

ミクスト・クリティカリティ IoT エッジの実現

VOSYSIoTは、エンドツーエンドのIoTソフトウェア・スタック製品であり、単一のハードウェア・プラットフォーム上にて、アイソレートされ、リアルタイムで、安全かつセキュアにアプリケーションを実行できます。これにより、コンソリデーション/統合とインフラのコストの低減が可能です。

Features

- ▶ セーフティでクリティカルなアプリケーションの強力なアイソレーション
- ▶ 柔軟で弾力性にとむソフトウェア構造
- ▶ Arm Cortex-A プロセッサ すべてにおいて、互換性あり
- ▶ ノーマルワールドとセキュアワールド間のセキュア・シェアド・メモリの利用
- ▶ ノーマルワールドとセキュアワールド間のセキュアでシェアされたネットワーク・コミュニケーション
- ▶ ファンクショナル・セーフティ認証済のクリティカル・ソフトウェア・コンポーネント
- ▶ モジュラー・システム・デザイン
- ▶ スペクター脆弱性・メルtdown脆弱性に対する保護

Benefits

- ▶ システム・コストの削減。2つ以上のOSのコンソリデーション/統合
- ▶ オープンソースのバーチャライゼーション・レイヤーによる、システムの拡張
- ▶ ベアメタルレベルのパフォーマンスの実現 オーバヘッドなし
- ▶ 完全カスミ化可能(ソフトウェア追加、ペリフェラルの共有 等)
- ▶ 現行のOSを、そのまま使用可能

The Challenge

現代のIoTシステムは、安全でクリティカルな環境下において、クリティカルな機密データを取り扱う必要があります。

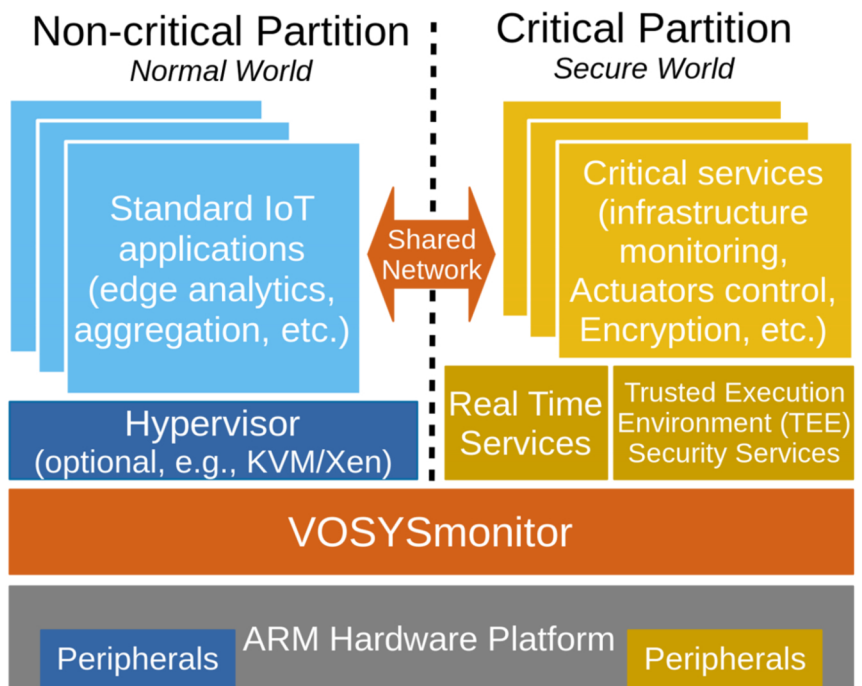
今日、クリティカル/非クリティカルのデータ処理において、適切にアイソレーションを確保し、かつ、安全性とセキュリティを保証するには、重複したリソースが必要です。

この意味で、コスト管理のためには、コンソリデーション/統合が、ますます重要になってきています。

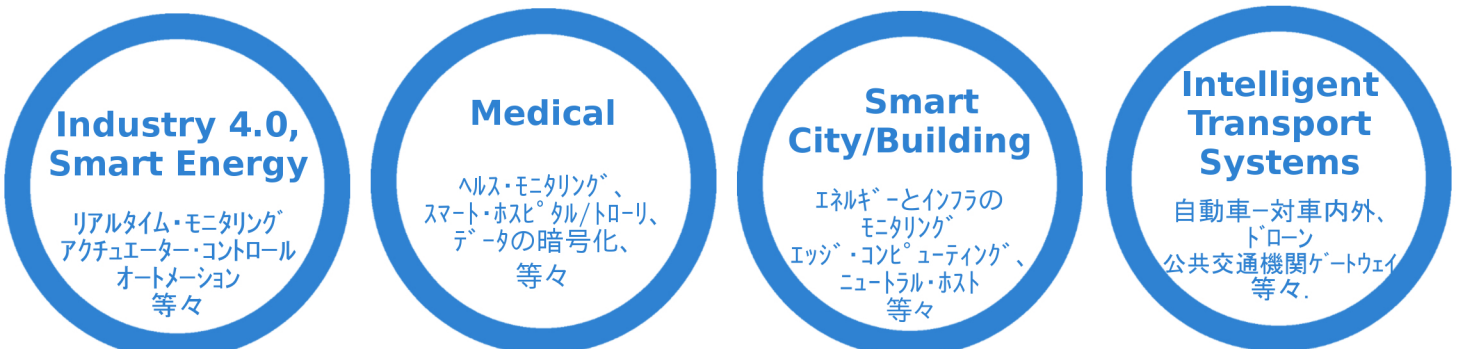
The Solution

VOSYSIoTソフトウェア・スタックにより、単一のハードウェア・プラットフォーム上にて、クリティカリティ・レベルの異なるOSやアプリケーションを同時に実行することができます。

そのうえ、Arm TrustZoneのセキュリティ・エクステンションを活用し、セキュアで、ISO認証可能なソフトウェア/VOSYSmonitorにより、VOSYSIoTは、最高のアイソレーションを保証します。



ユースケースの例



バーチャル・オープン・システムスは、EUに拠点を持つハイテクIT企業で、IoTや、車載/コネクティッド・カー用、コミュニケーション市場向け、その他一般のエンベデッド・システム向け等の複雑なミクスト・クリティカルティ・システムにおいて、オープンソースのバーチャライゼーション・ソリューションやカスタム・サービスを提供しています。

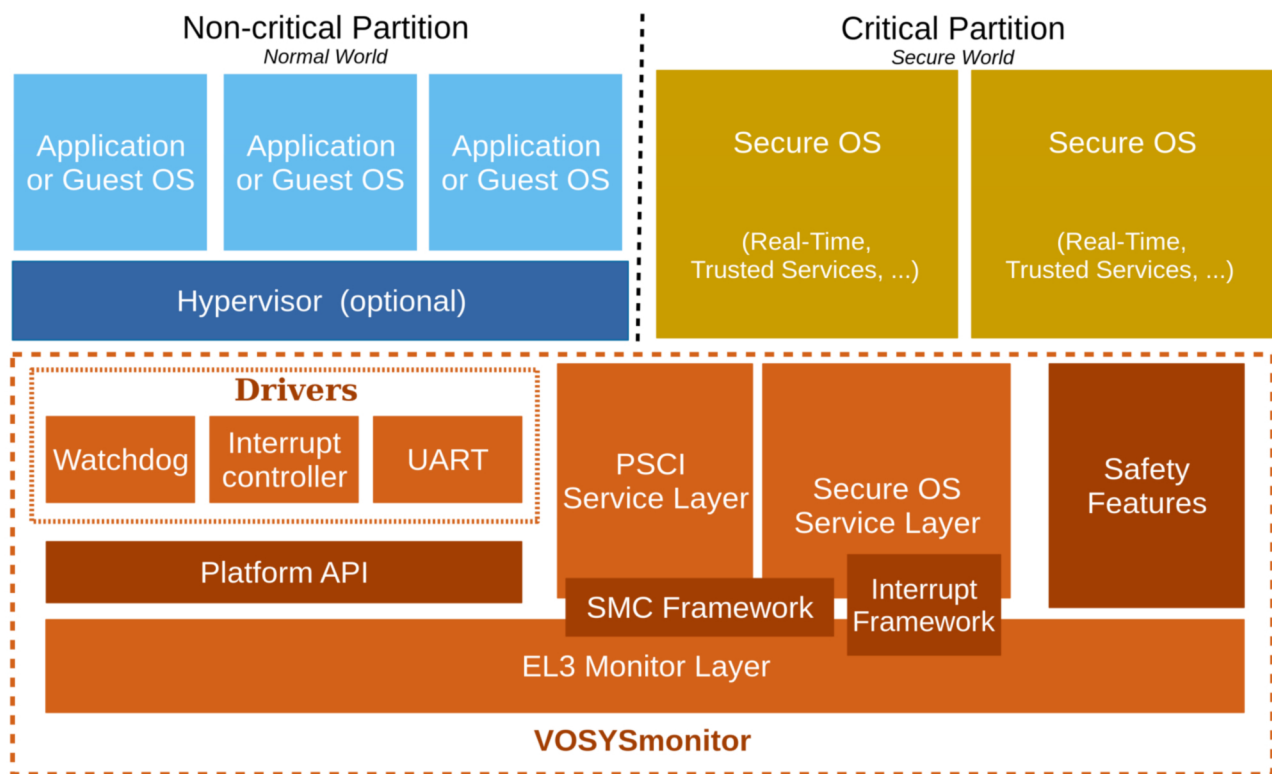
VOSYSmonitor software product

ミクスト・クリティカルティ・システム用の低遅延の認証システム・パーティショナー

VOSYSmonitorは、単一のマルチコア・ハードウェア・プラットフォーム上にて、異なったクリティカルティ・レベルの複数のアプリケーションの統合を可能とするソフトウェア・システム・パーティショナーです。

それは、クリティカルな、あるいは、ノンクリティカルなオペレーティング・システムの同時実行を可能とするソフトウェア・バイナリーとして提案されています。

複雑なユースケースをサポートするために、オープンソース・ハイパーバイザ（オプション）を追加することにより、ノンクリティカル・パーティションにて複数のバーチャル・マシンを実行できます。



VOSYSmonitorのよって得られるアイソレーションは、ARMプロセッサの最上位エクセブションにて、実行される従来のいかなるバーチャライゼーション・ソリューションよりも強力です。

実際、他のハイパーバイザでは、セキュリティや性能を犠牲にせざるえないのとは対照的に、VOSYSmonitorは、ARM TrustZoneを活用して、2つに分離したコンパートメントにおいて、プロセッサ・コア、バス、メモリおよびペリフェラルをアイソレートするようなシステムレベルのセキュリティ・アプローチを可能とし、最高のプロテクションと、本来のパフォーマンスを確保します。

VOSYSmonitor hardware target

- ARM TrustZoneを持ったARMv8-A および ARMv7プロセッサ（つまり、Cortex-A57/A53/A72等）
- セキュア・モニター・モードへのアクセス（EL3）
- TrustZone有効のインタラプト・コントローラ、および セキュリティIP

VOSYSmonitorは、ISO 26262 ファンクショナルセーフティ 認証のソフトウェア・システムパーティショナーであり、60μs以下のブートタイムと平均1μs以下のRTOSインタラプト遅延時間を実現しています。