脅威の増加に伴い、ハードウェア・セキュリティへのダイナミック・トラスト・アプローチに対する要求が増大

ラティスセミコンダクター ホワイトペーパー

2020年8月

詳細：

www.latticesemi.com

コンタクト：

www.latticesemi.com/contact
www.latticesemi.com/buy

V. 2 WP0025J

目次

ダイナミック・トラストへのニーズ

多くの市場で使用される電子製品の設計に携わる開発者にとって、ファームウェアへの攻撃から製品を保護することが重要な課題になっています。米国のNational Vulnerability Databaseによれば、2016年から2019年の間にファームウェアの脆弱性の件数が700%超の増加を示しており[注1]、業界アナリストのガートナーは2022年までに「ファームウェアの適切なアップグレード計画を持たない組織の70%が、ファームウェアの脆弱性によりセキュリティを侵害される可能性がある」と報告しています[注2]。

こうした脆弱性は、現場で使用される最終製品を危険にさらすだけではありません。最初のコンポーネント製造時点から製造委託業者への出荷、システム組み立てに至るまでの、急速に変化し予測不能性を増しているグローバルなエレクトロニクス・サプライチェーンで、さらには現場での全製品寿命にわたって、個々のコンポーネントに影響を及ぼす可能性があります。脆弱性は悪意のある行為者に悪用され、結果的にデータ盗難、データ破損、トロイの木馬やマルウェアの挿入、機器のハイジャック、複製、設計盗難などのさまざまなセキュリティの問題を発生させる可能性があります。プラットフォーム・ファームウェアへの攻撃が成功すると、システムは恐らく恒久的に運用不可能になるか、身代金、データ盗難、ハッキングなどの危険にさらされることがあります。このような弱点に対する攻撃はオペレーティング・システムより下位のレベルへ行われることから、損害が生じる前に検出することは不可能です。こうした攻撃は企業の業績や評判に多大な影響を与える可能性があります。

電子システムのハードウェアを不正アクセスから保護することは今に始まった問題ではなく、不正なユーザーによるコンポーネント・ファームウェアへのアクセスを防止するソリューションがすでに存在しています。しかし、これらのソリューションは一般的にフォン・ノイマン・アーキテクチャ・マイクロコントローラ（MCU）を使用しており、このMCUは多くの場合、複数のデバイスが攻撃された際の対応に必要なリアルタイム性能を備えていません。本質的に並列プロセッシングを行うFPGAは、複数デバイスのモニタリング、保護、復元をナノ秒の応答時間で同時に実行することができます。

現在最も優れたTPMやオペレーティング・システム・セキュリティ・ソリューションを使用しても、システム・ファームウェアはシステムの製造前、製造中、製造後に攻撃される可能性があります。さらに、システム・コンポーネントは通常、オペレーティング・システムやソフトウェア・ベース・セキュリティ・ソリューション（起動後バリデーション・チェックなど）が運用可能になる前にファームウェアをローディングすることから、不正なファームウェアの検出は困難になります。不正なファームウェアはスタティックな起動後整合性チェックから自身をクローキングし、セキュリティやマルウェアのスキャンから不可視化します。

新たな脅威が進化する中で電子システムは変化と対応を迫られており、侵害されたファームウェアが検出された際に適切なアクションを自動的に実行することが求められています。システム・ファームウェアの保護のために、セキュリティ・ソリューションには「ダイナミック・トラスト」が必要です。すなわち、コンポーネントのサプライチェーン全体にわたる、最初の製品アセンブリから最終製品の出荷、組み立て、製品の全動作寿命に至るまでのシステムの全ライフサイクルにわたって包括的なファームウェア保護を提供しリアルタイムな並列処理を行う素早いソリューションをベースとした、ファームウェア攻撃に対するレジリエンス（復元性）が必要になります。

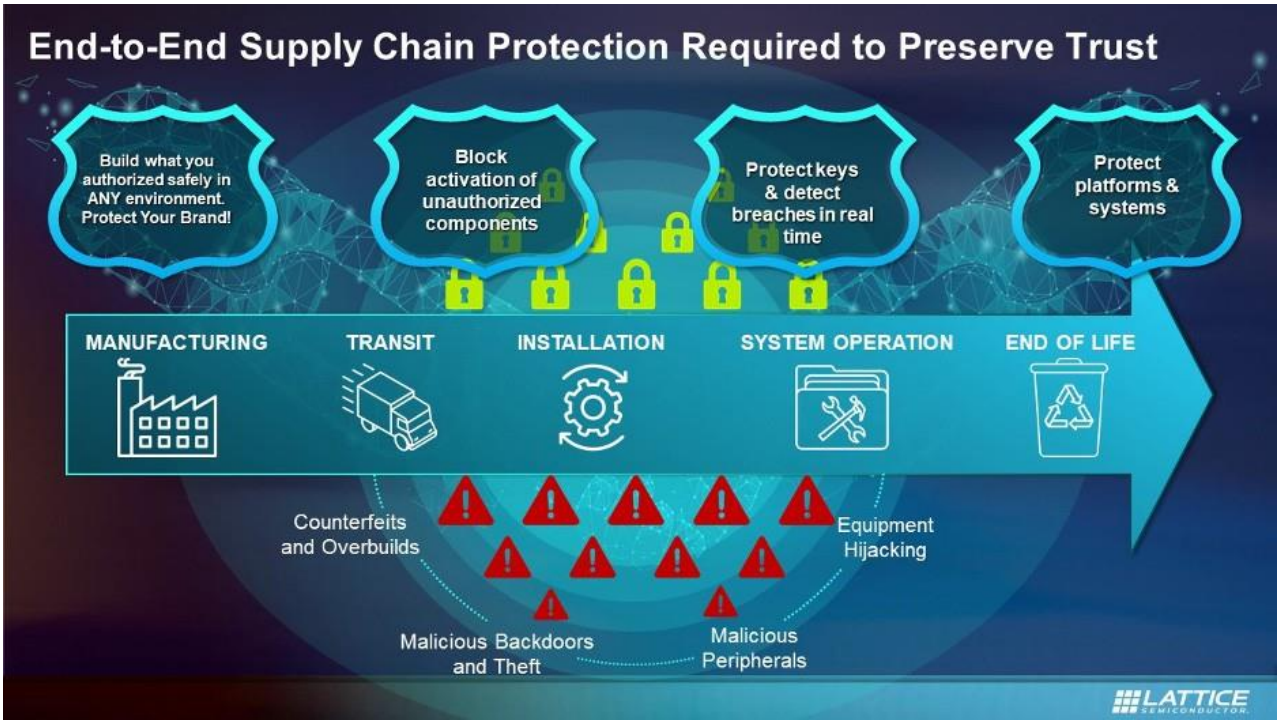

図 1: さまざまな潜在的脅威により、サプライチェーン全体にわたりコンポーネントのセキュリティを保つこと

新NIST標準

絶えず進化する脅威からどのように身を守ればよいのでしょうか。幸いにして、米国国立標準技術研究所（NIST）はファームウェアに対する脅威を認識し、プラットフォームファームウェアレジリエンス（PFR）の適切な実装の重要性を呼びかけるNISTプラットフォームファームウェアレジリエンス（PFR）ガイドライン（NIST SP-800-193）を発表しました。このガイドラインはプラットフォームがレジリエンスを持つために、不正な変更からのプラットフォームの保護、発生した不正な変更の検出、攻撃からの迅速かつセキュアな復元のためのセキュリティ・メカニズムを記載しています。

ガイドラインは攻撃に対するプラットフォームのレジリエンスをサポートするために、次の3つの原則を定めています。

- 保護：NISTの保護ガイドラインには、ファームウェア・アップデートの確実性や整合性を確保するプロセスなど、プラットフォーム・ファームウェアと重要なデータの完全な状態での維持と破損からの保護を確実に行うためのメカニズムが定義されています。また、ガイドラインは保護された外部メモリすべてとそのインタフェース・バスのランタイムでの同時モニタ（応答時間はナノ秒）と、すべてのファームウェアに対する厳格なアクセス制御の実行を求めています。
- 検出：プラットフォーム・ファームウェア・コードや重要なデータが破損した際の検出メカニズム。保護されたICの起動前にファームウェアの自動認証が必要です。
- 復元：破損が検出された際にはDoS攻撃やリプレイ・アタックに対しても、さらには認証済みメカニズムによる復元が強制された際にも、プラットフォーム・ファームウェア・コードや重要なデータを、既知の良好で認証済みの完全な状態に復元するメカニズム。この復元は、市場でのサポート・リソースの利用を最小限に抑制すると同時にシステムのオンライン状態を維持するために、自動的かつリアルタイムで行われる必要があります。

急速に進化する市場や新しい標準に対応するため、ラティスセミコンダクターは新たな付加価値を提供するセキュリティ・ソリューション・スタックとサプライチェーン・セキュリティ・サービスを発表し、ハードウェア・セキュリティ製品の機能を大幅に拡充しました。Lattice Sentry™ソリューション・スタックはシステム内のすべてのプログラマブルなコンポーネントに対しリアルタイムでダイナミックな保護、検出、復元機能を提供することにより、システム内ファームウェア攻撃の脆弱性を最小限に抑えます。Sentryソリューション・スタックはラティスのMachXO3D™セキュアFPGAを使用し、事前検証済みで容易にカスタマイズ可能な、完全なNIST 800-193準拠PFRソリューションを提供します。このソリューション・スタックには、すぐに使用可能で製造工程で検証済みのレジリエントなIPコア一式が含まれており、システム内のSPI / I2Cデバイスとそのバスの保護とモニタを可能にします。また、PFR機能のテストと評価のためのデモボードとリファレンス・デザインも提供します。スタックで使用できるソフトウェア・ツールには、ラティスの最新IPエコシステム／開発環境であるLattice Propel™も含まれています。PropelはスタックのRISC-Vプロセッサ IP向けCコードの変更や、フル・システム開発に使用されるIPの視覚的レイアウトを可能にすることから、非FPGAユーザーでもPFR実装をカスタマイズできます。このシステムをLattice Diamondツールにインポートし、コンフィギュレーション・ビットストリームを生成することができます。さらに、スタックには容易に変更可能なPFRマネジメント・コード、SPI/QSPi向けクイック・スイッチ回路図、マニフェスト・ジェネレータ、プロセッサ・コマンド・エミュレータなどの包括的なPFRリファレンス・デザインも含まれています。

Lattice Sentryソリューション・スタックは製品開発期間の大幅な短縮を可能にします。事前検証済みIPコアやリファレンス・デザインがない場合、こうしたソリューションの開発には数か月かかります。Sentryを使用すると、開発者はFPGAのリアルタイム動作を管理するCコード・サンプルを変更することにより、完全NIST 800-193準拠ソリューションを開発できます。事前検証済みIPはラティスのPropelソフトウェアを使用し、Cコードを実行するRISC-V CPUとともに、FPGAのコンフィギュレーション・ビットストリームに統合することが可能で、開発にはFPGAデザインの経験や知識は不要です。もちろんお客様自身のFPGA IPや回路の追加を行うことも可能です。

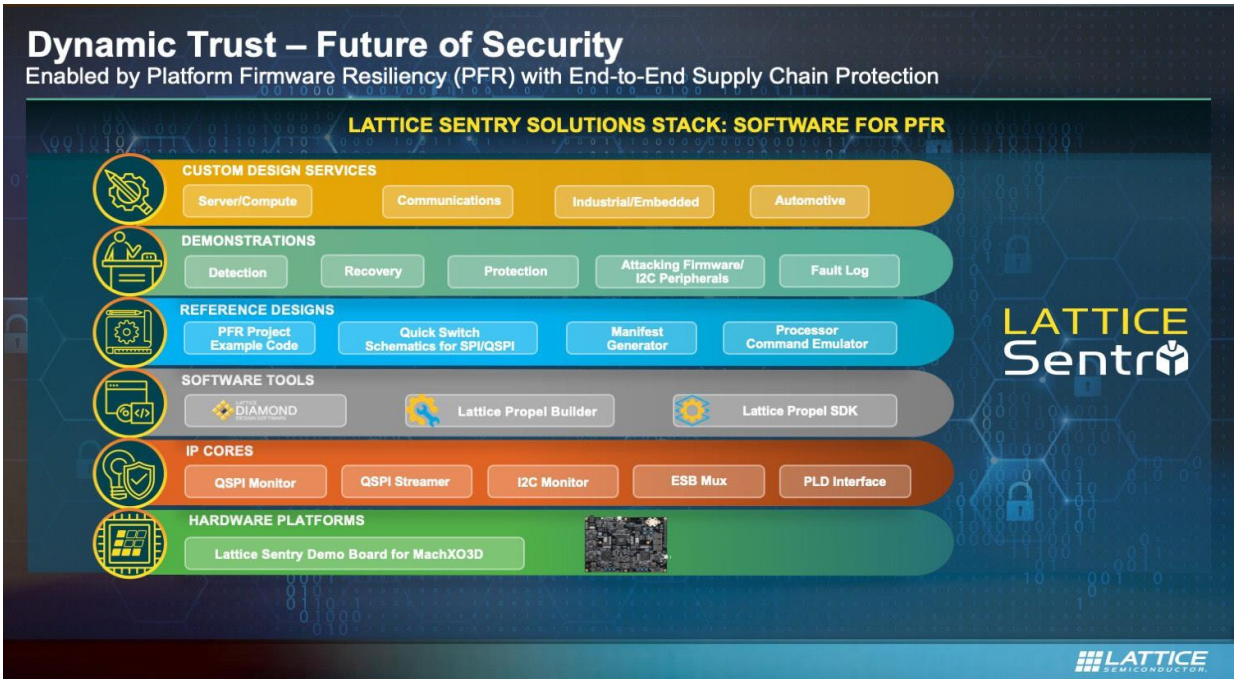

図 2: Lattice Sentryソリューション・スタック

Sentryに加え、ラティスはエンド・ツー・エンドのサプライチェーン・セキュリティ・サービスであるSupplyGuard™を提供しています。SupplyGuardはカスタマーIPのサプライチェーン通過にあたって、改ざん、トロイの木馬挿入、過剰生産、偽造、IP盗難への耐性を備えた、出荷時にロック済みのラティスFPGAを提供することにより、サプライチェーン全体にわたってカスタマーIPを保護する先駆的なサブスクリプション・サービスです。このサービスにより、お客様はFPGA上に保存されたコンフィギュレーション・ビットストリームと外部ファームウェア認証鍵のコピーや改ざんに対するレジリエンスを確保できます。SupplyGuardを使用すれば、開発者はサプライチェーン全体にわたる製品の保護が可能になります。SupplyGuardはセキュアな独自の方法で実行されるセキュアなキー・プロビジョニングとデバイス所有権の移行により保護を提供することから、現在入手可能な他のプロビジョニング・ソリューションと一線を画しています。

SupplyGuardのプロセスは、お客様のFPGAへのラティスによるお客様固有部品番号の割り当てから始まります。お客様固有のFPGAはラティスの工場でプログラムされ、コンフィギュレーション・ビットストリームと認証鍵によってお客様にのみFPGAのプログラミングを許可する、カスタマイズ済みの暗号化された認証情報とともに提供されます。SupplyGuardサービスは一般的な輸送会社を使用してFPGAがサプライチェーンを通過する際や、システムがサードパーティーの工場で組み立てられる際に信頼と保護の維持を可能にします。チップはラティスの工場で完全にロックされて出荷され、お客様だけがFPGAのロック解除に必要な認証情報を保有します。ラティスはFIPS 140-2認証済みHigh Security Module（HSM）を使用してこれらのロック解除認証情報を生成し、お客様に提供します。その後、お客様は自身のHSMを使用して認証情報を解読します。この際、サプライチェーンのいかなる人もこの認証情報にアクセスすることはできません。お客様のHSMはお客様のカスタマイズ済みコンフィギュレーション・ビットストリームと認証鍵の暗号化と署名に必要な認証情報を保有します。さらに、どのような形であっても、お客様のIPと暗号鍵がラティスやサプライチェーンにさらされることはありません。

SupplyGuardによりロックされると、お客様のFPGAはサプライチェーンを通過する際に「ミニ要塞」となります。お客様の認証ビットストリームによりプログラムされる準備が整うまでロックされ、アクセスは不可能です。暗号化と署名済みのお客様のビットストリームだけが、このカスタム・ロック済みFPGA上にローディング可能です。同時に、お客様のビットストリームは別のFPGA上へのローディングが不可能で、これにより、お客様のIPや認証鍵の複製や過剰生産を防止します。お客様のビットストリームのプログラミング・プロセスでは、ラティスによる出荷時のロック状態からお客様によるロック状態に至るまで、チップの暗号による制御が継続されます。この所有権の移行はラティスFPGA内部で保護された暗号化済みの状態で発生し、標準の量産工場プログラミング機器を使用して標準製造ラインで実行されます。コンフィギュレーション・ビットストリームは常時セキュアで暗号化された状態を維持し、保護された所有権の移行は特別なセキュリティ手順、スタッフ、機器（HSMなど）を必要とせずに行われます。これにより、他の工場鍵プロビジョニング・ソリューションで発生する追加的な時間やコストが不要になります。

図3：Lattice SupplyGuardサービスは Lattice FPGAがグローバル・サプライチェーン全体で不正アクセスから保護します

セキュアなシステム制御を実現するLattice FPGA

SentryとSupplyGuardの新セキュリティ機能は、セキュアなシステム制御向けのラティスの画期的なMachXO3D FPGAファミリを活用しています。MachXO3Dはシステム制御アプリケーション向けの業界初の小型低消費電力FPGAで、広範なコンピューティング、通信、産業、車載アプリケーションでファームウェアを保護します。MachXO3Dはラティスの定評あるMachXOファミリとピン互換で、設計者にとって、すべての通信システム／サーバで半分以上のシェアを持つ実証済みアーキテクチャの利点の活用が可能になります。MachXO3DはECDSA、ECIES、AES、SHA、HMAC、TRNG、公開／秘密鍵生成などの独立したNIST認証済み暗号化機能を使用し、自身のコンフィギュレーション・ビットストリームを保護するとともにシステム・セキュリティを実現します。各デバイスはセキュアな認証済みデュアルブート構成をサポートするオンチップ・フラッシュ・メモリ、外部ファームウェア認証のための公開鍵ストレージ、ユニークIDを備えています。何らかの理由で元のファームウェアが破損した場合、MachXO3Dは認証済みバージョンに自動的にロールバックし、中断することなくシステム運用を継続します。MachXO3DはSentryソリューション・スタックを使用し、保護する外部ファームウェアのためにこの認証チェックとファームウェア復元を継続的に実行することができます。

図 4: ブロック図に示すように、Lattice SentryベースPFRアプリケーションはシステム内の全ファームウェアをリアルタイムで保護可能

MachXO3D FPGAの暗号化機能は真の乱数生成（TRNG）や暗号アルゴリズム認証プログラム（CAVP）のためのNIST SP 800-90B仕様に準拠しています。MachXO3DのCAVP機能は米国連邦政府の暗号化ソフトウェア標準である連邦情報処理標準（FIPS）への準拠のために独立的な認証が行われています。

ダイナミック・トラストを可能にするLattice SentryとSupplyGuard

LatticeのSentryソリューション・スタックとSupplyGuardは連携し、高度にレジリエントなエンド・ツー・エンドのダイナミック・トラスト・ソリューションの構築に必要なすべてを設計者に提供します。SupplyGuardの保護機能はMachXO3D FPGAと開発者のビットストリームの整合性、さらにはプラットフォーム・ファームウェアのその他の部分を保護する開発者のセキュリティ認証情報を保護することにより、このサプライチェーンでの最初のリンクを提供します。FPGAは工場でのプログラミング中にセキュアな所有権の移行を実行する機能を備えており、開発者の署名と暗号化済みのコンフィギュレーション・ビットストリームに保護をシームレスに移行します。これにより、システムの起動前、運用中、システム廃棄までの将来的なすべての起動／運用時にプラットフォーム・ファームウェアを保護するSentry PFR機能の実装を可能にします。システムは悪意のあるいかなる行為にもナノ秒で応答するとともに、意図した通りの機能を維持します。SentryとSupplyGuardを使用して構築されたシステムは既存のあらゆるBMC/MCU/TPMベース・アーキテクチャの補完が可能なことから、開発者は既存のハードウェア・セキュリティ・ソリューションを引き続き使用しながら、お客様固有のセキュリティ／サプライチェーンのニーズに対応することができます。

まとめ

今日のハードウェア・セキュリティ環境は急速に変化しています。ハッカーはサプライチェーン内部でシステム・ファームウェアの脆弱性を容易に悪用し、データや設計を盗み、製品をハイジャックし、グレー・マーケットで販売するために複製品を生成します。開発者はどう対応すればよいのでしょうか。その答えは、NIST 800-193標準に準拠し、新たな付加価値を提供するハードウェア・セキュリティ製品やサービスの使用、ハードウェア・セキュリティのためのエンド・ツー・エンドのダイナミック・トラスト・アプローチの追求です。新しいLattice Sentryソリューション・スタックとSupplyGuardサプライ・チェーン・セキュリティ・サービスは、こうした解決策の迅速かつ容易な導入を可能にします。

参考情報

1. 出典：National Vulnerability Database（2016年、2019年）
2. 出典：ガートナー（2019年7月）

詳細：

www.latticesemi.com

コンタクト：

www.latticesemi.com/contact
www.latticesemi.com/buy