

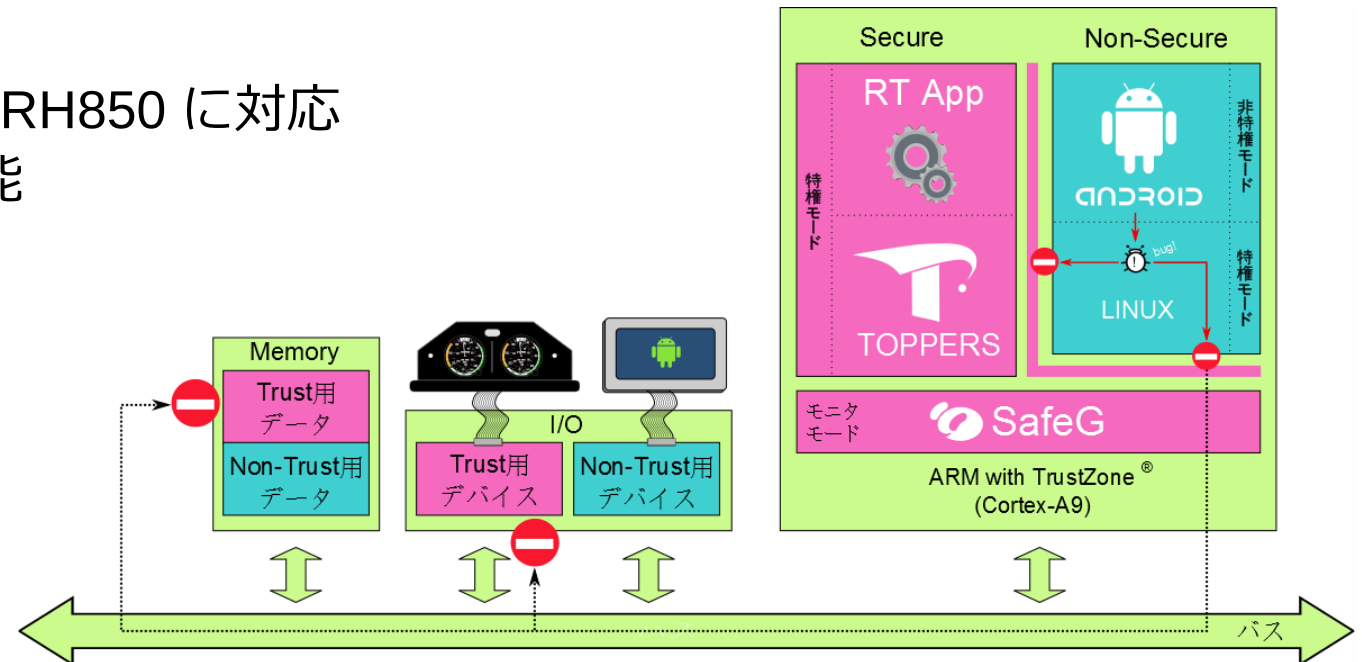
Xtensaのセキュリティ機構を用いた デュアルOSモニタSafeG-XLSを開発

本田 晋也
南山大学/名古屋大学
TOPPERSプロジェクトシニアテクニカルエキスパート

SafeG

TOPPERSプロジェクトで公開している一連のDual-OS環境

- SafeG/SafeG64
 - 32/64bit ARM-Aプロファイルに対応
- SafeG-M
 - ARM-Mプロファイルに対応
 - Secure側のRTOSにハイパーバイザーの機能をもたせる
- SafeG-AUTO
 - ルネサスエレクトロニクス RH850 に対応
 - N個の仮想マシンを実現可能

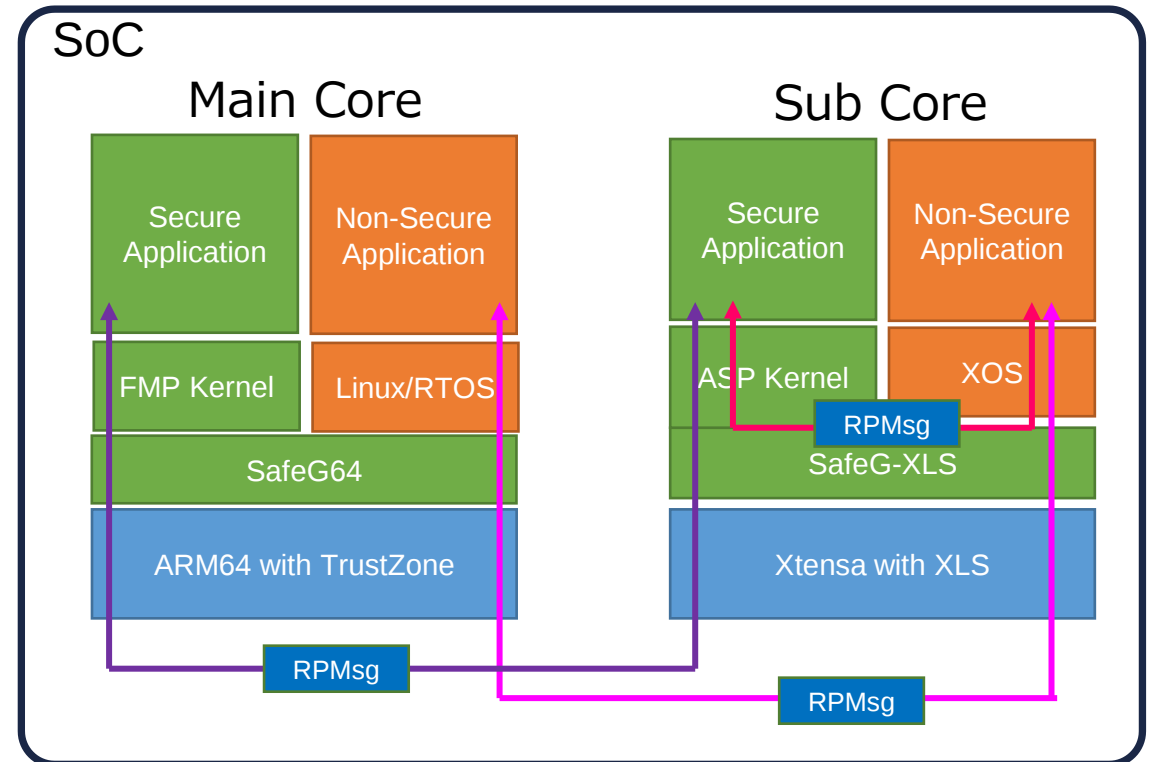


SafeG-XLS

Xtensaのセキュリティ機構を用いたデュアルOSモニタ

特徴

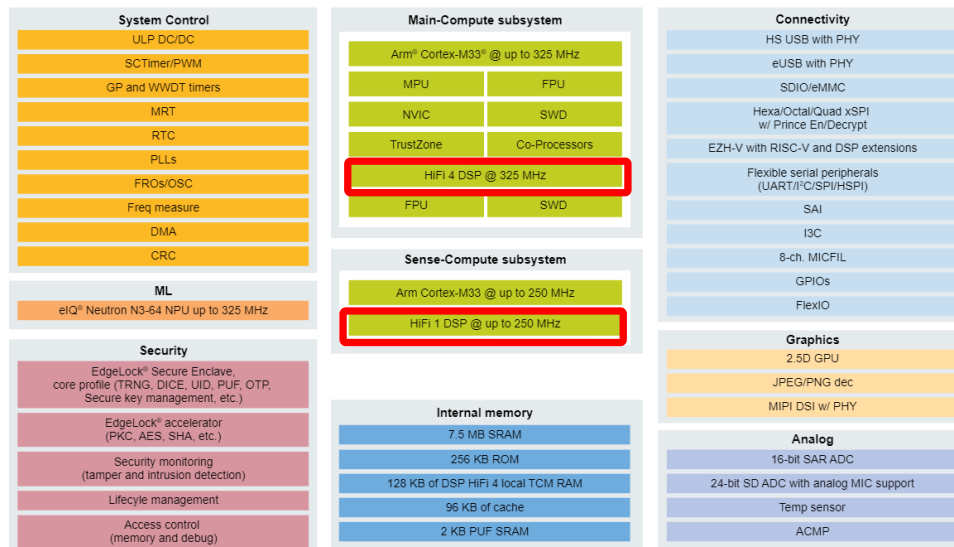
- SafeGの設計コンセプトを踏襲
- Secureで動作するASP3カーネルを拡張してデュアルOSモニタを実現
- Secure側はNonSecure側から保護される
- サブコアとしての実行に対応
 - メインコアはARM+SafeGにより実行
 - メインコアのSecure/NonSecureワールドそれぞれにサービスを提供
 - コア間通信にRPMsgを採用
- NonSecure側の変更は少ない



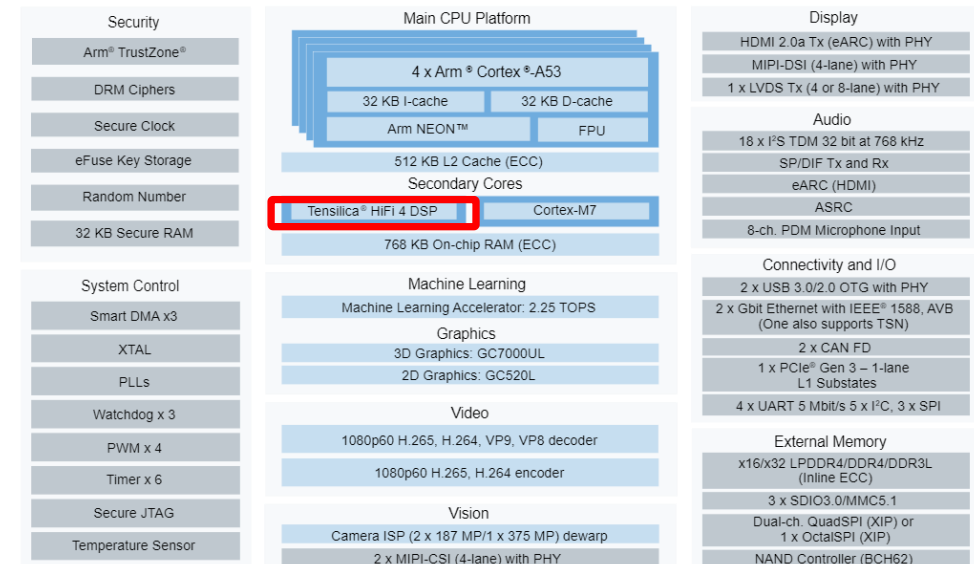
Cadence Tensilica Xtenza

- コンフィギュラブルプロセッサ
 - DSP命令やVLIW命令を追加可能
 - ユーザー独自の命令も追加可能
- サブコアとしての利用
 - メインプロセッサ（ARM等）に対して，音声やAI処理を提供
 - メインプロセッサではSecureとNon-Secureワールドが動作する

i.MX RT700

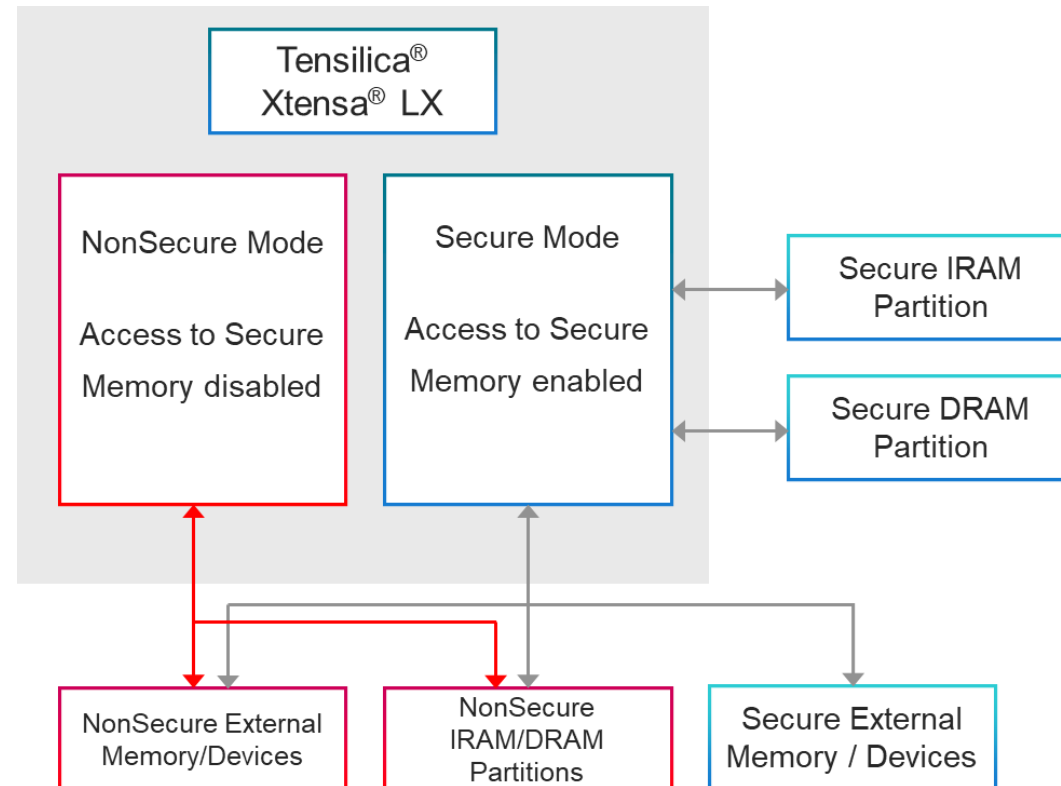


i.MX8M plus



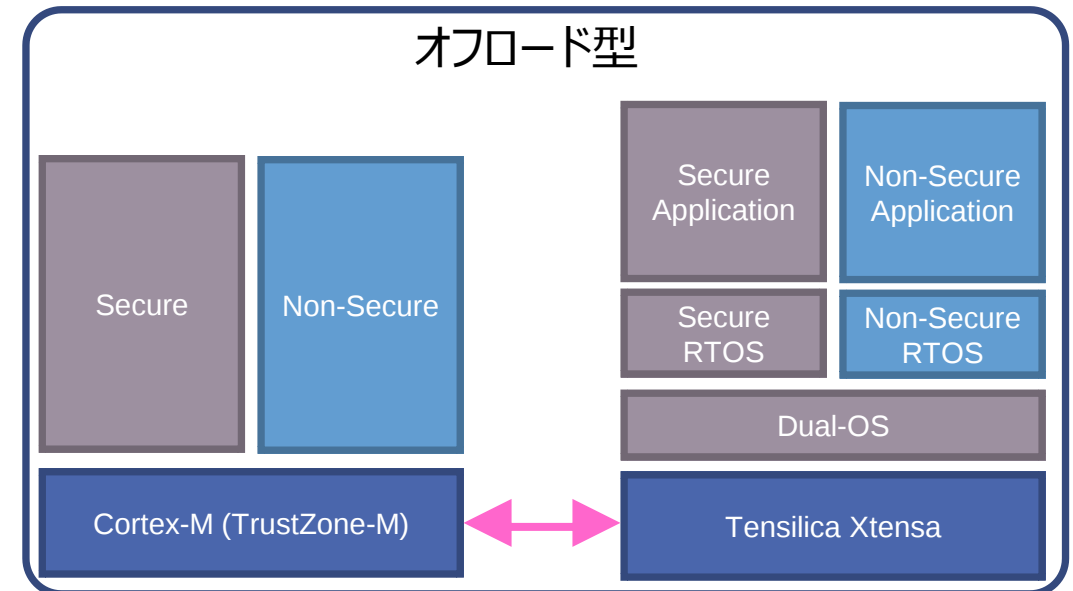
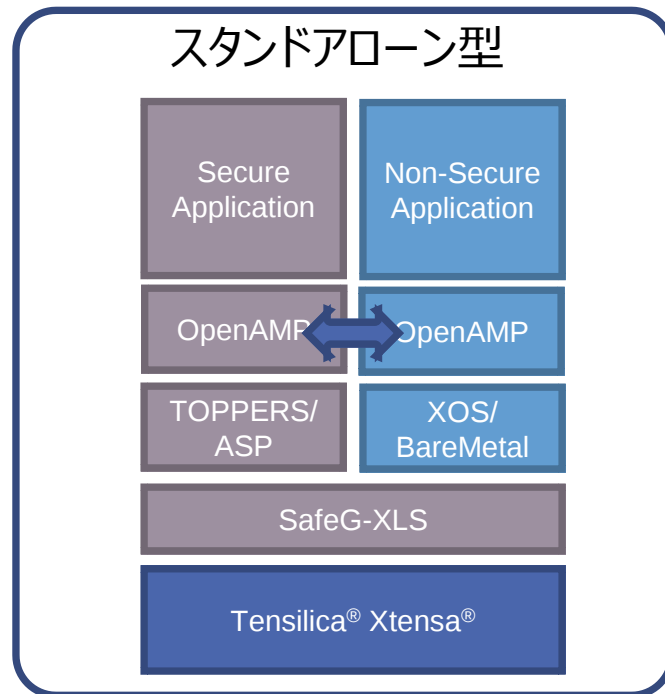
Cadence Tensilica Xtensa LX Secure Mode (XLS)

- TrustZoneと同様にCPU内を2種類のワールドに分割
 - Secureモード：システムの全てのリソースにアクセス可能
 - Non-Secureモード：システムの一部のリソースにアクセス可能
- それぞれのモードで別のOSを動作させDual-OS環境を実現可能
 - 別々のバイナリを実行可能（ソフトウェアへのパッチは必要）



機能

- OS間通信機能の実現
 - OpenAMP (RPMAG) を利用
 - ヘテロジニアスマルチプロセッサ間の通信機構
 - ロックフリー
- オフロード型ハイパーバイザー
 - 基本構成はスタンドアローン型と同じ
 - メインプロセッサでSecure/NonSecureが動作する場合を想定してスケジューリングや通信機能を検討.



まとめ

- Cadence Tensilica Xtensa LX Secure Mode (XLS) に対応した Dual-OS環境 SafeG-XLSの紹介
- 既存のRTOSを拡張
 - ハイパーバイザーを別途用意しない
 - 様々なスケジューリングが可能
 - Secure側のタスクのスケジューリング機能を利用
- Dual-OSの要件への対応
 - 空間保護, 時間保護, 独立したバイナリの実行, 変更量が少ない

