Virtual Open Systems

VOSySmonitor

統合されたミクスト・クリティカリティ・システムのための
安全認証済システム・パーティショナー

VOSYSmonitor

contact@virtualopensystems.com

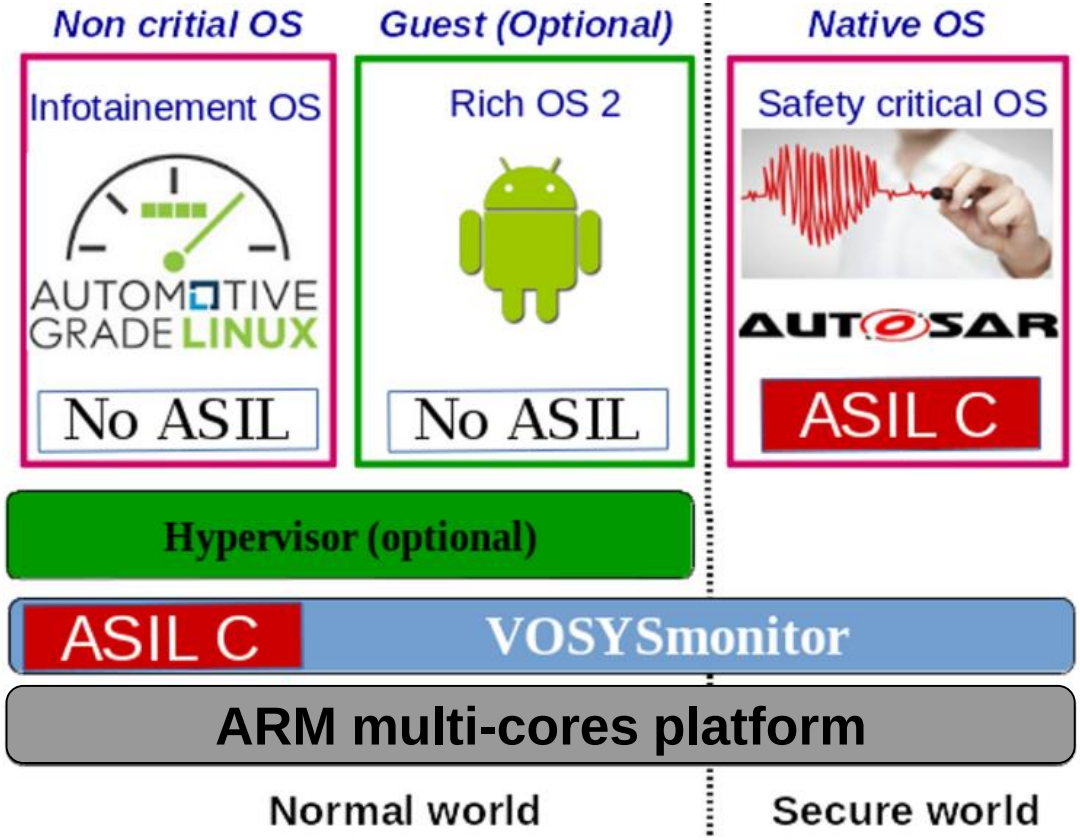
www.virtualopensystems.com

Virtual Open Systems 製品：

VOSYSmonitor

VOSySmonitorは、TrustZoneをベースとした安全規格認証済のバーチャライゼーション・レイヤーです。また、システム全体のセキュリティ・アプローチを可能とするための専用の機能を持ち、特に安全性に注意が払われています。 これにより、セーフティ・クリティカル領域のための最高クラスのプロテクションを保証します。

- 複数のRTOS と GPOSの実行
- ARM TrustZone を利用したセーフティ・クリティカル領域のアイソレーション
- 柔軟な コア/IO アロケーション・ポリシー（スタティック、ダイナミック、コンフィギュラブル/設定可能）
- PSCIを通したパワー・マネージメント
- Linux “warm” リブート機能
- ワールド間のコミュニケーション（バーチャル・ネットワーク・チャンネル）
- 高性能（速いブート・タイム、低割り込み遅延）

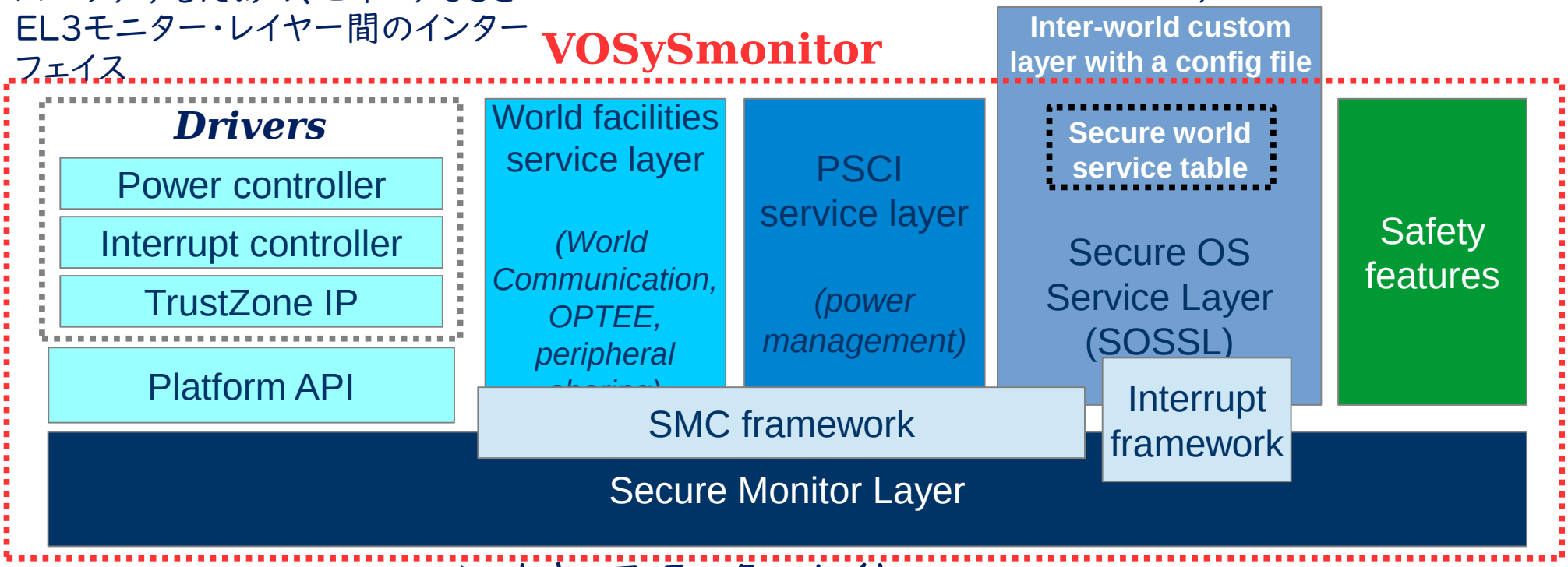


VOSySmonitor ソフトウェア・アーキテクチャー

- **SOSSL**
  割り込みフォワーディングの取り扱いとSMCセキュア・サービスのディスパッチするための、セキュアOSとEL3モニター・レイヤー間のインターフェイス

- **ワールド・ファシリティ・レイヤー**
  両方のワールドで実行されているOSへの高度なサービスの提供

- **PSCI**
  パワー・マネージメント・サービス (パワー ON/OFF コア等々)の提供



- **プラットフォーム API**
  EL3モニター・レイヤーからドライバー・ファンクション・コールをアブストラクトする機能

- **セキュア・モニター・レイヤー**
  ARM アーキテクチャー用に実装され、コンテキスト・スイッチの取扱い、および、トラップされたエクセプションを正しいハンドラーへのルーティングする機能

- **安全機能**
  内部/ハードウェアの障害時、セキュアOSの保持

VOSySmonitor　サービス

VOSySmonitorは、ARM コンベンション/プロトコル に完全に準拠したサービスを提供します。

- ***SMC コーリング・コンベンション(SMCCC):*** ARMv7/v8において、VOSySmonitorとベンダー(例えば、ARM、OEM、SIP)の共存を可能にする目的で、サービス・プロバイダーをパーティションニングするために、SMCのコンベンションを定義 する。
- ***パワー・ステート・コーディネーション・インターフェイス(PSCI):*** VOSySmonitor がパワー・マネージメント・リクエスト(例えば、Linux AArch64 kernelで使われているパワー・コントロール・メソッド)を調停できるように、プロトコルを定義する。
- ***トラスティッド・エグゼキューション・エンバイロメント(TEE):*** OP-TEE (セキュア・ストレージ、暗号化/復号化)の実行をサポートするためのサービス・レイヤーを提供する。

両方のワールドで実行されるOSに、それらの間のやり取りが容易になるような先進的な機能性を提供するために、次のようなカスタムサービスが、VOSySmonitorで、さらにサポートされています。

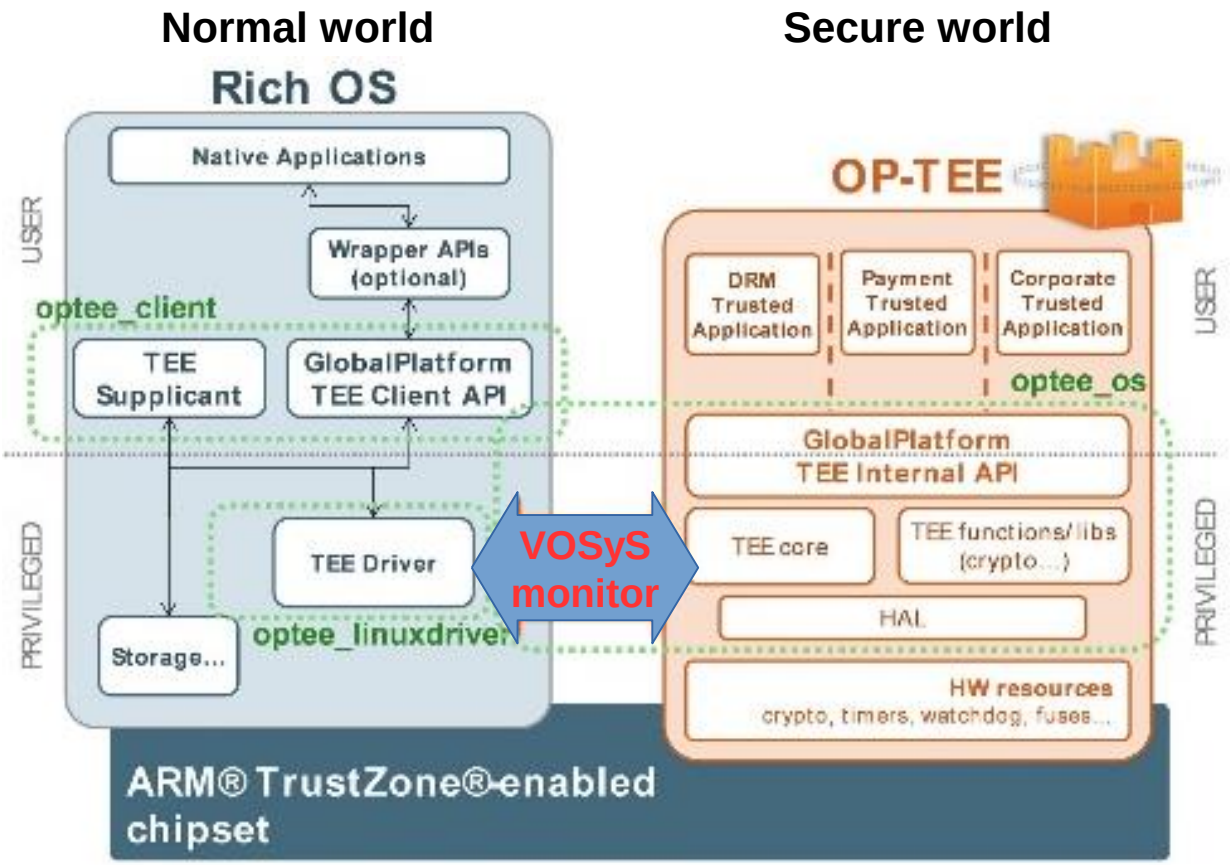
- ***VOSySVirtualNet:*** VOSySmonitor上で統合された両方のシステム間の安全で効率のいい統合されたコミュニケーション・チャンネルを提供します。
- ***セキュア・プロキシ:*** 両方のワールドからのアクセスが必要なペリフェラルを安全にために、そのキャパシティを提供します。

VOSySmonitor – OP-TEE サポート

VOSySmonitorは、ノーマル・ワールドで実行中のリッチOSに、OPTEEセキュア・サービスを提供するために、OPTEE要件に完全準拠のサービス・レイヤーを実装しています。

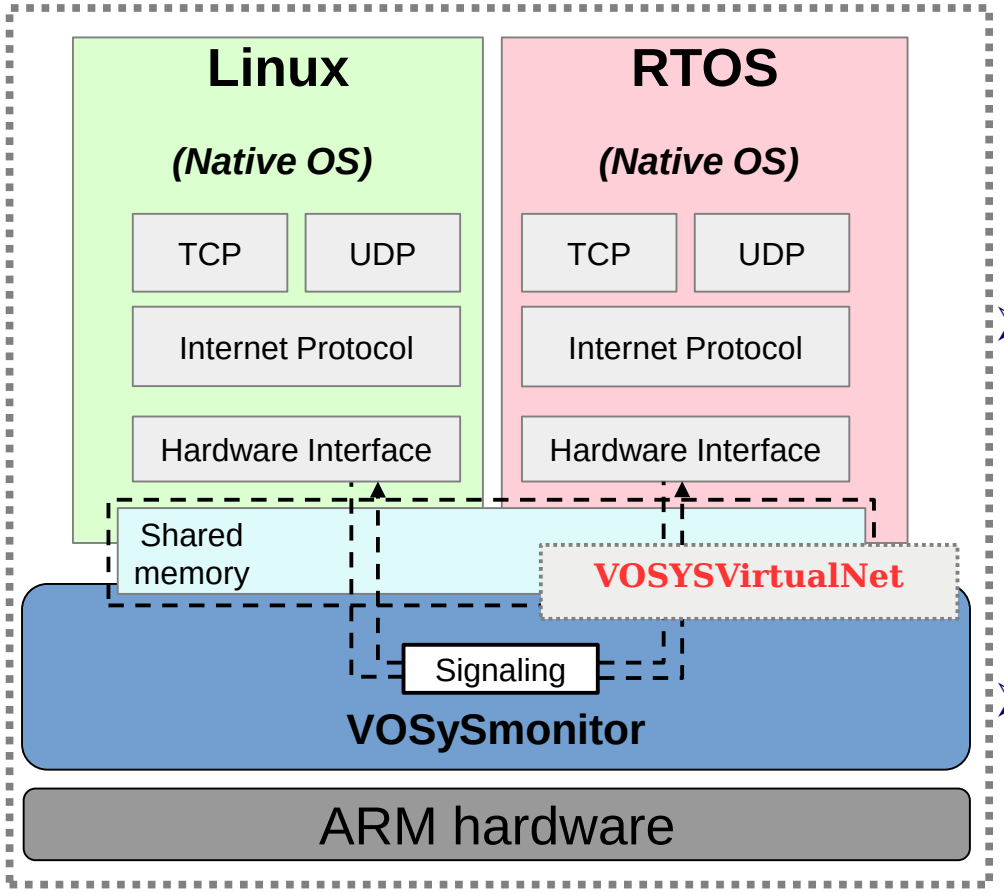
OP-TEE は、ARMアーキテクチャ用のオープン・ソースのTEEです。

- アイソレートされた実行環境のセキュリティの提供
- リッチ OS (セキュア、ストレージ、暗号化/複合化、等々)のためのトラスティッド・サービスをサポート
- GlobalPlatformで定義されたTEE システム・アーキテクチャーに準拠



VOSYSVirtualNet サービス - 概要

VOSYSVirtualNetの目的は、VOSySmonitor上で統合された両方のシステム間の安全で効率のいい統合されたコミュニケーション・チャンネルを提供することです。



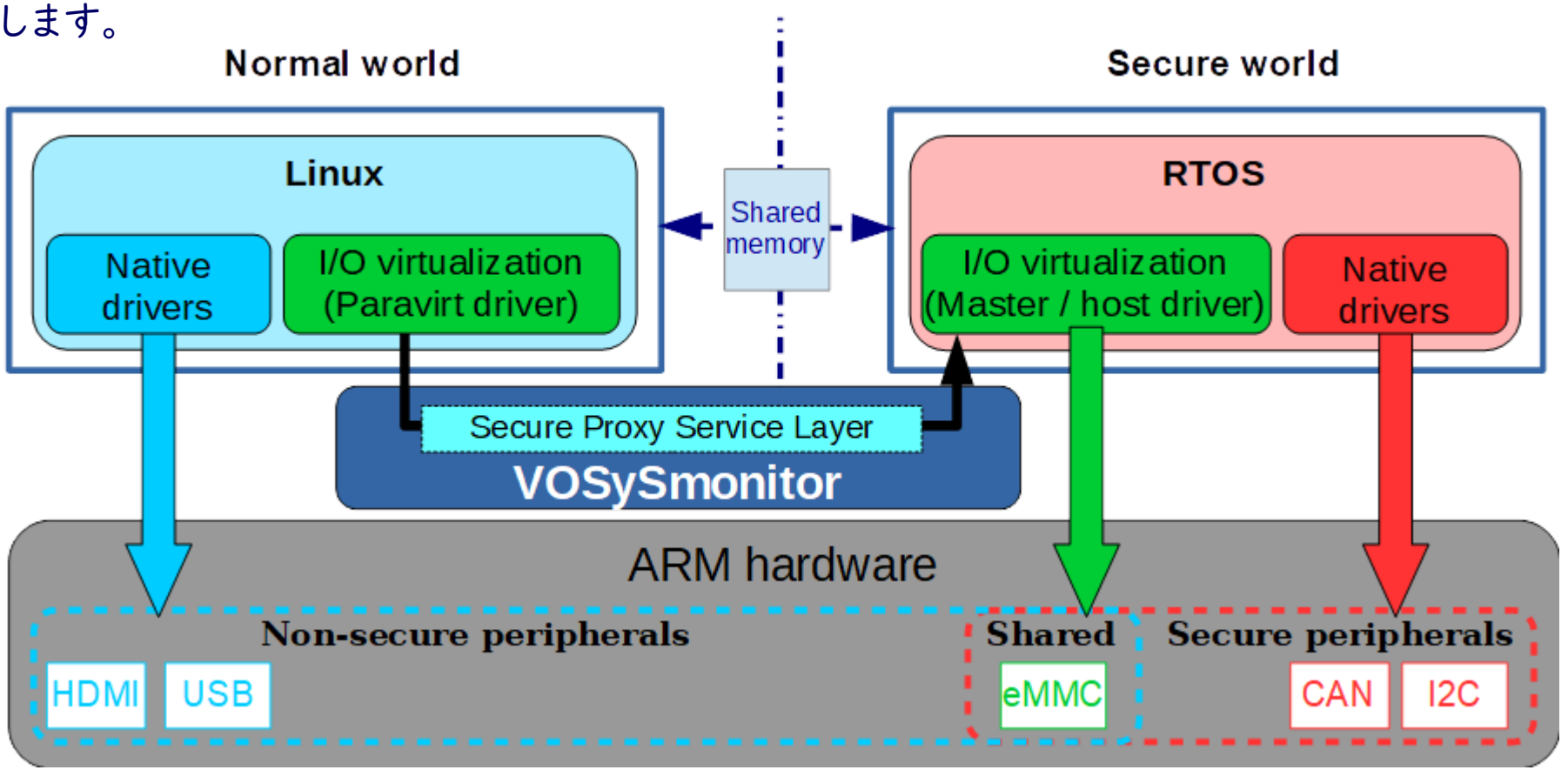
- **ネットワーク・スタックへの完全なインテグレーション:** VOSYSVirtualNetのコミュニケーション・エンドポイントは、透明な仕方で、OSネットワーク・スタックに統合されます。つまり、すべてのアプリケーション・ネットワーク・ツール（すなわち、route、ip、等々）がそのまますぐに使えます。

- **移植可能で、軽量の実装:** シェアド・メモリーをベースとした効率のいい実装とSGI(ソフトウェア生成インタラプト)シグナリングは、VOSySVirtualNetがハードウェアに特に依存しないので、最低限（つまり、Linux kernel アップデート ~10 LoC のみ）の移植/ポーティング作業で済みます。

- **セキュリティー対策:** **それらの対策が**クリティカルOSをコミュニケーション・リンク(つまり、レート・リミッター)を通してクラッシュさせようとする重大なアタックから守るために実装されています。

セキュア・プロキシ・サービス - 概要

- VOSySmonitor が、ノーマル・ワールドから セキュア・ワールド・システムに割り込みの要求とセキュア・メモリーへのアクセスの要求するとき、それができるように セキュア・プロキシ・レイヤーとして、動作します。



- ドライバー・ロジックが、セキュア・サイドに実装されており、ノーマル・ワールドのドライバーは、デバイスに直接アクセスする代わりに、セキュア・プロキ・サービス・レイヤーに適応してコールします。

VOSySmonitor　カスタム対応

VOSySmonitorは、VOSySmonitorの実行とそれぞれのワールドで実行されているシステムの双方のスケジューリングをカスタム化するため、コンパイル時に、ユーザーがそれらの構成/設定が可能である。

- VOSySmonitor上で実行されている異なったシステムに対して、利用可能なコアを割り当て、各々のコアが、ノーマル/セキュア・ワールドでの実行において、共有可能か判断する。.
- VOSySmonitorのいくつかの機能(例えば、セーフティ機能、VOSySVirtualNet、セキュア・プロキシ、OPTEE)が、貴社の製品にて、VOSySmonitor フットプリントが最適となるよう、貴社の必要に応じて、イネーブル/ディスエーブルが可能。
- 貴社の要望(例えば、セルフテストの実行、VOSySVirtualNetのレート・リミッター等)に合わせて、VOSySmonitor 機能を構成する。
- それぞれのARM ワールドで実行されているアプリケーションに対し、CPUモードとエントリー・ポイントを定義する。

VOSySmonitor　環境

- VOSySmonitorはのコンパイラー下記でコンパイル可能です。

✓ ARM コンパイラー 6

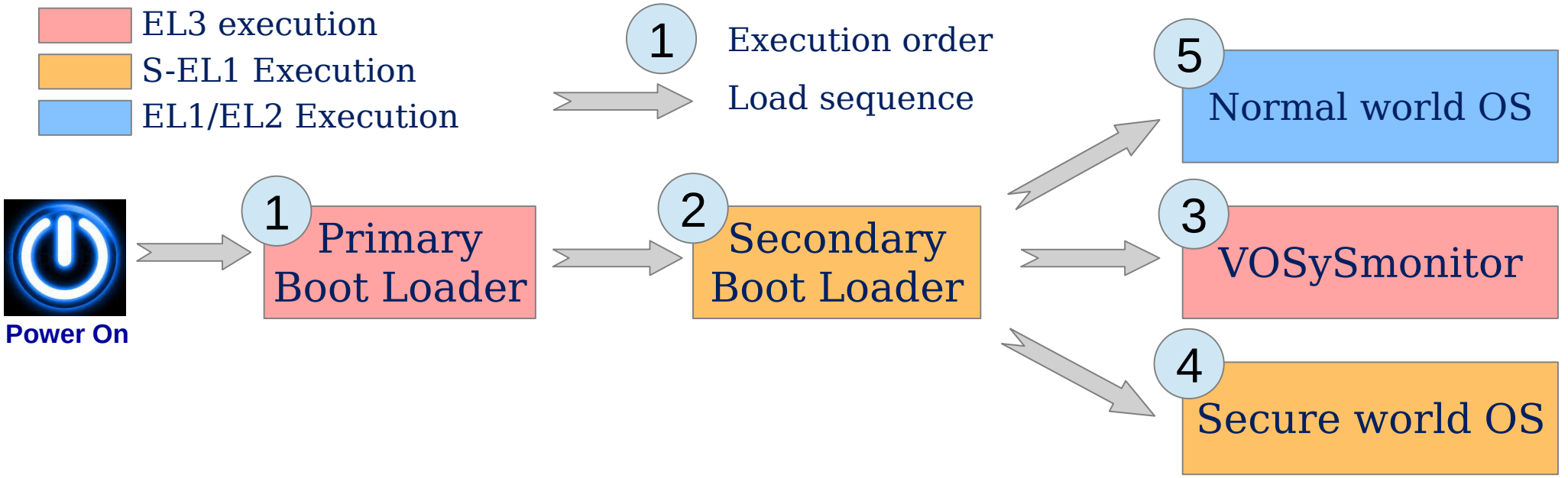
これは、安全規格準、以下拠で、ユーザーが認定作業無しで、安全規格関連の開発に対応できるコンパイラーです。

✓ GCC コンパイラー

これは、セキュリティー要件のないプロジェクトや評価用に適した無償のソフトウェアです。

- VOSySmonitorは、次のようなプラットフォームでの実績があります。
  - ✓ (ARMv8) - メディアテック社 Autus I20 (MT2712)
  - ✓ (ARMv8) - ARM社 JUNO Development board
  - ✓ (ARMv8) - ルネサス社 R-CAR H3/M3 board
    ISO-26262 (ASIL-B) 認証済
  - ✓ (ARMv8) - エヌビディア社 Jetson Tegra X1
  - ✓ (ARMv8) - ザイリンクス社 Ultrascale+
  - ✓ (ARMv7) - ルネサス社 RZ/N1D
  - ✓ (ARMv7) - アルテラ社 Cyclone V

VOSySmonitor　ブート・シークエンス



- 一次ブート・ローダーは、信頼連鎖の最初のステップであり、それは、単純なリプログラミング・アタックでは、変更したり置き換えたりされない唯一のコンポーネントである SoC のROM内にあります。
- 一旦、認証されると、RAM メモリにある二次ブート・ローダーが、異なったシステム・イメージをローディングし認証する役割で、そして、RTOS/GPOS の同時実行を管理する役割のVOSySmonitorにそのコントロールをさせます。

VOSySmonitor 差別化要因

VOSySmonitorにより、オートモーテイブやミクスト・クリティカリティ・システム用のECUの統合が可能になります。 いかなる既存で商用のバーチャライゼーション・ソリューションと比べて、セーフティ・クリティカル領域のより強力なアイソレーションが実現できます。

- ARM TrustZoneをベースとした強力なアイソレーション:
  VOSySmonitorパーティション・システムのリソースにより、セーフティー・クリティカル環境への無許可のアクセスの防止。
- **モジュラー型でオープンのアーキテクチャー ：**
  いかなるOS、**ツール**やﾀｲﾌﾟ 1 –ハイパーバイザのどれにも、クリティカル・ワールドとノンクリティカル・ワールドを混同させることは、ありません。
- **コスト低減:**
  クリティカル・リソースのアイソレーション、安全性、性能にフォーカスしたボトムアップ・ソリューションを提案; ユースケースに必要なものだけのコストで!

ARMv8-A/ARMv7-A TrustZone プラットフォームへ移植可能で、デザインにより、認証可能です。 VOSySmonitor v2.5が、現在入手可能です。また、 ASIL C認証済みのルネサス社R-Car gen 3 プラットフォームも入手可能です。

ISO 26262

VOSySmonitor
ターゲットとするマーケット・セグメント

ドローン

ドローンでは、メインのコントロールOSがクラッシュした場合、セーフティ・ソフトウェア（つまり、離着陸、飛行、帰着、等々）を実行します。

交通手段

交通手段やオートメーションにおけるミクスト・クリティカリティ・システムでは、VOSySmonitorのアドバンテージを利用できます。

VOSySmonitor

オートモーテイブ

VOSySmonitorにより、インフォーテインメント、クラスター機能およびECUが、単一のプラットフォームに統合できます。

インダストリアル および オートメーション

industrial AUTOMATION

ロボット、サーキット・ブレーカーにおいて、ヒューマン・インターフェイス・モジュール（HMI）と過電圧監視等を取り扱います。

contact@virtualopensystems.com

Web: virtualopensystems.com

Products: http://www.virtualopensystems.com/en/products/

Demos: virtualopensystems.com/en/solutions/demos/

Guides: virtualopensystems.com/en/solutions/guides/

Research projects: virtualopensystems.com/en/research/innovation-projects/