

OneSpin Solutions Customer Success

Infineon プロトコル プロセッサ

➤ 360 MVの使用によりエラーのない機能動作の達成と40%の検証工数削減に成功

ユーザープロフィール

ドイツ Infineon 社の Communication Solutions 事業部 (COM) の Intellectual Property & Reuse 部門 (IPR) は COM の世界中の製品グループに対して社内製およびサードパーティ製の IP コンポーネントを供給しています。タイム トウマーケットおよび利益率目標を達成するために、IPR は包括的な IP 再利用戦略を適用しています。IPR は一回目で設計を成功させるための機能動作と、IP の早期収益化を確保しなければなりません。そのため、IPR の必須検証手順には高度なテストベンチ自動化とフォーマル検証が組み込まれています。

ビジネス上の課題

IPR はデジタル加入者回線 (DSL) からルータまで幅広いアプリケーションに対応した COM の固定網向け各種チップの厳しいスループット要件を満たすためネットワークプロセッサ PPv2 を開発しました。IPR は両立することの難しい 3 つの問題を最適に解決しなければなりませんでした：

- 幅広いアプリケーションに対してコスト効率よく、リスクのない再利用を保証する。
- ハードウェアとソフトウェアの両方でエラーのない機能動作を実現するために必要な最高の品質を提供する。
- 幅広い再利用を前提として設計されていなかった PPv2 の前モデルと同等の R&D 工数に抑える。

検証目標

PPv2 はコンパクト、高性能かつ構成変更可能な 32 ビット RISC プロセッサであり、アプリケーション専用の 40 個の命令セットと 7 ステージパイプラインを備え、粒度の細かいマルチスレッド処理を特徴としています。この開発は、以前のプロトコルプロセッサ PPv1 の設計を流用したものでしたが、大幅な変更が必要であったために実質的には一からの設計に近いものとなりました。検証課題には以下がありました：

- 複数の命令が正しくパイプライン処理され、命令間に望ましくない干渉がないこと、またトラップや割り込み等の許容される (しかし予測不可能な) 動作の正しい処理を保証すること。
- パイプライン処理と関連した転送およびストール動作のソフトウェア プログラマに対する透明性を保証すること

- 複雑なビット操作を行うデータパスを包括的に検証すること。
- 許容できるレイテンシ内のトラップおよび割り込み実行等難しいリアルタイム要件を満足すること。
- あらゆる命令、スレッド切り替え、許容できる (しかし予測不可能な) 動作の組み合わせにおいて、複数のスレッドが独立して実行可能であることを保証すること。
- PPv2 が統合される可能性のあるすべてのハードウェア/ソフトウェア環境の統合要件を正確に記述すること。

検証戦略

検証対象となる動作は、プロセッサのハイレベルなトランザクションです。IPR は、RTL シミュレーションおよび RTL ベースの検証ツールを使って PPv2 のハードウェア/ソフトウェア動作状態を表現し、細かなパイプライン処理等の複雑なトランザクションをあらゆるコンフィギュレーションおよびコンテキスト切り替えの組み合わせに対して検証することは不可能であると考えました。さらに IPR は、RTL 検証アプローチがバックアップ戦略としてさえも現実的でないという結論に達しました。その結果、IPR にはトランザクションレベルで動作し、信頼の置けるフォーマル検証ソリューションが必要になりました。Infineon は既に OneSpin の技術を使って、これよりさらに大規模なスーパーカラー型の自動車アプリケーション向け 32 ビットプロセッサを検証し、プログラマのモデルに完全に準拠していることの証明に成功していました。その結果、IPR は PPv2 の検証に OneSpin の 360 Module Verifier (360 MV) を採用しました。

「OneSpin の技術を使うことにより、高度なコンテキスト切り替えを含む PPv2 プロトコル プロセッサを完全に検証することができました。この IP は弊社の通信アプリケーションの中核をなす IP コンポーネントです。この検証アプローチでは、PPv2 の完全な機能がカバーされていること、バグの抜け道がふさがれていることを確認することができました。さらに、開発人月をこれまでのシミュレーション ベースのプロジェクトと比較して約 40% 削減することができました。」

Alexander Haggemiller 氏
Director of the Intellectual Property & Reuse
Department Infineon Technologies

検証アプローチ

PPv2の仕様では、プログラムアドレス、レジスタファイル、ステータスフラグ等、プログラマから見えるレジスタを命令がどのように変更するか、命令およびデータに対するメモリアccess、そして許容できる(しかし予測不可能な)動作に対する望ましい応答が定義されていました。

各命令に対して、開発チームは命令がパイプラインをどのように通過していくか、実装上の信号およびレジスタにどう影響するかを記述するプロパティを開発しました。次いで、実装上のレジスタと仕様上のレジスタ間の整合性をチェックするため、これらに関連づけるプロパティのハイレベルビューを開発しました。これは重要な作業でした。命令により計算された結果は通常、格納されるまえにパイプラインを通り、予測できない転送やストールの影響を受ける場合があるからです。

その後、360 MVのプロパティチェッカを使ってプロパティおよび関連するVHDLコードのデバッグを行いました。数秒の内に、チェッカはカウンタシーケンスの診断結果波形を生成しました。その後、360 MVのデバッガを使ってプロパティ階層をナビゲートし、反例を説明する自動的にハイライトされた抽象的な変数および信号を確認しました。

解析対象となった複雑な動作の例としては、静的なパラメータにより最大4個までの遅延スロットの実行が設定される分岐命令の動作などがあります。割り込みを受信すると、これらのスロットはまず格納してから、割り込み後に実行されなければなりません。このシーケンスを様々なアプリケーションにおいて正しく動作させなければなりません。360 MVを使用することにより、これらのスロットが一部しか実行されないコンフィギュレーションが検出されました。これに基づいてVHDL記述が修正され、仕様に含まれる曖昧性と間違いが取り除かれました。

もうひとつの例としてはプロパティに含まれる「穴」があります。360MVを使用することにより、開発チームはコンテキスト切り替えバッファに格納されている間に命令ワードが変更されるケースを発見しました。この希な現象は仕様では考慮されていませんでした。この問題はシミュレーションベースの検証ではほぼ間違いなく見逃されていたと思われます。

すべてのプロパティが証明されると、プロパティにより記述された動作の仕様に対する準拠が確認されました。その後、360 MVの完全性自動解析を使ってPPv2のあらゆる可能な動作がこれらのプロパティに記述されていることが確認されました。

結果

IPRは360 Module Verifierを使って、PPv2に対して“True Functional Sign-Off”を達成しました。プロジェクトは設定されていた目標をすべて達成しました。360 MVフォーマル検証およびデバッグ手法により以下を達成しました：

- あらゆるコンフィギュレーションに対してPPv2全体でエラーのない機能動作
- 正しいPPv2の動作を3つの統合条件を満足するハードウェア/ソフトウェア環境で達成
- これらすべてを4人月で実現し、検証工数をPPv1と比較して約40%削減

またこの検証は、多数の曖昧性や特定されていない状況を含む130ページの仕様にもとづいて行われたものであり、シミュレーションの行われていない、新規開発のVHDLコード11,000行が含まれていました。360 MVを使うことにより、チームは以下の成果を上げました：

- PPv2アーキテクチャに対する完全な理解を得るとともに、正確な統合条件を生成
- 仕様の変更と、コンテキスト切り替えロジックの変更を必要とする10件の深刻なエラーおよび17件の問題を発見
- VHDLが仕様を正しく実装しており、機能の見落としがないことを確認
- PPv2のサイクル精度の動作を曖昧性なく記述した38個の証明済みプロパティを、読みやすい40ページの文書として生成
- 純粋な副産物として、VHDLに対してシーケンシャルに等価なことが証明されているトランザクションレベルモデルの形でのフォーマルな、実行形式のプログラマービューを生成

さらに、検証インフラは標準的なワークステーション1台と360 MVのライセンス1本のみでした。プロパティセット全体をこのワークステーションを使って1晩で処理でき、コード変更を短時間に検証することができました。

結論

OneSpinの技術は、プロトコルプロセッサPPv2のエラーのない機能動作を保証し、ターゲットとなるハードウェア/ソフトウェア環境での動作を正確に予測し、仕様の間違いと漏れを検出し、その結果True Functional Sign-Offを実現しました。またこの技術により検証工数を40%削減し、正確に定義された統合条件を生成することによりチップレベル機能検証の負担を軽減しました。

PPv2のようなIPにおいて、360 MVはIPプロバイダおよびIPインテグレータのニーズに対して理想的な製品です。