STM32WB – CM0+ セキュリティ

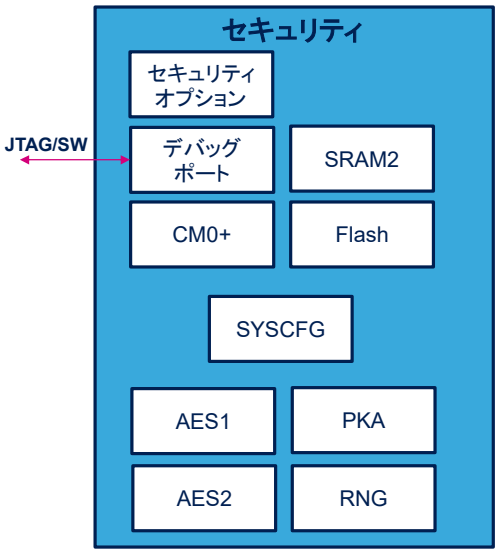
Cortex®-M0+ セキュリティ

1.0 版

life.augmented

STM32WB Cortex-M0+ のセキュリティ機能のプレゼンテーションにようこそ。

概要



- Cortex-M0+ セキュリティの管理対象:
  - 排他的 Cortex-M0+ アクセス
  - Cortex-M0+ ファームウェアのセキュリティ:
    - Flash メモリと SRAM2
    - デバッグアクセス
  - ペリフェラルのセキュリティ:
    - AES、PKA、TRNG
- セキュアユーザオプションと SYSCFG セキュアレジスタビットを経由した制御

アプリケーション側の利点

- セキュア CM0+ 側のアプリケーションキーのストレージ
- セキュアな暗号化
- 真正でセキュアな ST 無線ファームウェア更新

Cortex M0+ セキュリティは、ファームウェアとペリフェラルのセキュリティを管理し、ST 無線ファームウェアの認証に用いられ、暗号鍵のセキュアな処理を可能とします。
Cortex M0+ セキュリティは、セキュアオプションを使用して Flash メモリ、SRAM2、デバッグセキュリティの制御を行います。AES 暗号化エンジン、秘密鍵アクセラレータと真性乱数発生器が、システム設定ブロックのセキュアレジスタビットを通じて、セキュア Cortex-M0+ コアによってセキュリティが動的に管理されるペリフェラルです。

Cortex M0+ セキュリティキーの機能

3

ファームウェア認証とセキュアなキー処理

- セキュア Flash メモリと SRAM2領域
  - Cortex-M0+ により排他的にアクセス可能
- セキュアペリフェラル
  - Cortex-M0+ による AES2、PKA、TRNG への完全な排他的アクセス
  - Cortex-M0+ による AES1 キーのみへの排他的アクセス
- デバッグセキュリティ
  - セキュアメモリ領域とペリフェラルはデバッグポート経由でのアクセス不可

life.augmented

Cortex-M0+ セキュリティは、Flash メモリ、ならびに SRAM2a と SRAM2b の中のセキュア領域への排他的アクセスを与えることに基づいています。
その上、AES1、AES2、秘密鍵アクセラレータ、真性乱数発生器などのペリフェラルをセキュアにすることが可能であり、セキュアな暗号化とキー生成が可能となります。
セキュアメモリ領域とペリフェラルは、Cortex-M4 からもデバッガ経由でもアクセス可能ではありません。

Cortex M0+ セキュリティ

- Flash メモリと SRAM2 領域と CM0+ デバッグセキュリティ
  - STM32WB 生産時の RSS プログラミング後に ST により有効化
  - パラメータは RSS 経由で更新されるセキュアファームウェアにより修正
- セキュアペリフェラル
  - CM0+ 上で動作するコネクティビティファームウェアにより有効化
    - AES2、PKA、TRNG のセキュリティは CM0+ による自動処理
    - AES1 キーのセキュリティは CM4 アプリケーションリクエストに応じて CM0+ による処理

life.augmented

Cortex M0+ セキュリティは、Cortex M0+ 自体によってすべて処理されます。STM32WB の生産時、ルートセキュリティサービス（RSS）ファームウェアがユーザ Flash メモリにプログラムされた後に、Cortex M0+ セキュリティが有効化されます。その後のあらゆる Cortex M0+ ファームウェア更新（コネクティビティスタックまたは RSS）は RSS によって処理され、必要に応じて Cortex M0+ セキュリティパラメータが修正されます。
AES2、PKA、RNG のセキュリティは、Cortex M0+ ファームウェアによって必要とされる場合には必ず Cortex M0+ によってすべて処理されます。AES1キーのセキュリティについても、Cortex M4 アプリケーションファームウェアからリクエストを受けたときに、Cortex M0+ によって管理されます。

セキュアオプションレジスタ

- Cortex-M0+ セキュリティは、セキュアユーザオプションによって設定可能。

レジスタ	フィールド									
OPTR (*)	ユーザオプション								ESE	RDP
SFR (*)	Res.						DDS	Res.	FSD	SFSA
SRRVR (*)	C2OPT	NBRSD	SNBRSA	Res.	BRSD	SBRSA	SBRV			

*OPTR：オプションレジスタ
*SFR：セキュア Flash レジスタ
*SRRVR：セキュア RAM & リセットベクタレジスタ

- Cortex-M0+ セキュリティが有効になると、セキュアユーザオプションが Cortex-M0+ から排他的に書込み可能。
  - 非セキュアな Cortex-M4 は、セキュア領域のサイズを求めるなどのために、セキュアユーザオプションを読み出し可能。

life.augmented

Cortex-M0+ セキュリティは、デバイスの起動時にセキュア Flash レジスタとセキュア RAM & リセットベクタレジスタにロードされるセキュアユーザオプションを通じて制御されます。
セキュアユーザオプションは、セキュアな Cortex-M0+ によってのみ修正可能であり、セキュア Cortex-M0+ ソフトウェアの更新時にパラメータが変更されます。
非セキュアな Cortex-M4 は、セキュア領域の開始アドレスを決めるために、セキュアユーザオプションへの読出しアクセスが可能となっています。

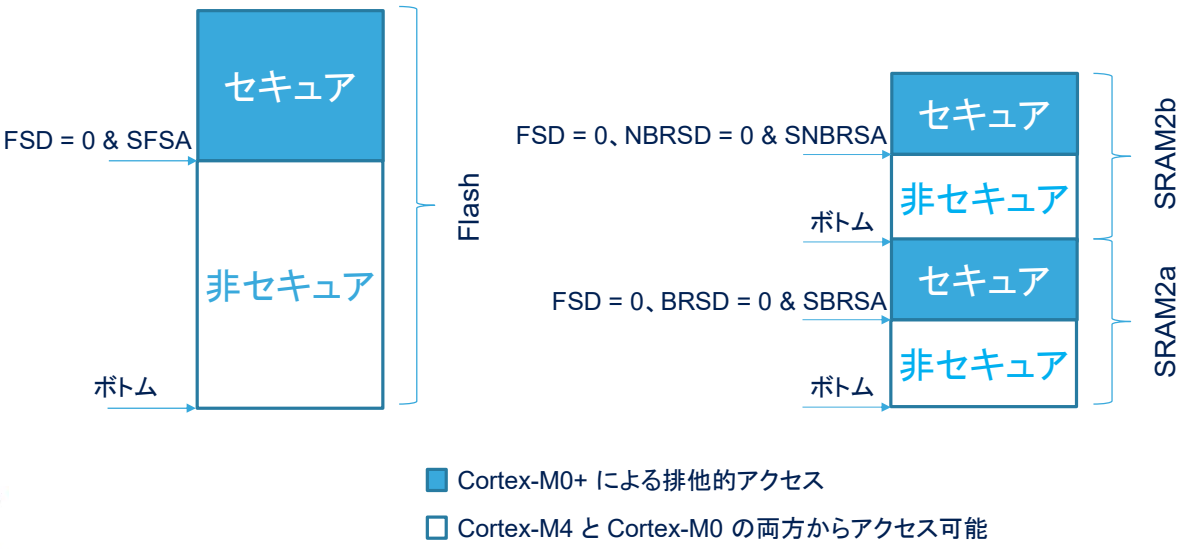
セキュアユーザオプション

- メモリセキュリティはセキュアユーザオプションにより処理
- Flash メモリのセキュリティ
  - セキュリティイネーブル（**FSD**）➔ Cortex-M0+ セキュリティがグローバルに有効化
  - セキュア Flash 開始アドレス（**SFSA**）
    - Flash メモリは、この開始アドレスから Flash メモリの先頭までセキュア。
- RAM のセキュリティ
  - RAM セキュリティイネーブル（**BRSD**：バックアップ RAM2a）（**NBRSD**：非バックアップ RAM2b）
  - セキュア RAM 開始アドレス（**SBRSA**：バックアップ RAM2a）（**SNBRSA**：非バックアップ RAM2b）
    - RAM は、その開始アドレスから RAM の先頭までセキュア。
- イネーブルセキュリティ環境（**ESE**）
  - セキュリティが常に有効化されているため、このビットは読出し専用ビット。

life.augmented

メモリセキュリティは、セキュアユーザオプションによって有効化と設定が行われます。
Flash セキュリティディセーブルビットによって、グローバルな Cortex-M0+ セキュリティが有効化されます。
セキュア Flash 開始アドレスによって、Flash メモリがセキュアとなる開始アドレスが定義されます。
バックアップ RAM セキュリティディセーブルビットによってバックアップ RAM のセキュリティが制御され、セキュアバックアップ RAM 開始アドレスによって、バックアップ RAM がセキュアとなる開始アドレスが定義されます。
非バックアップ RAM セキュリティディセーブルビットは、非バックアップ RAM のセキュリティを有効化するために用いられ、セキュア非バックアップ RAM 開始アドレスによって、非バックアップ RAM がセキュアとなる開始アドレスが定義されます。
セキュア領域へのデバッグアクセスは、デバッグディセーブルセキュリティビットによって制御されます。
Cortex-M0+ コア上でセキュリティが常に有効化されているため、イネーブルセキュリティ環境ビットは読出し専用ビットです。

メモリのセキュリティ



メモリの先頭は、Cortex-M0+ による排他的アクセスのためにセキュリティ保護可能です。
セキュア Flash 開始アドレスから始まる Flash メモリの先頭は、Flash セキュリティディセーブルビット（FSD）が“0”にセットされている場合にセキュアとなります。
セキュアバックアップ RAM 開始アドレス（SBRSA）から始まるバックアップ SRAM2a の先頭は、Flash セキュリティディセーブルビットとバックアップ RAM セキュリティディセーブル（BBRSD）ビットの両方が“0”にセットされている場合にセキュアとなります。
セキュア非バックアップ RAM 開始アドレス（SNBRSA）から始まる非バックアップ SRAM2b の先頭は、Flash セキュリティディセーブルビットと非バックアップ RAM セキュリティディセーブルビット（NBRSD）の両方が“0”にセットされている場合にセキュアとなります。
どの RAM もセキュアにせずに Flash メモリだけをセキュアにすることも可能ですが、Cortex-M0+ ソフトウェアによって使用されている Flash メモリと RAM を両方ともセキュアにすることをお勧めします。

Cortex-M0+ ブートリセットベクタ

- Cortex-M0+ ブートリセットベクタは、セキュアブートリセットベクタ（**SBRV**）オプションでプログラム可能。
  - ワード境界整列値
- Cortex-M0+ は、セキュア CPU2 オプション（**C2OPT**）によって選択された Flash メモリまたは SRAM2（a または b）からブート可能。
- 生産時に、Cortex-M0+ ブートリセットベクタは、Flash メモリの中の RSS ブートリセットベクタにセット。

life.augmented

Cortex-M0+ ブートリセットベクタは、セキュアブートリセットベクタオプションとセキュア CPU2 オプションでプログラムされます。 生産時に、Cortex-M0+ ブートリセットベクタは Flash メモリのルートセキュアサービス開始アドレスを示します。セキュアモードでは、Cortex-M0+ ブートリセットベクタはセキュア Cortex-M0+ 側でのみ変更可能です。

デバッグの無効化

デバッグアクセスはセキュアユーザオプションにより制御

- デバッグアクセス制御はセキュリティとは独立。
- セキュアデバッグディセーブルオプション（**DDS**）によって制御。
  - Cortex-M0+ に対するデバッグポートアクセスを無効化
- デバッグは、セキュアモードと非セキュアモードにおいて有効化と無効化が可能。
  - セキュアモードでは、デバッグアクセスはセキュア Cortex-M0+ 側でのみ変更可能。

life.augmented

Cortex-M0+ デバッグアクセスは、デバッグディセーブルオプションビットによって制御されます。セキュリティとは独立していて、セキュアモードと非セキュアモードのどちらでも有効化と無効化が可能です。セキュアモードでは、デバッグアクセス制御はセキュア Cortex-M0+ 側でのみ変更可能です。

セキュリティ&メモリ消去

- Flash ページ消去
  - セキュアページは、セキュア Cortex-M0+ のみが消去可能。
- Flash 全体消去
  - Flash メモリは、Cortex-M0+ からリクエストされたときに全体消去のみ可能。
  - 非セキュアな Cortex-M4 からリクエストされた Flash 全体消去操作は拒否。
- RDP 解除による Flash 消去
  - 非セキュア Flash メモリ領域のみ、複数ページの消去が可能。
- RDP 解除による Flash 全体消去
  - Flash 全体消去と SRAM2 消去が実行されて、RSS を含むセキュリティが解除。
  - ST 無線スタック認証は失われ、再プログラム不可。

life.augmented

STM32WB には、Coretex-M4 と Cortex-M0+ 両方のソフトウェア用として Flash メモリが 1 つだけ搭載されています。Cortex-M0+ セキュリティによって、非セキュアな Cortex-M4 によってセキュア Flash メモリページが消去されることが防止されます。Cortex-M4 Flash 全体消去操作は拒否され、Cortex-M4 ソフトウェアの消去には複数ブロック消去を用いる必要があります。
読出し保護をレベル 1 からレベル 0 に解除すると、Flash メモリの非セキュア部分のみが消去されます。セキュア Cortex-M0+ ソフトウェアは保持されます。
読出し保護をレベル 1 からレベル 0 に解除したときにのみ、Flash メモリがすべて全体消去され、セキュリティが解除されます。この場合、ST 無線スタック認証とセキュリティは失われ、プログラムできなくなります。

セキュアシステム設定ビット

- セキュアシステム設定ビットは、ペリフェラルのセキュリティ処理のために使用。
  - ペリフェラルセキュリティは、(FSD)でセキュリティが有効化された場合にのみ使用可能。
    - SAES1 によって有効化される AES1 キーセキュリティ
      - Cortex-M0 ソフトウェアによってセキュアアプリケーションキーストレージ機能が提供。
    - SAES2 によって有効化される AES2 フルセキュリティ
    - SPKA によって有効化される PKA フルセキュリティ
    - SRNG によって有効化される True RNG フルセキュリティ
  - ペリフェラルのセキュリティ
    - 動的管理が可能
    - セキュア Cortex-M0+ によって有効化と無効化が可能
    - Cortex-M4 によってセキュリティイネーブルビットの読出しが可能

life.augmented

AES アクセラレータ 1、AES アクセラレータ 2、公開鍵アクセラレータ、真性乱数発生器の各ペリフェラルは、システム設定ブロックのセキュアレジスタビットを通じて、Cortex-M0+ ファームウェアによって動的にセキュアにすることができます。AES 2 と公開鍵アクセラレータと真性乱数発生器の各ペリフェラルは、ペリフェラルのセキュリティをフル提供します。AES 1 はキーセキュリティのみを提供し、Cortex-M4 で動作するアプリケーションはセキュアキーを用いた暗号化を使用できます。セキュアキーストレージは、Cortex-M0+ ファームウェアによって提供されます。
Cortex-M4 は、ペリフェラルセキュリティビットを読み出して、そのセキュリティステータスを判定できます。

セキュアな暗号化

- 無線スタック暗号鍵が生成され、セキュア Cortex-M0+ 側に格納。
- Cortex-M0+ 無線スタックによって暗号鍵管理機能（CKS：Cryptographic Key Storage (暗号鍵ストレージ)）が提供。
  - アプリケーションが暗号鍵の生成と格納を行うことが可能。
  - アプリケーションがセキュア AES1 に格納された暗号鍵のロード可能。

life.augmented

Cortex-M0+ 上で動作する無線スタックによって、アプリケーションに暗号鍵管理が提供されます。
暗号鍵が生成され、暗号鍵ストレージ（CKS）を用いてセキュア Cortex-M0+ 側に格納されます。

セキュアファームウェア更新

- セキュアファームウェアは、Cortex-M0+ 上で動作するセキュア RSS 経由でのみ更新可能。
  - RSSは、STM32WBxx 工場レベルで事前にプログラム可能。
- セキュアファームウェアダウンロードは、次のものを通じて有効化。
  - システムブートローダ経由のインサーキットプログラミング（ICP）
  - 無線通信でのアップデート(OTA) を含むアプリケーション内プログラミング（IAP）
- セキュア Cortex-M0+ は、すべての RDP レベルでユーザオプションの更新が可能。
- セキュアファームウェア
  - 通信スタック
  - RSS

life.augmented

STM32WB には事前にプログラムされた RSS が含まれており、セキュア Cortex-M0+ ソフトウェアの更新が可能です。
無線スタックソフトウェアと RSS 自体の両方が更新可能です。
システムブートローダによるインサーキットプログラミング（ICP）経由で、あるいは 無線通信でのアップデート(OTA)を含むアプリケーションブートローダによるアプリケーション内プログラミング（IAP）で、セキュアソフトウェアのダウンロードが可能です。
セキュア Cortex-M0+ ソフトウェア更新は、すべての読出し保護レベル（0、1、2）で可能です。

イベント

Cortex-M4 の動作	生成されるイベント
セキュア RAM メモリ領域への Cortex-M4 書込みアクセス*	バスエラー
セキュアペリフェラルレジスタへの Cortex-M4 書込みアクセス	バスエラー
セキュア Flash の全体消去をリクエストする Cortex-M4	バスエラー
セキュア Flash のページ消去をリクエストする Cortex-M4	バスエラー
セキュア Flash ページをリクエストする Cortex-M4	バスエラー
セキュア Flash への Cortex-M4 書込み操作	バスエラー
セキュア Flash メモリ領域への Cortex-M4 読出しアクセス	バスエラー + ゼロ値読出し
セキュア RAM メモリ領域への Cortex-M4 読出しアクセス	ゼロ値読出し
セキュアペリフェラルレジスタへの Cortex-M4 読出しアクセス	ゼロ値読出し

* RDPレベルが 1 で SRAM1 から起動する場合には、バスエラーは生成されません。(SRAM2 はロックされる)

life.augmented

このスライドには、Cortex-M0+ のセキュリティ機能によって生成されるイベントがリストアップされています。イベントは、非セキュア Cortex-M4 に対してのみ生成されます。Cortex-M4 のアクセスタイプによっては、非セキュア Cortex-M4 に対してバスエラーが生成されます。セキュア領域を読み出すとゼロが返されます。非セキュア Cortex-M4 によって読出し可能なのは、セキュアユーザオプションとシステム設定ペリフェラルセキュリティイネーブルビットのみとなります。

関連ペリフェラル

- この機能に関連した以下のトレーニングを参照してください。
  - STM32WB 電源制御（Flash メモリインタフェース)
    - セキュアユーザオプション
  - STM32WB システム設定（SYSCFG）
    - セキュアペリフェラルイネーブルビット
  - BLE スタック
    - セキュア Cortex-M0+ BLEスタック

life.augmented

このトレーニングに加えて、Flash メモリインタフェースとシステム設定モジュールが役に立つことがわかるでしょう。