こんにちは。このプレゼンテーションでは、STM32U5 での TF-M のご提案について、詳しく説明します。

STM32U5 TFM の概要

- 基本的な SBSFU サンプルから完全な TFM サンプルまでモジュール式/設定可能
- 幅広いセキュリティ概念：
  - リセット時はシングルエントリポイントとします。強制的にコード実行してセキュアブートコードを起動します。
  - TFM_SBSFU_Boot コードと改変不可の「機密情報」：変更または改変ができません。
  - 3 つの保護/隔離ドメイン：
    - PSA で不変の信頼の起点（RoT）を実行するためのセキュア・ドメインと特権ドメイン
    - PSA で更新可能な RoT を実行するためのセキュア・ドメインと特権ドメイン
    - アプリケーションで更新可能な RoT を実行するためのセキュア・ドメインと非特権ドメイン
  - アプリケーションの状態に応じた実行面の制限：
    - TFM-SBSFU コード：リセットからインストールされたアプリケーションの確認まで
    - アプリケーションのセキュア/非セキュアコード：インストールされたアプリケーションが確認された場合
  - デバイスへの JTAG アクセスを除外します。
- ソフトウェアおよび物理的攻撃に対する保護

life.augmented

2

暗号は、整合性、認証、機密性を保証します。
しかし、暗号の使用だけでは不十分です。考えうる攻撃に対抗するには、重要な操作、機密データ（秘密鍵など）、および実行フローを保護するために、一連の対策とシステムレベルの戦略が必要です。
Cortex-M（または TF-M）用の信頼できるファームウェアに基づいたセキュア・ブートおよびセキュア・ファームウェア更新（または SBSFU）ソリューションは、モジュール式で設定可能なフレームワークを提供しており、このセキュリティ概念については後述します。
3 つの保護され、隔離されたドメインが作成されます。

- セキュア/特権：関連付けられた秘密鍵を使用して PSA で不変の RoT コードを実行し、またセキュアな特権 STM32U5 ペリフェラルを使用します。このドメインは、不変の PSA RoT コードの実行が完了すると、非表示になります。
- セキュア/特権：関連付けられた秘密鍵を使用して PSA で更新可能な RoT コードを実行し、またセキュアな特権 STM32U5 ペリフェラルを使用します。
- セキュア/非特権：アプリケーションで更新可能な RoT とそれに関連付けられた秘密鍵を実行し、またセキュアな非特権 STM32U5 ペリフェラルを使用します。

実行面はアプリケーションの状態に応じて制限されています。

- 製品のリセットからインストールされたアプリケーションが検証されるまで：TFM_SBSFU_Boot コードのみを実行できます。
- インストールされたアプリケーションが確認された場合：アプリケーション・コード（セキュア部分と非セキュア部分）を実行できます。

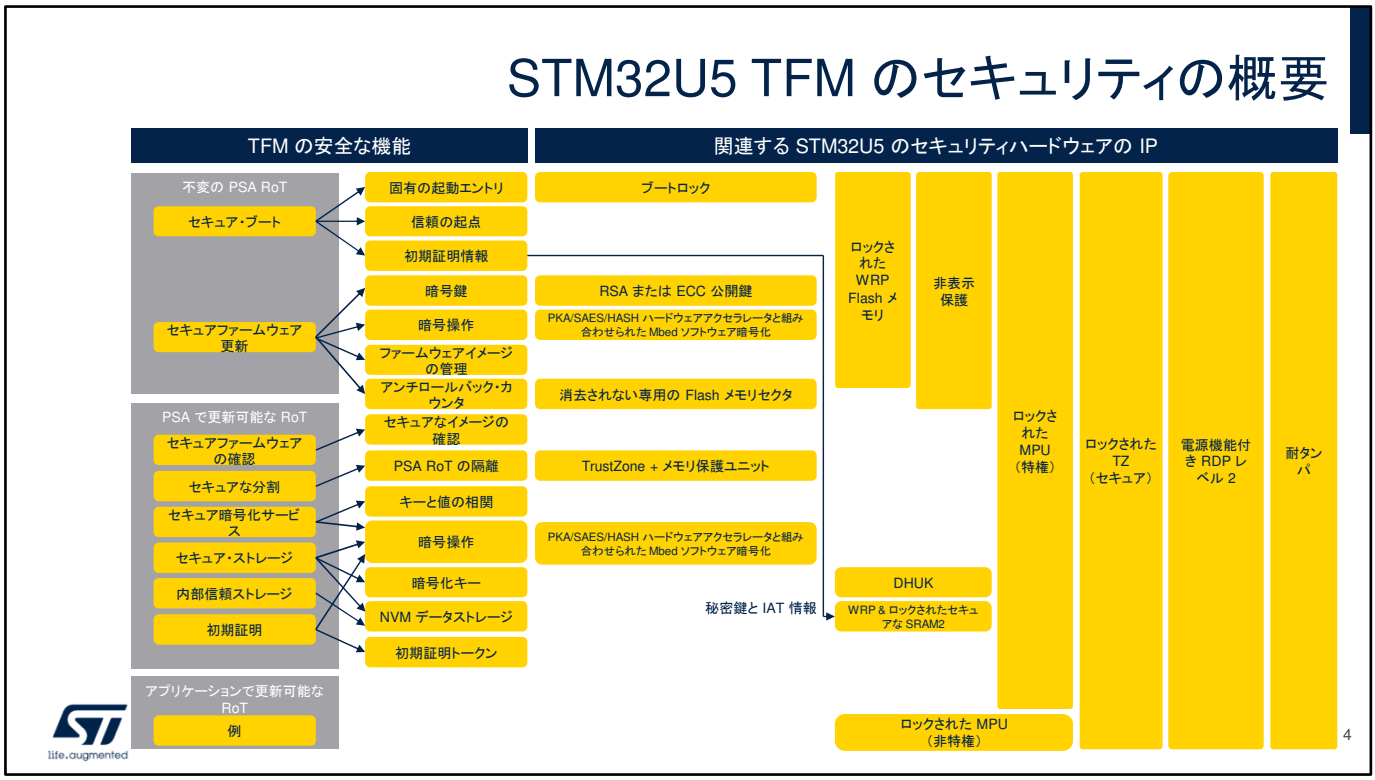
STM32U5 は、ソフトウェアおよび物理的攻撃に対する保護も備えています。

STM32U5 TFM の上面図

STM32U5Cube ファームウェアへの TFM 実装は、ARM TF-M のリファレンス実装に基づいています。
この上面図に、前のセクションで説明したすべての TFM コンポーネントをまとめています。
STM32CubeU5 パッケージでは 2 つのアプリケーションを提案しています。

- TFM：TFM の完全なサービスを備えたアプリケーション
- SBSFU：ARM TF-M のセキュア・ブートおよびセキュア・ファームウェア更新サービスのみを備えたアプリケーション

この図では、Tera Term HyperTerminal を使用してツールセットと接続し、サンプルの設定、実行、実行結果の表示を行っています。
サンプルとヘルプについては、次の UM2851 ユーザマニュアルを参照：
STM32CubeU5 TFM アプリケーション入門



この図では、TFM の安全な機能と、外部および内部への攻撃に対する保護メカニズムを強化するために STM32U5 デバイスに統合されたハードウェアセキュリティの IP の詳細を示しています。
TF-M は、Arm Limited 社が推進するオープンソースのソフトウェアフレームワークであり、Arm® Cortex®-M33 プロセッサに PSA 標準のリファレンス実装を提供します。

- PSA の不変の RoT（信頼の起点）は、どのリセット後にも実行される不変の*「セキュア・ブートおよびセキュア・ファームウェア更新」*アプリケーションです。
- PSA で更新可能な RoT は、セキュア/特権環境に隔離された一連のセキュアサービスを実装する*「セキュア」*アプリケーションで、以下の PSA API 経由で非セキュアアプリケーションのランタイムに非セキュアアプリケーションによってコールされる場合があります。
  - セキュア・ストレージ・サービス
  - 内部信頼ストレージサービス
  - 暗号化サービス
  - 初期証明サービス
- アプリケーションで更新可能な RoT は、セキュア/非特権環境に隔離され、非セキュアアプリケーションのラインタイムに非セキュアアプリケーションによってコールされる場合がある、サードパーティのセキュアサービスです。

図の右側は、安全に関するさまざまな機能に関連するセキュリティハードウェアの IP について詳しく説明しています。

外部攻撃からの保護

- 外部攻撃の定義 = デバッガやプローブなどの外部ツールによる攻撃
- STM32U5 TFM SBSFU サンプルに実装されている 4 つの保護メカニズム（黄色）:

デバイスのライフサイクル

- 4 つの RDP レベル
- RDP2 の最高保護
- RDP2 でのデバイスへの JTAG のアクセスなし
- プロビジョニングされた場合、OEM パスワードで回帰可能

ブートロック

- **BOOT_LOCK** はデバイスユーザオプションバイト（OB）
- OB によって定義されたメモリ位置への固定エントリポイント
- TFM の場合：リセット後のブートエントリポイントを **TFM_SBSFU_Boot コード**に固定

保護された SRAM2

- RDP1 への侵入対策
- 侵入が検出時に消去
- SRAM2 WRP：有効な場合、内容は次のリセット時まで凍結
- TFM の場合：TFM_SBSFU_Boot とセキュアアプリケーションの間で初期証明情報を共有し、凍結するために使用

耐タンパ

- 機密データを物理的な攻撃から保護するために使用
- TFM_SBSFU_Boot の開始時に有効化
- TFM_Appli および TFM_Loader の適用中はアクティブなまま
- タンパ検出時：SRAM2、キャッシュ、および暗号ペリフェラルが消去され、強制的に再起動される
- タンパは内部イベントまたは外部ピンの場合がある

DAP 無効化 + IWDG

STM32U5 デバイスで使用可能な、TFM では使用されないセキュリティ機能：

- DAP の無効化
- ブート時間を制御するための IWDG

life.augmented

5

このスライドでは、デバッガやプローブなどのツールによる外部攻撃から保護するために使用されるメカニズムについて説明します。
デバイスライフサイクル機能は、最高の保護レベルを実現するために、読出し保護レベル 2 に基づいています。
OEM2 パスワード機能を備えた読出し保護レベル 2 は、OEM2 パスワードを挿入する場合を除いて JTAG デバッガがデバイスにアクセスできないようにするために使用されます。
RDP レベル 2 では、OEM2 パスワードが JTAG ポートに挿入されると、RDP レベルはレベル 1 に戻ります。
RDP レベルが 0 の場合は、最初に OEM2 パスワードをプロビジョニングしておく必要があります。
ブートロック機能は、BOOT_LOCK オプション・バイトに基づいており、オプション・バイトで定義されたメモリ位置にエントリポイントを固定するために使用されます。
TFM アプリケーションの例では、リセット後のブートエントリポイントは TFM_SBSFU_Boot コードに固定されます。
システムが RDP レベル 1 で設定されると、SRAM2 は自動的に侵入から保護されます。
SRAM2 の内容は、侵入が検出されると直ちに消去されます。さらに、SRAM2 の内容は、ロックビットを有効にすることで、次のリセットまで書込み保護可能です。
TFM アプリケーションの例では、システムは保護された SRAM2 を使用して、TFM_SBSFU_Boot アプリケーションとセキュアアプリケーションの間で初期証明情報を共有し、凍結するように設定されています。
耐タンパ保護は、機密データを物理的な攻撃から保護するために使用されます。TFM_SBSFU_Boot の開始時に有効化され、TFM_Appli および TFM_Loader の適用中はアクティブなままです。
タンパが検出されると、SRAM2、キャッシュ、および暗号ペリフェラル内の機密データが直ちに消去され、強制的に再起動されます。
外部のアクティブタンパピンと内部タンパイベントの両方が使用されます。
外部攻撃から製品を保護するために、他の STM32U5 ペリフェラルも使用できますが、現在の TFM サンプルでは使用しません。

- デバッグ保護とは、デバッグアクセスポートを無効にすることです。無効にすると、JTAG ピンは内部バスに接続できなくなります。DAP は RDP レベル 2 では自動的に無効になります。
- 独立型ウォッチドッグ（IWDG）はフリーランニングダウンカウンタです。一度起動すると停止できません。定期的な更新が必要で、怠るとリセットされます。このメカニズムを使用して、TFM_SBSFU_Boot の実行時間を制御できます。

内部攻撃からの保護

- 内部攻撃の定義 = STM32 で実行しているコードによる攻撃
  - 攻撃の原因:
    - 不具合やセキュリティ欠陥を悪用する悪意のあるファームウェア
    - 不要な操作

- TFM で使用される内部攻撃からのハードウェア保護:
  - **TZ**(TrustZone®)
  - **MPU**(メモリ保護ユニット)
  - **SAU**(セキュリティ属性ユニット)
  - **GTZC**(グローバル TrustZone® コントローラ)
  - **WRP**(書込み保護)
  - **HDP**(非表示保護)

life.augmented

6

内部攻撃とは、STM32 で実行しているコードによる攻撃を指します。
攻撃は、不具合やセキュリティ欠陥を悪用する悪意のあるファームウェアや、不要な操作による場合があります。
TF-M は、内部攻撃に対し、次の保護を提供します。

- ARM TrustZone により、厳密に分離されたセキュア環境と非セキュア環境の 2 つの実行環境が有効になります。
- MPU を使用して、Flash や SRAM のメモリマップを個別の特権アクセス許可を持つ領域に分割することで、組込みシステムの堅牢性が向上します。
- SAU により、アドレス範囲にセキュリティ属性が割り当てられます。
- GTZC ファイアウォールにより、ペリフェラルとメモリを対象としたトランザクションのセキュア属性と特権属性がチェックされます。
- 書込み保護を使用して、外部からの攻撃や、重要なコード／データの不要な書込み／消去操作などの内部変更から、信頼できるコードを保護します。
- この HDP 領域で実行されるコードと、それに関連する関連データとキーを、ブート後から次のシステムリセット時まで非表示にします。

STM32CubeU5 TFM の設定機能

- STM32Cube U5 マイクロコントローラ・パッケージによる、2 つの異なるアプリケーション例の提案
  - TFM：完全な TF-M サービスを備えたアプリケーション
  - SBSFU：TF-M のセキュア・ブートおよびセキュア・ファームウェア更新サービスのみを備えたアプリケーション

機能	完全な TFM_SBSFU_Boot
暗号方式	RSA 2048、RSA 3072、EC 256
イメージ暗号化	AES-CTR、なし
暗号化モード	ソフトウェア、混合ハードウェア/ソフトウェア、DPA ハードウェア暗号化 SAES+PKA、SAES への HUK 直接接続
スロットモード	プライマリ専用スロット（アクティブなイメージは上書きされる） プライマリおよびセカンダリ・スロット（OTA FW 更新 UC の有効化）
イメージ数モード	1 つのイメージ（セキュア + 非セキュア）、2 つのイメージ（独立したセキュア + 非セキュアなイメージ）
Flash メモリの設定	内部 Flash メモリ + 外部 Flash 機能
イメージのアップグレード方法	上書き専用、スワップ
ローカル・ローダ	Ymodem、なし
耐タンパ	なし、内部タンパのみ、内部および外部タンパ

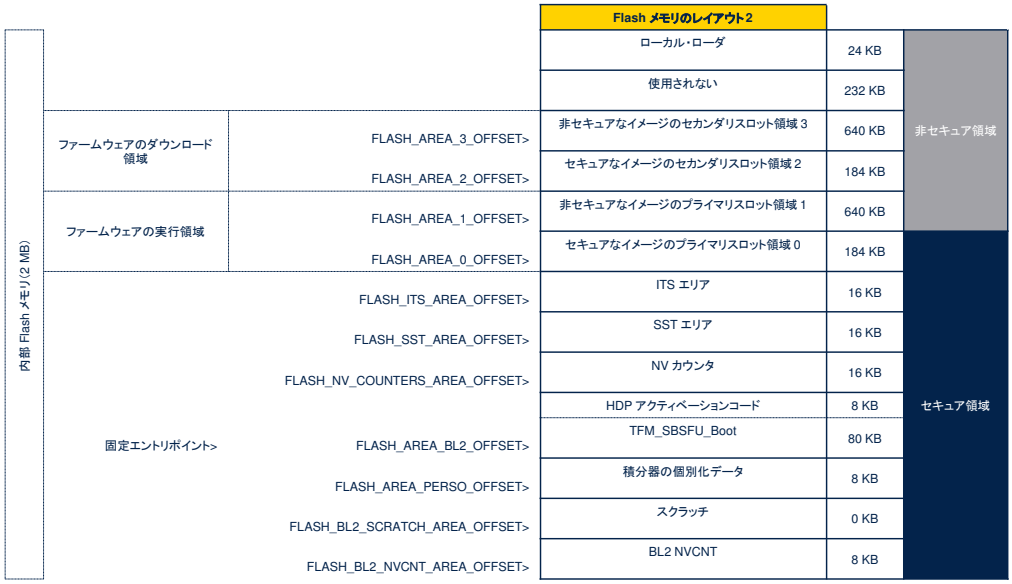
life.augmented

7

STM32Cube U5 マイクロコントローラ・パッケージには、2 つの異なる例が用意されています。
- TFM アプリケーションは、[TF-M] の完全実装です。
- STM32CubeU5 SBSFU という TF-M のセキュア・ブートおよびセキュア・ファームウェア更新機能のみを実装する 2 番目のアプリケーションも使用できます。

この表は、セキュア・ブートおよびセキュア・ファームウェア更新アプリケーションの主な機能を示しています。

TFM サンプルの Flash メモリのレイアウト（デフォルト設定）



life.augmented

8

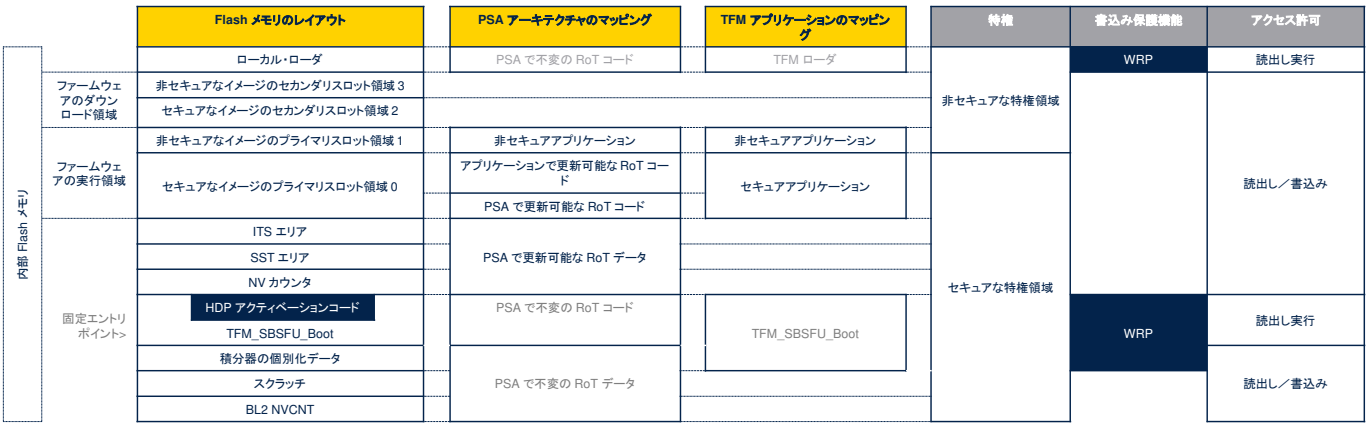
STM32CubeU5 TFM アプリケーションは、さまざまな領域を定義する Flash メモリのレイアウトに依存しています。
Flash メモリのレイアウトは、スロットモード、イメージの数、イメージのアップグレード方法、およびローカル・ローダの有効化によって異なります。
TFM アプリケーションでのこれらの機能のデフォルト設定は、次のとおりです。

- スロットモード：プライマリおよびセカンダリスロット
- イメージ数モード：2 つのイメージ
- イメージのアップグレード方法：上書き専用モード
- ローカル・ローダ：Ymodem

各領域には特定の用途があります。

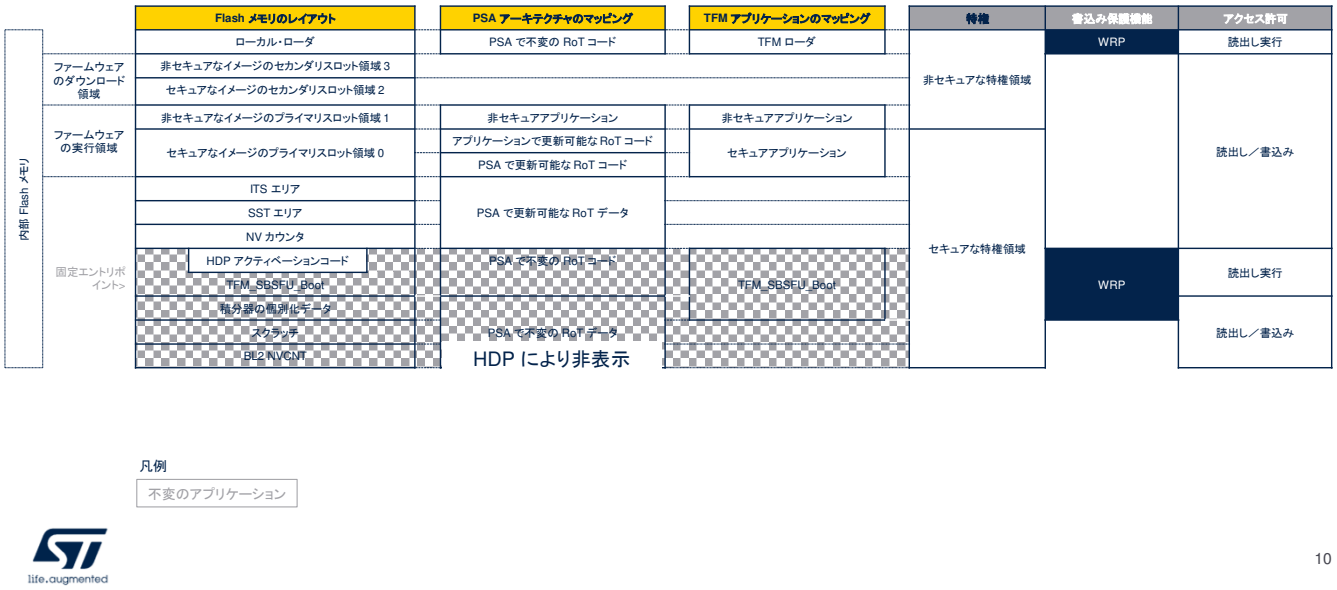
- **BL2 NVCNT 領域**：最後にインストールされた（セキュア／非セキュア）イメージバージョンに関する不揮発性情報を取得します。
- **SCRATCH 領域**：TFM_SBSFU_Boot で、イメージスワップ処理中にイメージデータを一時的に格納するために使用されます。
- **積分器の個別化データ**：積分器固有または STM32U5 固有の TF-M データを個別化します。
- **TFM_SBSFU_Boot バイナリ**：TFM_SBSFU_Boot コードバイナリをプログラムします。
- **NV COUNTER**：セキュアアプリケーションが、SST サービスによって使用される不揮発性カウンタを管理します。
- **SST 領域**：セキュア・ストレージ・サービスの暗号化されたデータが格納される領域。
- **ITS 領域**：内部の Trusted Storage サービスのデータが平文で格納される領域。
- **セキュアなイメージのプライマリスロット**：「アクティブ」なファームウェアのセキュアなイメージをプログラミングするための領域。
- **非セキュアなイメージのプライマリスロット**：「アクティブ」なファームウェアの非セキュアなイメージをプログラミングするための領域。
- **セキュアなイメージのセカンダリスロット**：「新しい」ファームウェアのセキュアなイメージをプログラミングするための領域。
- **非セキュアなイメージのセカンダリスロット**：「新しい」ファームウェアの非セキュアなイメージをプログラミングするための領域。
- **非セキュア・ローカル・ローダ**：TFM_Loader の非セキュアコードバイナリをプログラミングする領域。
- **セキュア・ローカル・ローダ**：TFM_Loader のセキュアコードバイナリをプログラミングする領域。

TFM_SBSFU_Boot アプリケーション実行中の保護スキーム



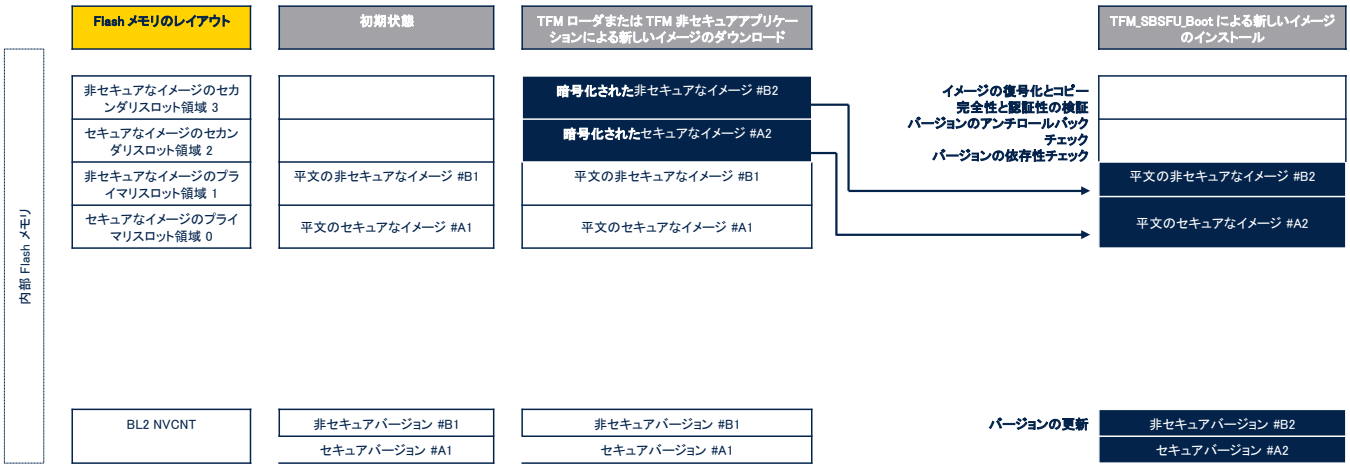
TFM_SBSFU_Boot の実行中、不変のローカル・ローダによって実行できる Flash メモリ領域は、TFM_SBSFU_Boot コード領域のみです。
この図では、TF-M 領域ごとの保護機能を示しています。
ローカル・ローダとファームウェアのダウンロード領域、および非セキュアアプリケーション領域は、非セキュアおよび特権としてマークされています。
Flash の残りの部分は、セキュアおよび特権としてマークされています。
ローカル・ローダと TFM SBSFU ブート・プログラム、ならびに積分器の個別化データ領域は書込み保護されています。
ローカル・ローダと TFM SBSFU は、実行できる唯一の領域です。

TFM_SBSFU_Boot アプリケーション実行中の保護スキーム



TFM_SBSFU_Boot アプリケーションを終了してセキュアアプリケーションに戻ると、TFM_SBSFU_Boot の実行に使われた Flash メモリ領域はすべて非表示になり、セキュアおよび非セキュアなプライマリスロット領域での実行が許可されます。
すべての実行および遷移のケースに対応する詳細な保護スキームは、UM2851 に記載されています。

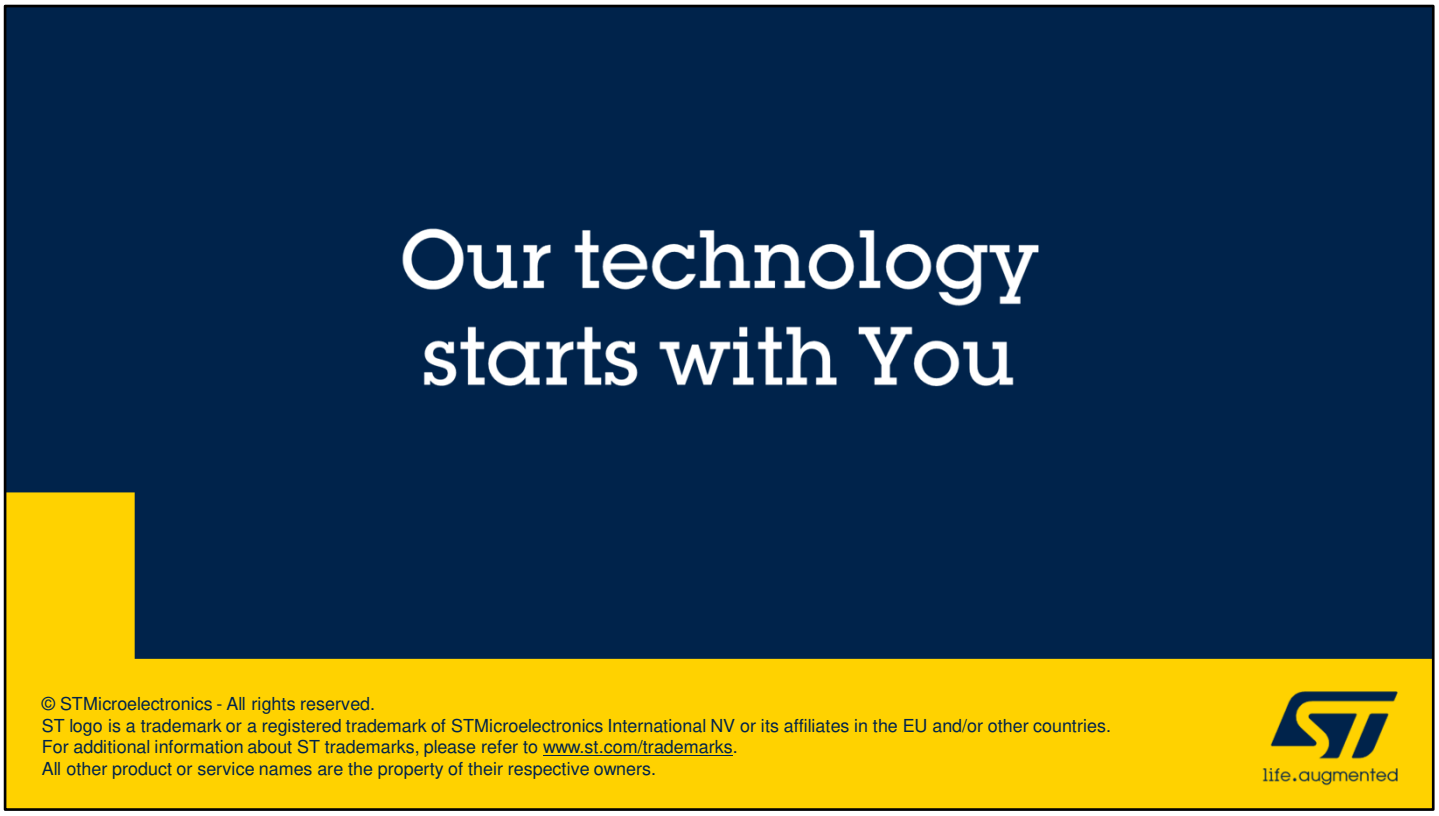
デフォルトの TFM 設定を使用したファームウェアイメージの更新



life.augmented

11

ファームウェアイメージを更新するメカニズムは、イメージの数、イメージのアップグレード方法、およびスロットモードの設定によって異なります。
ここで説明する手順は、デフォルト設定に基づいています。
上書きモード用の新しいファームウェアをダウンロードしてインストールする手順、2 つのファームウェアイメージの設定、およびプライマリスロットとセカンダリスロットの設定について説明しています。
ローダは暗号化されたイメージをダウンロードします。これらのイメージは、復号化され、認証されてから、対応するスロット領域に平文でプログラムされます。
BL2 NVCNT 領域には、アンチロールバック機能のファームウェアバージョン情報の管理に使用されるデータが格納されます。



このプレゼンテーションにご参加いただき、ありがとうございました。
TFM の機能を詳しく説明したプレゼンテーションを参照してください。

- TFM Flash メモリのフットプリント
- TFM ポインタ