OneSpin® 360 信頼性とセキュリティソリューション

自動化された IC 信頼性保証およびセキュリティ検証

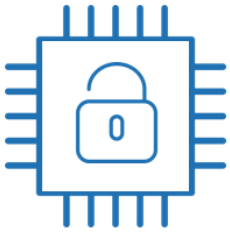
特長

- 悪意および意図しない脆弱性の両方を検知する独自の包括的アプリケーション
- 自動化された信頼性評価および一般的な脆弱性の検知のための使いやすいアプリケーション
- 網羅的なセキュリティ検証および信頼性保証のための高度なアプリケーション
- **RISC-V** コア等特定 IP 向けのアプリケーション
- 専用 ISA コア等、特定のデザインファミリー用にカスタマイズ可能

敵対者の攻撃からハードウェアを守る

エレクトロニクスシステムは秘密情報を抜き取るまたは機能を侵害することを目的とした敵対的攻撃の標的となります。これまでは、セキュリティ侵害の原因はソフトウェアの脆弱性やバグでした。しかし現在は、半導体 IP や IC も大きなリスク懸念となっています。

不十分なアーキテクチャ設計、予期していなかった不正な使い方、あるいは設計段階でのエラーによって生じた**ハードウェアセキュリティの脆弱性**はシステムをさまざまな物理的、論理的、そしてソフトウェアベースの攻撃に晒すことが明らかになっています。ハードウェアの複雑性が指数関数的に高まる中で、機能検証はコーナーケースのバグを見逃すことがしばしばです。高度かつ厳密な検証プロセスであっても、それらは意図したユースケースのみにフォーカスしたものです。ところが、敵対者は目的のハードウェアアプリケーションには関係のない不正な使い方を用いて、結果的にセキュリティを侵害します。



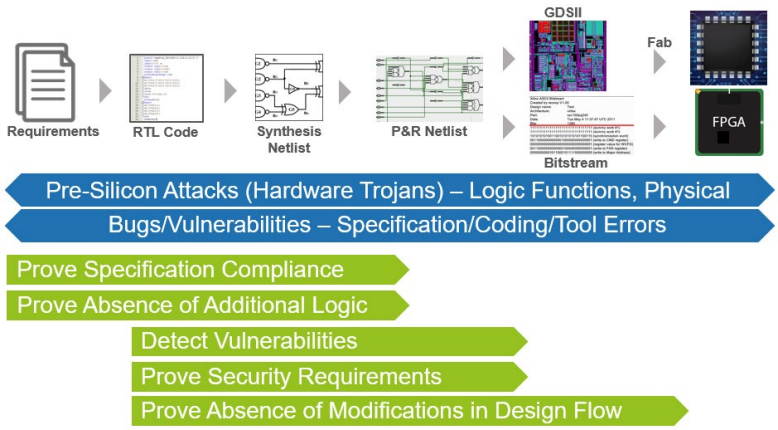
- Denial of Service
- Side Channels
- Privileges Escalation
- Kill Switches
- Hardware Backdoors
- Hardware Trojans
- Secret Data Integrity/Confidentiality

悪意ある**故障注入**は特定の、重要なメモリやレジスタビットに格納された値を反転することによりある程度コントロールすることができます。事実、悪意ある故障の注入は、ハードウェアの動作を混乱させセキュリティ機能を無効にする強力な方法であることが実証されています。

ハードウェアトロイの組み込みや独立した信頼性評価ステップをパスしていないサードパーティ製 IP の統合によりもたらされる、悪意あるロジックもまた重要な懸念事項です。ハードウェアトロイはステルス性が注意深く設計され、攻撃者のみが知る非常に稀な条件でのみアクティブ化します。このため、それらを従来の検証フローで検知することは非常に困難です。

HRoT（Hardware root of trust）やセキュアエンクレーブは強力なセキュリティ機能を提供するもので、多くのセキュリティ/セーフティクリティカルなシステムに欠かせない存在です。しかし、HRoT もシステムのその他の部分のどちらに対しても、脆弱性が存在しないことを証明するには厳密なセキュリティおよび信頼性検証が必要です。エンジニアは IP および IC に対する信頼性保証およびセキュリティ検証に対するホリスティックかつ効率的なアプローチを必要としています。

OneSpin® 360 信頼性とセキュリティソリューション



複数の保証レベルをサポートする包括的なアプリケーションセット

OneSpin の信頼性とセキュリティソリューションは、長年の実績ある OneSpin の **IC インテグリティ**のための機能正確性および安全性ソリューションを補完するソリューションです。このソリューションはインテリジェントな設計構造解析、ドメイン特有のデータおよび専門知識、そして高度な専用フォーマルエンジンを駆使しています。これらは複雑な SoC に脆弱なロジックが存在しないことを証明する上で極めて重要であり、これを従来のシミュレーションやエミュレーションアプローチでは達成することはできません。

秘密情報の秘匿性（データ漏洩防止）と完全性（データが毀損されないこと） は**セキュアパス検証**テクノロジによって検証可能であり、これは複雑なインターコネクトを含む大規模な SoC にも適用できます。このアプローチはメモリマップ、アドレスデコーディング、ペリフェラル設定に含まれる意図しないエラーや悪意あるエラー、あるいは重要なレジスタや保護されたメモリ領域への不正なリード/ライトアクセスを検知します。チェックは故障注入シナリオで行うことができますが、**Fault Contribution Analysis** を使って悪意ある故障の解析をシンプルに行うこともできます。

OneSpin の EC-ASIC™ ならびに EC-FPGA™ はフォーマル等価性チェック（EC）を使用して RTL またはゲートレベルの 2 つの設計を比較します。これにより、設計の変換の過程でトロイや悪意あるロジックが挿入されていないことを確認することができます。

OneSpin 360 DV RISC-V Verification App は機能的バグおよび悪意あるロジックが存在しないことを確認する非有界証明を提供します。このアプリケーションはオープンソース Rocket Core への適用により、文書化されていないカスタム命令や複数のコーナーケースバグを検知することに成功しています。参考文献："Complete Formal Verification of RISC V Processor IPs for Trojan-Free Trusted ICs”（GOMACTech 2019 カンファレンス）OneSpin の **GapFreeVerification™** 完全性検証技術を使用することにより、専用 ISA コアやその他のクリティカルな IP に対しても同様のアプリケーションを作成し、設計が仕様以外のことを何も実行しないことを証明することが可能です。

オプションのカスタマイズおよび導入サービス

OneSpin は信頼性の高いセキュアなハードウェア開発フローを導入したい組織をサポートするエキスパートサービスを提供します。ソリューションをカスタマイズすることにより適切な証拠を生成し、最小限の手間で特定のセキュリティ要件および保証要件を満たすと同時に、既存のフローとの統合も行うことができます。

連絡先 · info@onespin.com · www.onespin.com

USA: +1 408 734 1900 · Europe: +49 89 99013-0 · 日本: (045) 285 1573

2021-01 V. 3