア、ブラジル、サウジアラビア、インド、アラブ首長国連邦に産業および商業拠点を設立しています。17000人以上の従業員と35億ユーロを超える総収益により、セレックスES社はより安心、スマート、安全な社会のためのソリューションを提供しお客様とパートナーからの信頼を得ています。**www.selex-es.com**

お問い合わせ

PRQAのソリューションに関する詳細は、お近くの営業担当者または下記メールアドレスまでご連絡ください:
info@programmingresearch.com