



WP493 (v1.0) 2017 年 9 月 6 日

# インテリジェント IIoT エッジ プラットフォームの重要な特性

著者: Chetan Khona

ザインクスの All Programmable SoC および 7 シリーズ FPGA は、現在のインダストリアル IoT (IIoT) プラットフォームに必要な機能を幅広くサポートし、将来に向けた最大限の柔軟性を備えています。これにより、産業用システムのライフサイクル全体で投資利益率 (ROI) の最大化と総保有コスト (TCO) の最小化が実現します。

## 概要

このホワイト ペーパーでは、産業用通信、サイバーセキュリティ、およびエッジ コンピューティング (簡単なデータ最適化から機械学習まで) の例を挙げながら、IIoT エンベデッド システムに Zynq®-7000 SoC および Zynq UltraScale+™ MPSoC ファミリーを採用した場合の利点について説明します。ARM® アプリケーション プロセッサと FPGA ロジック (プログラマブル ハードウェア)、ペリフェラル、およびその他の統合ブロックを組み合わせたこれらのデバイスを利用することで、個々のシステムにおいてソフトウェア インテリジェンスとハードウェア最適化の理想的なバランスをとることができます。このホワイト ペーパーでは、産業用機器のライフサイクルに着目し、ソフトウェアとプログラマブル ハードウェアを組み合わせることによってより高機能なシステムを容易に構築できるという短期的な利点、そして急速に変化する IIoT 市場トレンドの中でシステムの耐用年数を延長できるという長期的な利点について説明します。このホワイト ペーパーでは、ソフトウェアとプログラマブルハードウェア間の機能分割を容易にするソフトウェア ツールを紹介すると共に、All Programmable ソリューション以外を選択した場合のビジネス上のリスクとコストについても論じます。

© Copyright 2017 Xilinx, Inc. Xilinx, Xilinx のロゴ、Artix, ISE, Kintex, Spartan, Virtex, Vivado, Zynq、およびこの文書に含まれるその他の指定されたブランドは、米国およびその他の国のザインクス社の商標です。すべてのその他の商標は、それぞれの所有者に帰属します。

この資料は表記のバージョンの英語版を翻訳したもので、内容に相違が生じる場合には原文を優先します。資料によっては英語版の更新に対応していないものがあります。日本語版は参考用としてご使用の上、最新情報につきましては、必ず最新英語版をご参照ください。

## IT-OT 融合へのアプローチ

インダストリアル IoT (IIoT) とは、エッジ機器、クラウド アプリケーション、センサー、アルゴリズム、安全性、セキュリティ、プロトコル ライブラリ、ヒューマン マシン インターフェイス (HMI) などの要素を密結合したシステムであり、これらの要素には相互運用性が必要とされます。IIoT のビジョンは運用技術 (OT: Operational Technology) と情報技術 (IT: Information Technology) の融合として語られることもありますが、実際にはもっと大きな目標があります。リアルタイム性が要求される OT アプリケーションと大量のデータ処理が発生する IT アプリケーションのそれぞれの性質を考えると、これらすべての要素が連携し、クリティカルなタスクを時間どおりに確実に実行できるようにする必要があります。しかしもう 1 つの基本的要件である耐用年数の長さまで考慮すると、ある矛盾が発生します。耐用年数の長さは、システム サプライヤーとカスタマーの双方にとって IIoT システムの投資利益率 (ROI) に直結します。解析、機械学習、サイバーセキュリティをはじめ、IIoT システムの基盤を構成する多くの分野がめざましい進歩を遂げています。しかし緊密に統合されたこれらシステムに対して、長いライフ サイクルの間に変更やアップグレードを繰り返していくと、システムの実タイム性能に望ましくない影響が波及する可能性があります。

この課題に対する対処法として最も一般的なのは、IIoT エッジシステムの心臓ともいえる組み込み電子機器を選定する際に、最も高スペックなものを選択して不確定要素に対するマージンを確保するという方法です。エッジシステムは確定的な組み込み通信およびリアルタイム制御エンジンであり、工場やその他の産業用環境 (モーション コントローラー、保護リレー、プログラマブル ロジック コントローラー (PLC)、類似システムなど) の物理世界に最も近いネットワーク エッジに存在します。ギガヘルツ クラスのクロック周波数、大容量のメモリ、多数の I/O ポート、最新の暗号エンジンを採用してソリューションを構築すれば、不確定的な将来の要件に対応できると考えるかもしれません。しかし産業用機器は数百マイクロ秒 (またはそれ未満) のタイムスケールで動作するクリティカルなサブシステムで構成されており、工場や遠隔拠点で何十年も動作する必要があります。このように産業用機器のタイムスケールに対応しながら IIoT に求められるスケーラビリティを確保する手段として、最先端のマルチコア エンベデッド プロセッサのみを使用するのは不十分です。このようなアプローチをとると、最悪の場合、性能ボトルネックに起因する機能タイミングの問題に対処するためにマーケティングとエンジニアリングの面で困難かつコストのかかるトレードオフが多数発生することが考えられます。タイムスケールを考慮すると、IIoT エッジではスケーリングに関してもっと高い自由度が不可欠です。エンベデッド プロセッサ コア上で動作するソフトウェアをプログラマブル ハードウェアで増強すると、このようなスケーリングの自由度を引き出すことができます。このアプローチの方が一貫性が高く、確定性、レイテンシ、および性能を容易に管理できるだけでなく、IT ドメインと OT ドメイン間の干渉や OT ドメインのサブシステム内の干渉をなくすることができます。

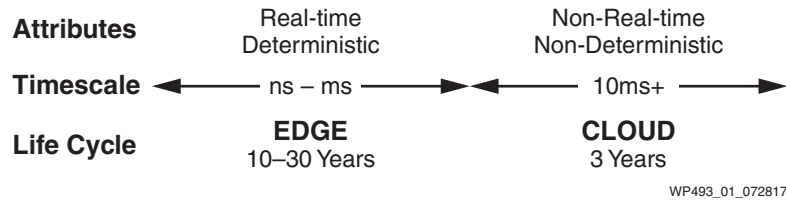
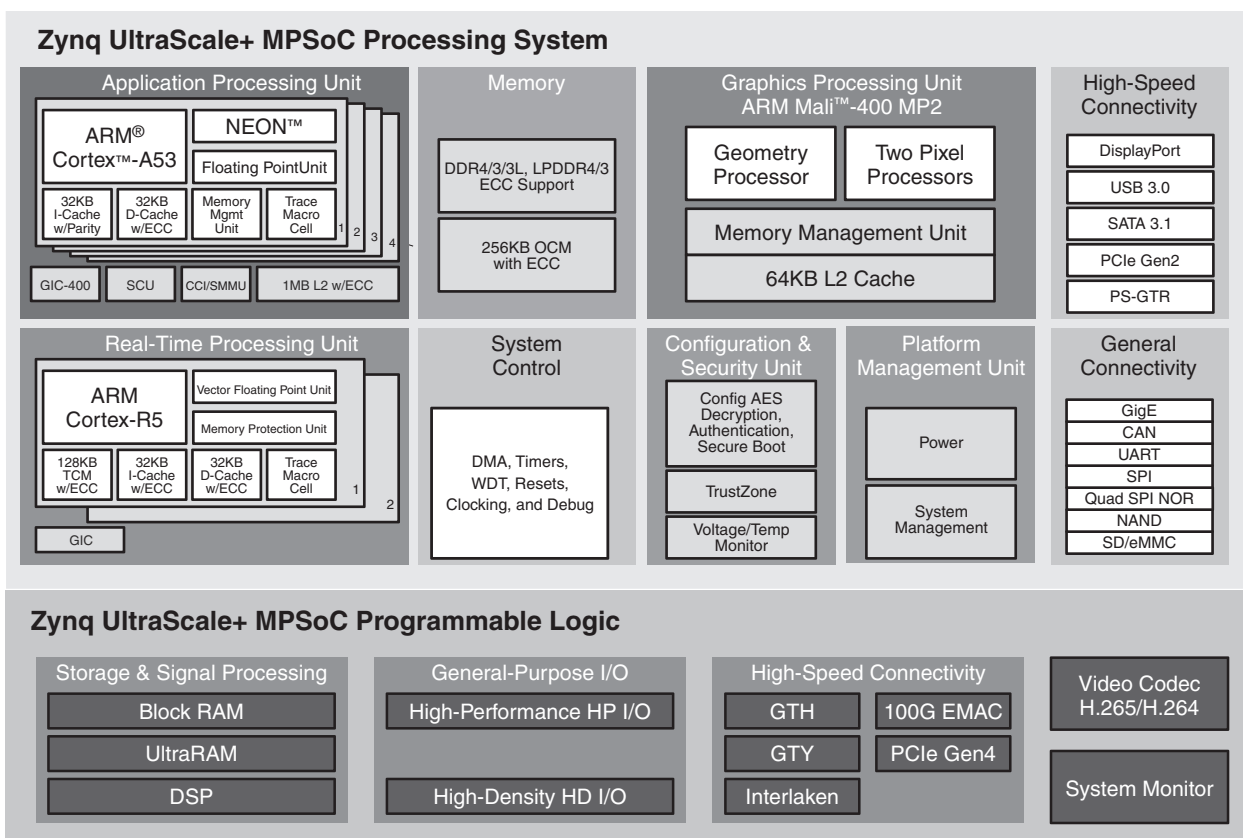


図 1: 代表的な IIoT システムのタイムスケール、特性、およびライフ サイクル

同時に、ハードウェア仮想化などの機能を利用すると新しいゲスト オペレーティング システムの導入や必要に応じたレベルの自律性と隔離が可能になるため、これらの機能を備えたプロセッサには持続可能な価値があります。また、パリティや ECC (後者を推奨) などのメモリ保護のように、将来的に有用性が失われることがないと考えられる機能もあります。固定プロセッサに専用ハードウェアを組み合わせ、目的に応じてタスクをバランスよく分散して処理を実行するアーキテクチャ自体、組み込み電子機器の世界ではそれほど新しい考え方ではありません。これまでと異なっているのは、タスクと分業の両方を長期的なスパンで適応させていく必要があるという点です。たとえば予知保全アルゴリズムを更新した場合、それまでより多くのセンサー入力が必要になることがあります。増大した計算量をハードウェアでオフロード実行すると、全体的な負荷、そして何よりもプロセッサ サブシステムのサイクルタイムを維持できます。このような柔軟性は、システムを購入して設置するカスタマーにとっても、その機器の付加価値ソフトウェアで提供される多くのサービスを今後数十年にわたって収益源とできるシステム サプライヤーにとっても大きなメリットとなります。

このホワイト ペーパーでは、長期的な市場トレンドの影響に適応できる IIoT エッジプラットフォーム選択という観点から、IIoT の基盤を構成する 3 つの重要なアプリケーション分野、すなわちコネクティビティ、サイバーセキュリティ、およびエッジ コンピューティングについて説明します。IIoT プラットフォームを導入する際には、卓越した柔軟性とスケーラビリティを備え、OT と IT の両方のテクノロジをどちらも同じように扱えるものを選択することが重要です。All Programmable SoC、すなわちハードウェアとソフトウェアの両方がプログラマブルな SoC がソリューションとして理想的です。また、ここでは All Programmable SoC に関連するテクノロジトピックとして、(1) ソフトウェア定義ハードウェア、(2) All Programmable SoC と ディスクリット エンベデッド プロセッサのアクセラレータとしての FPGA の比較についても取り上げます。ザイリンクスは、IT と OT のタスクを包括的にカバーする独自ソリューションとして Zynq-7000 SoC および Zynq UltraScale+ MPSoC ファミリーを提供しています (図 2 参照)。



WP493\_02\_042517

図 2: Zynq UltraScale+ のブロック図

## コネクティビティ: レガシ規格から将来のプロトコルへの移行

IIoT 時代のコネクティビティが合理化されたアプローチへと移行するのに伴い、これまでになかった複雑さが生じています。OPC Foundation の OPC-UA (Open Platform Communications-Unified Architecture) や DDS (Data Distribution Service for Real-Time Systems) などのエッジおよびシステム レベルプロトコルが、それぞれのアプリケーション分野で急速に普及しています。どちらのプロトコルも TSN (Time-Sensitive Networking) を活用しています。TSN はイーサネットをベースにした確定的な転送技術であり、異なる重要度が混在したストリームを扱うことができます。TSN はベスト エフォート トラフィックと並行してさまざまなレベルでスケジューラされたトラフィックをサポートするため、エッジだけでなくほとんどの IIoT ソリューションチェーンを対象にしたネットワークプロトコル一元化のビジョンが実現に向けて大きく前進します。TSN はまだ発展途上の規格であり、規格およびエンドマーケット固有のプロファイルが完全に確定する前に ASIC や ASSP などの専用チップセットで標準規格への準拠を謳うには大きなリスクが伴います。同様に、リアルタイム データを管理している既存のコントローラーに完全なソフトウェア ベースのアプローチで TSN のサポートを追加しようとする、タイミングの挙動が予測不能になる可能性があります。また、割り込みへの応答やメモリ アクセスのタイミングなどが悪化することも予想されます。結局、TSN では現在のコントローラーにはない形で時刻を認識する必要があるため、これは理にかなったソリューションではありません。TSN を同じデバイスに統合してエンドポイントなどの制御機能を管理するのではなく、外部 TSN スイッチをシステムに追加した場合でも、各種エンドポイントを接続するスイッチによって TSN 非対応のコントローラーに対するイーサネット後方互換性が得られる可能性があります。目標は、TSN をエンドポイントに統合してスケジューラされたトラフィックとベスト エフォート トラフィックの両方をサポートし、なおかつ制御機能のタイミングへの影響を最小限に抑えることです(図 3 参照)。

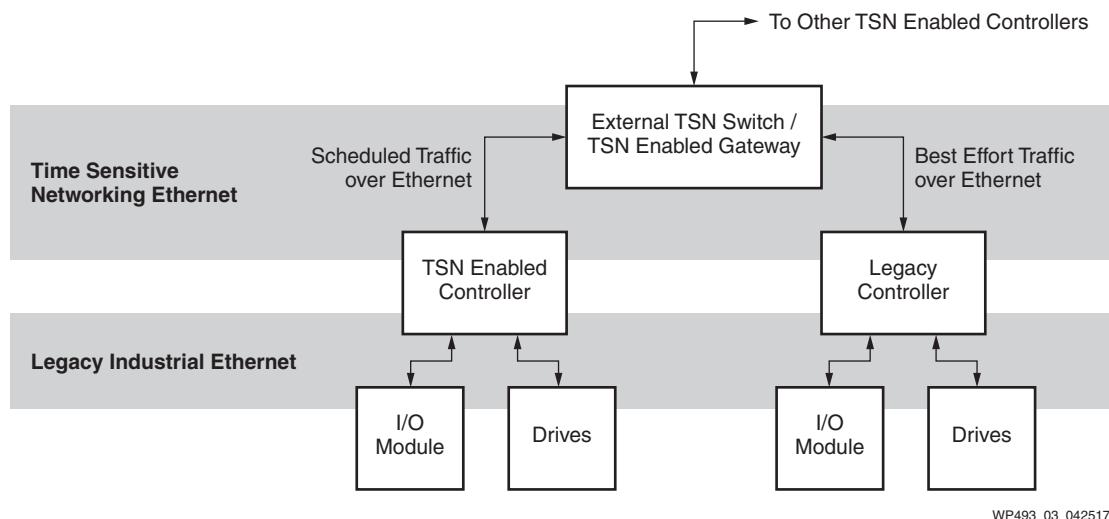


図 3: TSN のトポロジと利点

All Programmable デバイスにインプリメントした TSN をコントローラーに統合すると、広い帯域幅を必要とするリアルタイム機能をハードウェアに実装でき、ソフトウェアのタイミングにはそれほど大きな影響を与えないため、移行による変化の影響は最小限に抑えられます。ザイリンクスは標準に完全に準拠した、最適化済みの TSN 実装を社内で開発しており、これを使用することで純粋なエンドポイントまたはブリッジ接続したエンドポイントの実現が可能になります。All Programmable SoC ベースのコントローラーをイーサネットから TSN へアップグレードするにせよ、発展途上の TSN 規格を使用して新規コントローラーを設計するにせよ、ザイリンクスの All Programmable アプローチではクリティカルなタイミングへの影響を最小限に抑えながら変更を追加でき、ASIC や ASSP に比べ将来への高い適応力が得られます。

もう 1 つ、これと同じくらい一般的なユースケースについても考慮する必要があります。産業用ネットワークには長い歴史があるため、IIoT システムはこれまで産業分野で用いられてきた数多くのレガシプロトコルもサポートする必要があります。最近の SoC は、これらプロトコルの一部さえも満足にサポートしていないものがほとんどです。また、これらの固定された SoC でネットワーク インターフェイスの数に十分対応できる I/O 機能を備えたものもほとんどありません。これに対し、ザイリンクスの All Programmable SoC で構築したシステムなら、レガシプロトコルや関連する I/O コネクティビティのサポートなど、カスタマー固有のカスタマイズにも対応できます。プロトコルで必要とされるサイクル時間が 250 $\mu$ s であれ 64 $\mu$ s であれ、これらのインダストリアル通信コントローラーを完全にカプセル化してハードウェア オフロードした形で実装することにより、追加デバイスのコストが削減されます。しかも、ソフトウェア ベースのアプローチとは異なり、メインストリームのソフトウェアおよびファームウェアへの影響もありません。TSN を使用するにせよ産業用のレガシプロトコルを使用するにせよ、あるいはより一般的なケースとして過去と未来のプロトコルをブリッジ接続して混在させるにせよ、ザイリンクスが提供する Any-to-Any コネクティビティは確定的な動作が仕様上確約されています。

## サイバーセキュリティ：ハード化と同時に将来の脅威にも適応

IIoT の第一人者は、サイバーセキュリティの幅広いトピックに対して「多層防御」のアプローチを採用しています。多層防御とは階層型セキュリティの一形態で、サプライヤーのサプライチェーンから始まり、エンド カスタマーのエンタープライズおよびクラウド アプリケーション ソフトウェアまでをカバーし、場合によってはソフトウェアが接続するモノまで含みます。このセクションでは、IIoT エッジに導入された組み込み電子機器に対するトラスト チェーン (信頼の鎖) に範囲を限定して説明します。ネットワークがアナログとデジタルの境界まで伸びた現在、データはデジタルドメインに入った時点ですぐにセキュリティ保護する必要があります。多層防御セキュリティを実現するには、強力なハードウェア RoT (Root of Trust、信頼のルート) を利用して (1) セキュアブート/メジャーブート、(2) ハードウェア、オペレーティング システム、ソフトウェアの分離によるランタイムセキュリティ、(3) セキュアな通信を確保する必要があります。信用されたリモート認証サーバーや認証局など、チェーン全体で資格情報を個別に検証することも必要です。

サイバーセキュリティ攻撃は今後増えていくことが予想されるため、セキュリティ対策は固定的なものではなく進化させていく必要があります。たとえばセキュア メッセージング プロトコルの TLS (Transport Layer Security) は 1995 年以降、5 回の大規模なアップデートが行われており、今後もさらなるリビジョンが予定されています。IIoT システムのサプライヤーおよびカスタマーは、しだいに高度化するセキュリティ リスクを軽減しつつ、高価な資産の耐用年数を最大化する方法を見つける必要があります。TLS などのプロトコルを強調する暗号アルゴリズムは一般的にソフトウェアで実装されますが、IT と OT の融合が進んでくると、IT 側でのこうした変更によって OT 側のリアルタイム性能に影響が出る可能性があります。こうした影響を軽減する手段として、ハイパーバイザーやその他の隔離手法といったソフトウェア アーキテクチャ ツールを利用できます。

これらのソフトウェア コンセプトにプログラマブルハードウェアを組み合わせると、現時点では定義もされていない新しい暗号機能をフィールドへの導入から何年も後にサポートするといったことが可能です。このアプローチによって、より強力なリスク軽減計画が実現すると共に、リコール、パッチ、あるいは訴訟に伴うコストを未然に防ぐことができます。

## ソフトウェア定義ハードウェア

「サイバーセキュリティ:ハード化と同時に将来の脅威にも適応」のセクションで述べたようなハードウェア オフロードは、All Programmable SoC のプログラマブルハードウェアだけでは十分にサポートできません。このビジョンを完全な形で実現するには、このテクノロジーを簡素化するソフトウェアによる自動化が必要です。SDSoC™ 開発環境を使用すると、数ある言語の中でも特に C/C++/OpenCL を用いて機能の全体または一部をプログラマブルハードウェアまたはソフトウェアに分割できます。SDSoC 開発環境では、プロセッサとプログラマブルハードウェア間でデータを移動するためのエンジンとインフラも生成されます。2015 年に行った実証実験では、SDSoC ツールを使用して AES (Advanced Encryption Standard)-256 アルゴリズムの一部をプログラマブルハードウェアに移動することにより、性能は 4 倍に引き上げられました。詳細は、[Xcell Software Journal](#) の記事「SDSoC を使用した AES 暗号化のアクセラレーション」を参照してください。

このベンチマークは、ソフトウェア インテリジェンスとプログラマブルハードウェア最適化の理想的なバランスをとることを目的として実施したものです。しかしこの開発環境では関数全体をプログラマブルハードウェアにオフロードすることもできます。同様に、モーター制御ループの収束時間もハードウェア アクセラレーション エンジンを使用するとソフトウェアのみによる実装に比べ性能が 30 ~ 40 倍に向上することが確認されています (図 4 参照)。

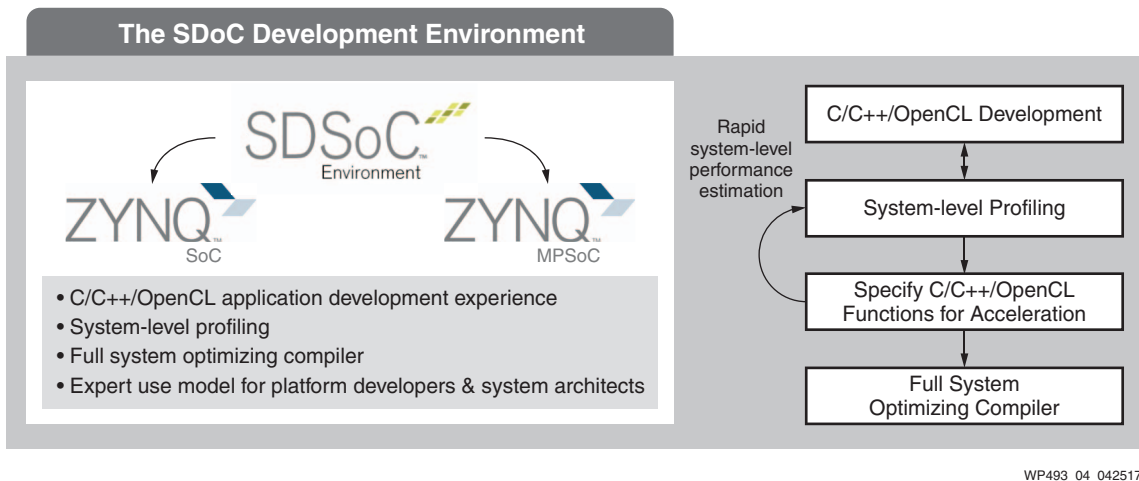


図 4: SDSoC デザイン環境のデザイン フロー

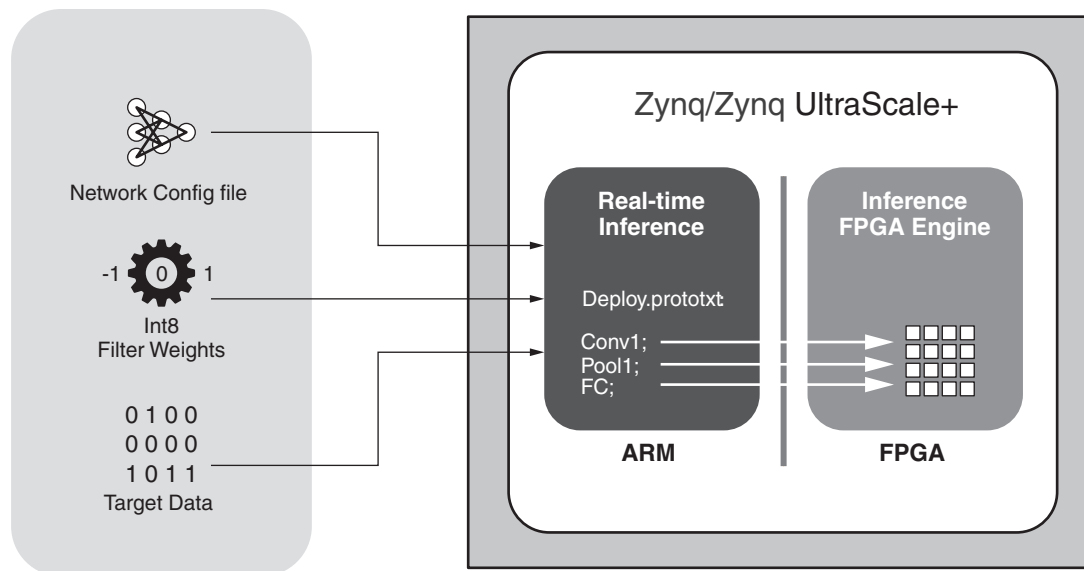
## エッジ コンピューティング: スケーラビリティ、コスト効率、リアルタイム性

通信およびセキュリティと同様に、エッジ コンピューティングもさまざまな方向へ進化しつつあります。これまでアクセスできなかったシステムから解放されたデータ ストリームをクラウドの強力なコンピューティング能力で処理することにより、ユーザーはこれまで見ることも理解することもできなかった知見に基づいて行動できるようになっています。これによってユーザーの期待値は上がり、それがそのまま新しい基準値となっています。GPS を利用したナビゲーションシステムが利用されるようになって道路地図がほとんど使用されなくなったのと同様、産業用機器の購入者およびユーザーが IIoT システムからのフィードバックに期待する内容も変化してきています。最近では、こうした知見をクラウドではなくエッジで生成しようという傾向が見られます。これには、主に次の 3 つの要因があります。

- エッジからクラウド経由で知見を適用すると時間がかかる
- 往々にして膨大な量になるデータをクラウドに送信するとコストがかかる
- データをクラウドに送信するとセキュリティ、信頼性、およびプライバシーの面で問題が生じる

これらは業界トレンドであり、絶対的なものではありません。データをローカルで前処理して、最適化および難読化したデータをクラウドへ送信するだけでもセキュリティとプライバシーの懸念のいくつかは大きく改善されます。非常に単純な例として、あるマシンを制御しているコントローラーの内部で時系列データに対してローパス (平均化) フィルターを適用する場合を考えてみます。こうすると、クラウドに送信されるデータポイントの数が減少すると同時に、異常値データも抑制できます。複雑なメモリトランザクションを使用した場合、データに基づく意思決定の応答時間が損なわれますが、プログラマブルハードウェアを使用すると、これらの最適化機能をマシンから出力されるデータストリームに適用できるため、データ処理効率は最大限に向上します。この例は1つのセンサーからの1つのデータストリームとして考えることもできますが、実際はほとんどの産業用システムが数百あるいは数千ものデータストリームを同時に処理しています。接続の数が増えるほど問題も大きくなりますが、各種センサーフュージョン手法やオンチップ解析などを利用したプログラマブルハードウェアによるソリューションの価値も大きくなります。

ここに示した例では、リアルタイム性が要求されるフィードバック項目に関してはコントローラーに埋め込んだインテリジェンスによってローカルで調整し、それほどリアルタイム性が必要とされないデータは圧縮してクラウドにプッシュ送信します。これは、エッジとクラウドの補完関係を理想的な形で実現した例と言えます。このようにエッジにインテリジェンスを埋め込んでクラウドと協調動作させる方式は、近年 IIoT 分野でも注目されつつあるエッジ側での機械学習にも適用できます。機械学習にはニューラルネットワークを利用した推論と導入のほか、回帰などを利用した古典的な手法もありますが、優れた電力効率とカスタマイズ性を備えた超並列アーキテクチャのプログラマブルハードウェアに非常に適しています。このため、クラウドではプログラマブルハードウェアベースのアクセラレーションカードが広く使用されています。これと同じ All Programmable テクノロジをエッジで使用すると、複数センサーを利用した機械学習アプリケーションのレイテンシ、消費電力、コストを最小限に抑えられます。All Programmable テクノロジは IT-OT 融合のすべての基盤要素を効率的にサポートすると同時に、急成長中の分野においても優れた機能を提供できるため、1つのデバイスで最も広範な IIoT アプリケーションをカバーできます。たとえばモーター制御、マシンビジョン、ネットワーク通信、機能安全、サイバーセキュリティなどのアプリケーションをエッジ側での解析や機械学習と組み合わせることが、IIoT における All Programmable テクノロジのユースケースとして期待されます。SDSoC 開発環境のようなツールとその支援ライブラリを使用すれば、最も小規模な All Programmable デバイスのごく一部に大規模なアルゴリズムを実装できます (図 5 参照)。



WP493\_05\_042517

図 5: Zynq-7000 および Zynq UltraScale+ SoC を使用した機械学習の推論フロー

## レガシ プロセッサに対するコプロセッサとしての FPGA

IIoT エッジプラットフォームで幅広い IT-OT 機能を実装する場合、最も一般的な選択肢となるのは All Programmable SoC です。このデバイスを利用すると、これまでに述べた統合の利点が得られるだけでなく、消費電力とコストも削減できます。しかし実際には、レガシ エンベデッド プロセッサ上でレガシ コードを実行するなど、既存のアーキテクチャを引き続き使用することが必要なケースもあり、このような場合は別の選択肢があります。つまり、それはプログラマブル ハードウェアのみで構成されるデバイス、すなわち FPGA を利用しても先に述べた利点のいくつかは得られません。コンパニオン デバイスとして動作する FPGA は、メイン エンベデッド プロセッサとの接続が容易です。このような FPGA はメイン エンベデッド プロセッサのコプロセッサとして動作させることができ、オプションとしてコンパクトなマイクロコントローラーまたはマイクロプロセッサ (ザイリックス MicroBlaze™ プロセッサなど) を実装できます。プログラマブル ハードウェアを使用して構築したソフト プロセッサは、幅広い種類のオペレーティング システムおよびリアルタイム オペレーティング システムをサポートします。これらのオプションを利用すると、レガシ システムにおいても発展途上の機能やリアルタイム性が要求される機能をオフロードできます。FPGA と SoC を含むザイリックスの All Programmable ポートフォリオは長期のライフ サイクルおよび拡張温度範囲に対応した高可用性のシリコンをサポートしており、動作中でもデバイスの全体または一部をリコンフィギュレーションできます。フットプリント互換の FPGA も多数存在しており、柔軟なプラットフォーム構築が可能です。プロセッサと FPGA の 2 チップ構成では、All Programmable SoC を 1 つだけ使用した場合に比べチップ間の帯域幅に制限があります。モノリシック SoC なら十分な帯域幅と接続を確保できるため、先の例で示したような動的なハードウェアとソフトウェアの分業が容易になります。これは 2 チップ構成のソリューションでは不可能です。こうした制約があるものの、プログラマブル ハードウェアの価値は非常に大きいため、一般に PCIe、SPI、QSPI などの規格を使用して構築した FPGA 専用インターフェイスをデータシートに含めているエンベデッド プロセッサが増えています。

## 新しいインダストリアル時代に耐用年数の長さをもたらすハードウェアとソフトウェアのプログラマビリティ

電動式の産業用制御システムが登場してから 100 年以上が経ちます。第四次産業革命と呼ばれることもある IIoT では、利用可能なテクノロジーと必要なタスクばかりでなく、産業全体が破壊的なペースで変化しています。現在、IIoT エッジプラットフォームの構築ブロックとして新しいテクノロジーが登場しており、これらを利用すると今後長期にわたって IT-OT のタスクをより広く、より深くカバーできます。Zynq-7000 や Zynq UltraScale+ デバイスなどの All Programmable SoC が提供するソフトウェアとハードウェアのプログラマビリティを利用すると、過去 20 ~ 30 年のエンベデッド アーキテクチャの構築ブロックに比べ、より耐用年数の長い資産を構築できます。IIoT システム開発コストの内訳を見ると、クラウドおよびエンベデッド ソフトウェア開発が全体の約 75% を占めています。このため、同じクラウド インフラに接続することを考慮せず最終製品ごとに異なるエンベデッド コントローラーを使用するのは正しいアプローチとは言えません。システム サプライヤーにとって最も重要なのは、通信インターフェイス、セキュリティ インフラストラクチャ、制御ループ タイミング、データ解析アルゴリズムなどを毎回開発し直すのではなく、共通のプラットフォームを採用し、価値を生むソフトウェア サービスに研究開発の時間と資金を投入できるようにすることです。FPGA ベースのアプローチは、レガシ プロセッサ システムを使い続けるをえないサプライヤーにこれら利点の多くを提供します。All Programmable SoC のアプローチは、利用可能なオプションを最大化し、産業用システムのサプライヤーとカスタマーの双方にとって投資利益率 (ROI) を向上させる鍵となります。

## まとめ

このホワイト ペーパーでは、ザイリンクス All Programmable SoC および FPGA によってシステム サプライヤーおよびカスタマーにとっての投資利益率 (ROI) が最大化する理由として、次の点について説明しました。

- ハードウェアとソフトウェアのプログラマビリティを備えたザイリンクス All Programmable SoC および FPGA はフィールド アップデートが可能で、IIoT に関する最新の規格やトレンドにもリスクなしに追随できるため、長期の耐用年数を実現できること。
- システム サプライヤーのさまざまなプラットフォームに対し、ザイリンクス製品は多くのデバイス ファミリ間でスケラビリティがあるため、包括的な製品ラインナップによって総保有コスト (TCO) を削減できること。
- IT および OT 分野のさまざまな IIoT 機能を柔軟性と電力効率に優れた 1 つの低レイテンシ デバイスに統合できること。

## これから開発を始められる方へ

ザイリンクスはスケラブルで包括的な IIoT エッジ プラットフォームのソリューション プロバイダーとして業界をリードし、IIoT 業界の主要企業と協力してウェブ セミナー、アプリケーション ノート、リファレンス プラットフォーム、評価キットの提供拡充に取り組んでいます。これには、主なものだけでもインダストリアル イーサネット コネクティビティ、モーター制御、セキュア ブート/メジャー ブートによるハードウェア RoT、機械学習などが含まれます。特に Avnet 社のインダストリアル IoT スターター キットおよびザイリンクス All Programmable インダストリアル制御システム (APICS) はエッジからクラウドまでのさまざまなテクノロジーを集約しており、All Programmable SoC の統合および機能がもたらす利点を評価していただけです。

IIoT 分野における All Programmable SoC および FPGA の詳細は、次を参照してください。

<https://japan.xilinx.com/applications/megatrends/industrial-iiot.html>

## 改訂履歴

次の表に、この文書の改訂履歴を示します。

日付	バージョン	内容
2017 年 9 月 6 日	1.0	初版



# 免責事項

本通知に基づいて貴殿または貴社(本通知の被通知者が個人の場合には「貴殿」、法人その他の団体の場合には「貴社」。以下同じ)に開示される情報(以下「本情報」といいます)は、ザイリンクスの製品を選択および使用することのためにのみ提供されます。適用される法律が許容する最大限の範囲で、(1)本情報は「現状有姿」、およびすべて受領者の責任で(with all faults)という状態で提供され、ザイリンクスは、本通知をもって、明示、黙示、法定を問わず(商品性、非侵害、特定目的適合性の保証を含みますがこれらに限られません)、すべての保証および条件を負わない(否認する)ものとします。また、(2)ザイリンクスは、本情報(貴殿または貴社による本情報の使用を含む)に関係し、起因し、関連する、いかなる種類・性質の損失または損害についても、責任を負わない(契約上、不法行為上(過失の場合を含む)、その他のいかなる責任の法理によるかを問わない)ものとし、当該損失または損害には、直接、間接、特別、付随的、結果的な損失または損害(第三者が起こした行為の結果被った、データ、利益、業務上の信用の損失、その他あらゆる種類の損失や損害を含みます)が含まれるものとし、それは、たとえ当該損害や損失が合理的に予見可能であったり、ザイリンクスがそれらの可能性について助言を受けていた場合であったとしても同様です。ザイリンクスは、本情報に含まれるいかなる誤りも訂正する義務を負わず、本情報または製品仕様のアップデートを貴殿または貴社に知らせる義務も負いません。事前の書面による同意のない限り、貴殿または貴社は本情報を再生産、変更、頒布、または公に展示してはなりません。一定の製品は、ザイリンクスの限定的保証の諸条件に従うこととなるので、<https://japan.xilinx.com/legal.htm#tos>で見られるザイリンクスの販売条件を参照してください。IP コアは、ザイリンクスが貴殿または貴社に付与したライセンスに含まれる保証と補助的条件に従うこととなります。ザイリンクスの製品は、フェイルセーフとして、または、フェイルセーフの動作を要求するアプリケーションに使用するために、設計されたり意図されたりしていません。そのような重大なアプリケーションにザイリンクスの製品を使用する場合のリスクと責任は、貴殿または貴社が単独で負うものです。<https://japan.xilinx.com/legal.htm#tos>で見られるザイリンクスの販売条件を参照してください。

## 自動車用のアプリケーションの免責条項

オートモーティブ製品(製品番号に「XA」が含まれる)は、ISO 26262 自動車用機能安全規格に従った安全コンセプトまたは余剰性の機能(「セーフティ設計」)がない限り、エアバッグの展開における使用または車両の制御に影響するアプリケーション(「セーフティアプリケーション」)における使用は保証されていません。顧客は、製品を組み込むすべてのシステムについて、その使用前または提供前に安全を目的として十分なテストを行うものとします。セーフティ設計なしにセーフティアプリケーションで製品を使用するリスクはすべて顧客が負い、製品の責任の制限を規定する適用法令および規則にのみ従うものとします。

この資料に関するフィードバックおよびリンクなどの問題につきましては、[jpn\\_trans\\_feedback@xilinx.com](mailto:jpn_trans_feedback@xilinx.com) まで、または各ページの右下にある[フィードバック送信] ボタンをクリックすると表示されるフォームからお知らせください。いただきましたご意見を参考に早急に対応させていただきます。なお、このメール アドレスへのお問い合わせは受け付けておりません。あらかじめご了承ください。