STM32WL5 セキュリティ - RSS

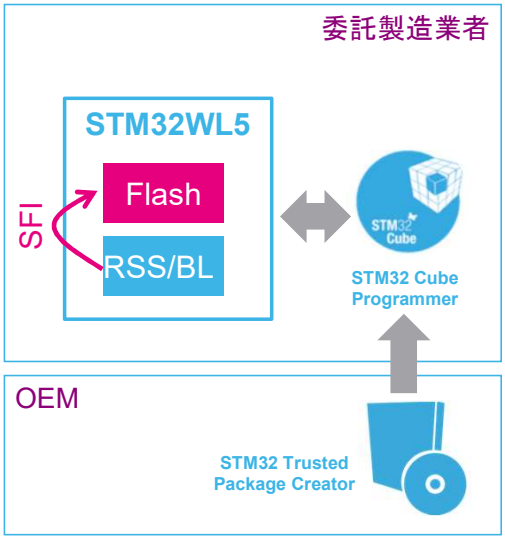
ルートセキュリティサービス

レビジョン 1.0

STM32WL5 の高度なセキュリティ機能であるルートセキュリティサービス（RSS）に特化したこのオンライン・トレーニング・モジュールへようこそ。

概要

- RSS はセキュア·ファームウェア·インストール（SFI）ソリューションのサービスをブートローダとユーザ·ファームウェアに提供



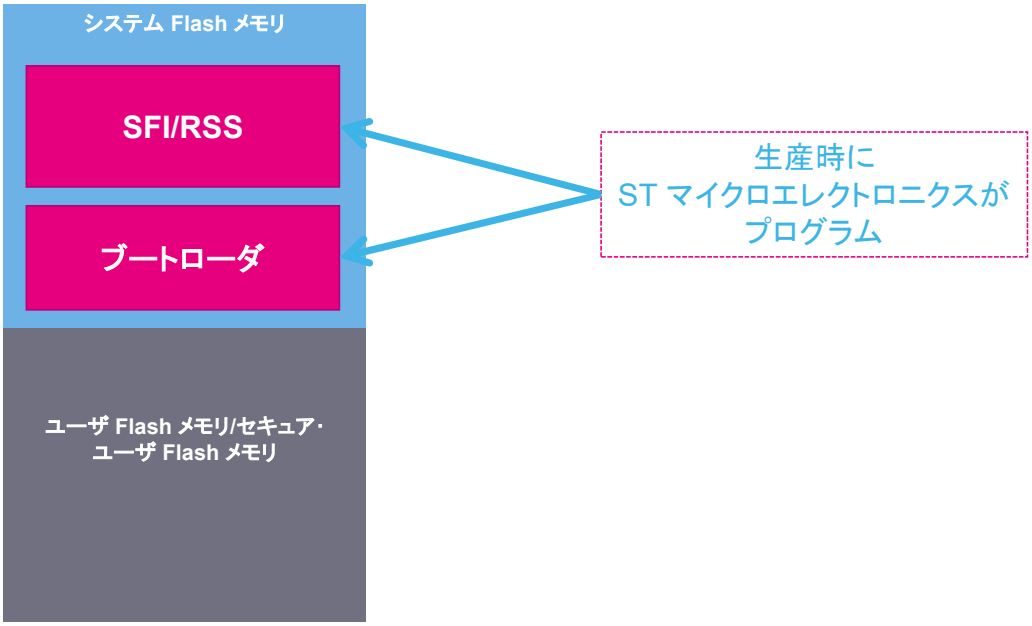
アプリケーション側の利点

- セキュアファームウェアインストール（SFI）の有効化

2

RSS を使用して、セキュアまたは非セキュアな Flash メモリの内容をロードします。
RSS は、STM32 のセキュアファームウェアインストール（SFI）ソリューションで使用する実行時ルート·セキュリティ·サービスを提供します。
保護されるメモリの詳細については、オンライン·トレーニング·モジュール「STM32WL5-Security-Memories Protection」を参照してください。

Flash メモリの構成



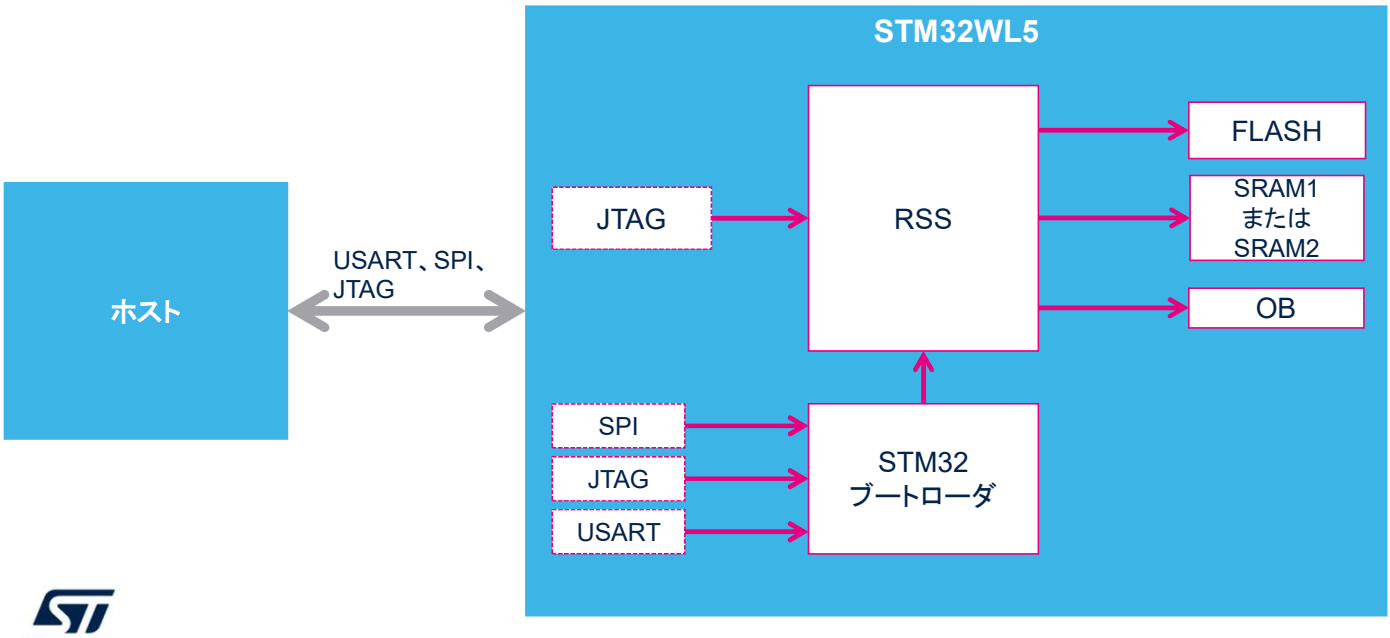
life.augmented

3

Flash メモリの情報ブロックの構成は次のとおりです。

- システム・メモリ・ブート・モードで CPU1（Cortex M4）のブート場所となるシステムメモリ。この領域は予約済みで、USART、I2C1、または SPI のいずれかのインタフェースを介した Flash メモリの再プログラミングに使用するブートローダが置かれています。ブートローダはデバイスの製造時に ST マイクロエレクトロニクスによってプログラムされており、誤った書込みや消去の操作から保護されています。詳細については、アプリケーションノート「STM32 マイクロコントローラシステム・メモリ・ブート・モード（AN2606）」を参照してください。
- システム・メモリ・ブート・モードで CPU2（Cortex M0+）のブート場所となるシステムメモリ。この領域は予約済みで、USART、I2C、または SPI のいずれかのインタフェースを介したファームウェアの認証と Flash メモリへのインストールに使用する SFI/RSS ファームウェアが置かれています。ブートローダはデバイスの製造時に ST マイクロエレクトロニクスによってプログラムされており、誤った書込みや消去の操作から保護されています。

ブートローダ



life.augmented

4

STM32WL5x マイクロコントローラでは、セキュアブートローダが内蔵 Flash メモリ（システムメモリ）に格納され、USART、SPI、および JTAG の各インタフェースをサポートしています。

STM32WL5x のセキュアブートローダは、インストールされているアプリケーションによって消去が許可されている場合、内部ユーザ Flash メモリを完全に消去した後で SFI プロセスを複数回実行できるようにします。

内蔵ブートローダは、Flash メモリをプログラムするために使用され、CPU1（Cortex M4）上で動作します。非セキュアなメモリ領域に内容をロードするために使用できます。

ルートセキュリティサービス（SFI/RSS）の一部である内蔵セキュアファームウェアインストールプロセスは、Flash を内蔵ブートローダとしてプログラミングできます。それはCPU2（Cortex M0+）上で動作し、セキュアおよび非セキュアなメモリ領域に内容をロードするために使用できます。

セキュアブートローダは、標準の ST ブートローダにセキュリティ機能を追加したものです。
セキュアブートローダは、SFI プロセス中に他のコードがユーザ Flash メモリと SRAM にアクセスすることを一切許可しません。

セキュア·ファームウェア·インストール（SFI）

- セキュア·ファームウェア·インストール（SFI）は、STM32WL5 シリーズのマイクロコントローラ向けのグローバル·ソリューションであり、信頼できない生産環境（OEM 委託製造業者など）で OEM ファームウェアの（不正コピー防止のための）インストール回数をカウントし安全·確実にインストールできるようにする
- SFI は、セキュア·ブートローダと RSSE （ルート·セキュリティ·サービス拡張）を使用して実装される
- SFI ツールの詳細については、AN5511 を参照

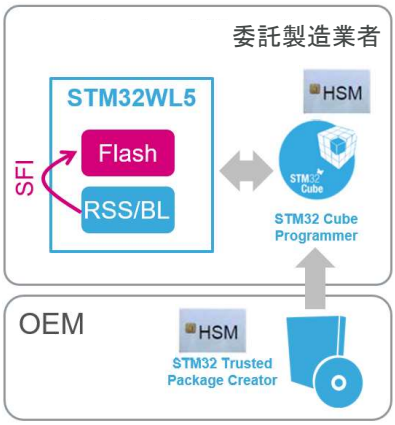
life.augmented

5

セキュアファームウェアインストール（SFI）は、STM32WL5 シリーズのマイクロコントローラ向けのグローバル·ソリューションであり、信頼できない生産環境（OEM 委託製造業者など）で OEM ファームウェアの（不正コピー防止のための）インストール回数をカウントし安全·確実にインストールできるようにします。
SFI は、セキュア RSS とセキュアブートローダを使用して実装されます。SFI で保護されている OEM ファームウェアは、デバイスの内蔵 Flash に格納できます。
STM32WL5 の SFI ソリューションでは、STM32 Trusted Package Creator ツールにより、OEM ファームウェア全体とオプションバイトが AES 秘密鍵で暗号化されています。これは、OEM ファームウェアの開発段階で実施されます。この AES 秘密鍵の機密性は、RSS によってのみ読出し可能として、STM32 デバイス固有のキーペアを使用して確保されています。

詳細については、セキュアファームウェアインストール（SFI）ソリューションのアプリケーションノート AN5511 を参照してください。

SFI のセキュリティ機能



- STマイクロエレクトロニクス純正の STM32 マイクロコントローラのみが、SFI を使用して、保護されているファームウェアをインストールでき、これは信頼できない環境や施設でも実行可能
- ファームウェアがインストールされている STM32 デバイスの数を HSM 内部でカウントできる
- OEM 内部ファームウェア（およびオプションバイト）の認証、完全性、機密性は、復号したファームウェア（およびオプションバイト）を内蔵 Flash へプログラムする前にチェック
- STM32CubeProgrammer は USART、SPI、または JTAG を通じ、STM32WL5 マイクロコントローラの SFI イメージのセキュアなプログラミングをサポート

life.augmented

6

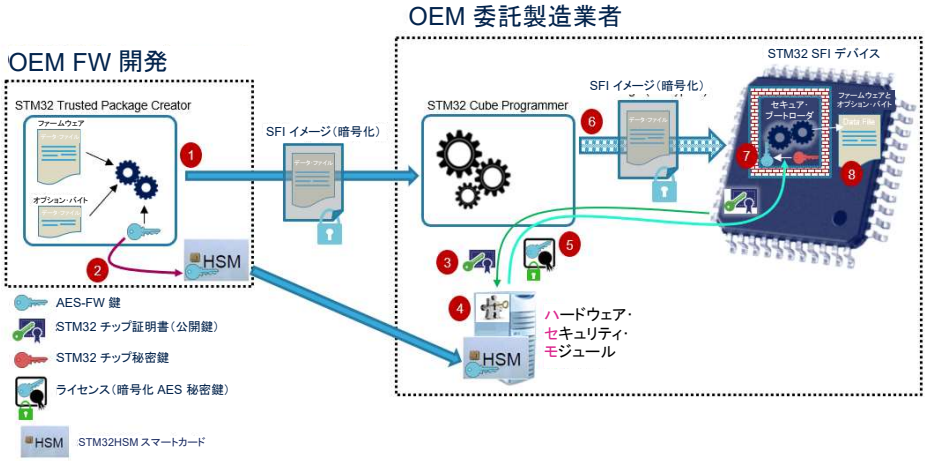
ST マイクロエレクトロニクス純正の STM32WL5 マイクロコントローラのみが、SFI を使用して、保護されているファームウェアをインストールできます。
ファームウェアがインストールされている STM32 デバイスの数は、SFI プロセスに関連付けられたハードウェア・セキュリティ・モジュール（HSM）内部でカウントできます（次のスライドを参照）。

OEM ファームウェアとオプション・バイトは、OEM ファームウェアの開発段階で STM32 Trusted Package Creatorツールによって暗号化されています。また、OEM でもこのツールを使用して、AES 秘密鍵とそのノンスおよび最大インストール・カウンタでハードウェア・セキュリティ・モジュール（HSM）をプログラムします。
OEM 委託製造業者は、STM32CubeProgrammer とプロビジョニングした HSM を使用して SFI プロセスを開始し、暗号化した SFI イメージを STM32WL5 デバイスに送信します。

OEM 内部ファームウェア（およびオプションバイト）の認証、完全性、機密性は、復号したファームウェア（およびオプションバイト）を内蔵 Flash へプログラムする前にチェックされます。

内部 Flash への SFI

- STM32 Trusted Package Creator から生成できる SFI イメージ（暗号化済み）
- OEM が AES 秘密鍵を使用して HSM をプログラミング
- HSM がライセンスを STM32 に提供
- デバイス証明書を取得
- HSM で STM32 デバイスを認証
- SFI プロセスを起動
- ライセンスで暗号化されている OEM の AES 秘密鍵を RSS が取得
- 暗号化されたファームウェアとオプション・バイトを復号してプログラミング



内部 Flash メモリへのセキュアファームウェアインストールは次の手順で実行されます（手順番号がスライドの図に示されています）。

1/ OEM が OEM FW（.sfi）を作成
2/ OEM が HSM で OEM FW 鍵をプロビジョニング
3/ Cube Programmer が証明書を取得
4/ HSM がライセンスを作成
5/ STM32 がライセンスを取得
6/ STM32 が OEM FW（.sfi）を取得
7/ STM32 が OEM FW と OB を復号
8/ STM32 が OEM FW と OB を復号

関連ペリフェラルとトレーニング

- RSS にリンクされている次のトレーニングを参照
  - STM32WL5-Security-Memories Protection
    - 外部と内部からの攻撃からコードとデータを保護
  - STM32WL5 システムの CM0+ セキュリティ･モジュール

life.augmented

これらのトピックの詳細については、メモリ保護、Flash、または
ブートのトレーニングを参照してください。
RSS と SFI に関連するペリフェラルのリストも参照してください。

参考文書

- 詳細については次を参照
  - RM0453：STM32WL5 リファレンスマニュアル
  - AN2606：STM32 マイクロコントローラ･システムメモリ･ブート･モード
  - AN4992：セキュアファームウェアインストール（SFI）の概要
  - AN5511：STM32WL5x SFI tools, bootloader and RSS interface
  - UM2237：STM32CubeProgrammer software description
  - UM2238：STM32 Trusted Package Creator software description

life.augmented

詳細については、次を参照してください。

- STM32 マイクロコントローラ システムメモリ･ブート･モードに関するアプリケーションノート AN2606
- アプリケーションノート AN4992 は、セキュアファームウェアインストール（SFI）の概要。アプリケーションノート AN5511 は STM32WL5x の SFI ツール、ブートローダ、および RSS インタフェースについて記載しています。
- ST の Web サイトから STM32CubeProgrammer と STM32 Trusted Package Creator のユーザマニュアルも入手できます。