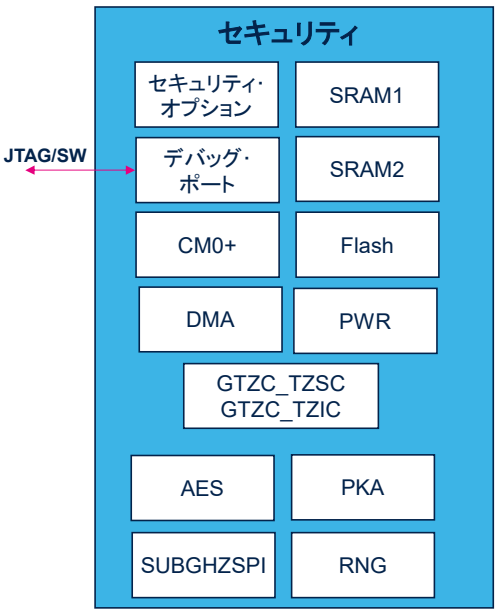
STM32WL5 – CM0+ セキュリティ

Cortex-M0+ セキュリティ

レビジョン 1.0

STM32WL5 Cortex-M0+ セキュリティのプレゼンテーションへようこそ

概要



- Cortex-M0+ セキュリティによる管理対象
  - Cortex-M0+ による排他アクセス
  - 次に対する Cortex-M0+ ファームウェアのセキュリティ:
    - Flash メモリ、SRAM1、SRAM2、デバッグ・アクセス
  - 次に対するペリフェラルのセキュリティ:
    - DMA、PWR、AES、PKA、TRNG、SUBGHZSPI
- Flash のセキュア・ユーザ・オプションと GTZC による制御
- 不正アクセス割込みによるセキュリティ違反の監視

アプリケーション側の利点

- セキュアな CM0+ 側でのアプリケーション・キーの保管
- セキュアな暗号化とセキュアな無線通信
- 正規でセキュアなファームウェアのインストールと更新

life.augmented

2

Cortex-M0+ セキュリティでは、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て、暗号技術を用いた Sub-GHz 無線通信のセキュアな取り扱いを可能にします。ファームウェアのセキュアなインストールとセキュアな更新の機能も提供します。
Cortex-M0+ セキュリティでは Flash メモリ、SRAM1、SRAM2、デバッグ、Sub-GHz シリアル・ペリフェラル・インタフェースのセキュリティを制御するセキュアなオプションが使用されています。
グローバル TrustZone コントローラのセキュア・レジスタ・ビットに基づき、高度暗号化標準（AES）、公開鍵アクセラレータ（PKA）、ハードウェア乱数発生器（TRNG）のセキュリティが、セキュアな Cortex-M0+ コアによって実行時に動的に管理されます。
グローバル TrustZone コントローラによる監視によって不正アクセス・イベントが発生すると、セキュアな Cortex-M0+ にセキュリティ違反が報告されます。

Cortex M0+ セキュリティの主要機能

ファームウェアの認証とセキュアな鍵処理

- Flash メモリ、SRAM1、SRAM2のセキュアな領域
  - Cortex-M0+ で排他アクセス可能
- セキュアなペリフェラル
  - Cortex-M0+ から SUBGHZSPI、AES、PKA、TRNG への排他アクセス
  - Cortex-M0+ からセキュアな DMA チャネルへの排他アクセス
- デバッグのセキュリティ
  - デバッグ･ポートを通じたセキュアなメモリ領域とペリフェラルへのアクセスは不可能
- 特権に基づくリソース保護
  - メモリとペリフェラルを特権で保護可能

life.augmented

3

Cortex-M0+ セキュリティは、Flash メモリ、SRAM1、SRAM2 のセキュアな領域への排他アクセスの付与に基づいています。
また、Sub-GHz シリアル･ペリフェラル･インタフェース、AES、公開鍵アクセラレータ、ハードウェア乱数発生器などのペリフェラルをセキュリティで保護できるので、セキュアな無線通信、暗号処理、鍵生成が実現します。
ダイレクト･メモリ･アクセス･チャネルを、チャネル単位でセキュリティ保護できるので、セキュアなデータ転送とチャネル制御が実現します。
セキュアなメモリ領域とペリフェラルには Cortex-M4 からアクセスできず、セキュアなデバッグを無効にしている場合はデバッガからもアクセスできません。
メモリとペリフェラルはセキュリティで保護できるほか、特権でも保護できます。

Cortex-M0+ セキュリティ

- Flash メモリ領域、SRAM 領域、CM0+ デバッグのセキュリティ
  - Flash のユーザ･オプションで有効化
  - パラメータの変更はセキュアな Cortex-M0+ ファームウェアでのみ可能
- セキュアなペリフェラル
  - Flash のユーザ･オプションで有効化
    - SUBGHZSPI では、リセット後も Sub-GHz 無線通信のセキュリティを維持
  - Cortex-M0+ 上で動作しているセキュアなファームウェアによって実行時に有効化
    - 必要に応じて、非セキュアな Cortex-M4 と AES、PKA、TRNG のセキュリティを共有可能
    - 必要に応じて、非セキュアな Cortex-M4 と DMA チャネルを共有可能
- セキュアな特権による保護
  - 特権のないセキュアなアクセスから、特権で保護したセキュアな Cortex-M0+ リソースを保護可能

life.augmented

4

Cortex-M0+ ファームウェアをインストールするときに、ユーザが Cortex-M0+ セキュリティを有効化します。そのインストール後に、Cortex-M0+ 自身によってセキュリティが全面的に処理されるようになります。製造時点の STM32WL5 では Cortex-M0+ セキュリティが無効になっているので、セキュア・ファームウェア・インストールによって Cortex-M0+ ファームウェアをセキュリティで保護してインストールできます。以降の Cortex-M0+ ファームウェアの更新は、Cortex-M0+ にインストールされた、セキュア･ブート、セキュア・ファームウェア・アップデートによって処理されます。
また、Cortex-M0+ ファームウェアをインストールするときに、Sub-GHz 無線のセキュリティも定義する必要があります。
AES、PKA、RNG の各ペリフェラルのセキュリティは、Cortex-M0+ アプリケーションで必要になると、全面的に Cortex-M0+ によって実行時に処理されます。ダイレクト･メモリ･アクセス･チャネルも、必要になったときに Cortex-M0+ によって実行時にセキュリティで保護できます。
さらに、Cortex-M0+ には特権による保護も用意されていて、Cortex-M0+ ファームウェアによって実行時に有効化できます。 これにより、特権がないセキュアなアクセスから、特権によるセキュアな Cortex-M0+ リソースを保護できます。

特権による Cortex-M4 の保護

- 特権による非セキュアな保護
  - 特権がないアクセスから、非セキュアな Cortex-M4 リソースを特権で保護可能

life.augmented

Cortex-M4 のファームウェアによって、特権による Cortex-M4 の保護を実行時に有効化できます。 これにより、特権がないアクセスから、非セキュアな Cortex-M4 リソースを特権で保護できます。

セキュア·オプション·レジスタ

- セキュア·ユーザ·オプションで Cortex-M0+ セキュリティを設定

レジスタ	フィールド									
OPTR(*)	C2BOOT_LOCK	ユーザ·オプション							ESE	RDP
SFR(*)	SUBGHZSPISD	Res.	HDPAD		HDPSA	Res.	DDS	Res.	FSD	SFSA
SRRVR(*)	C2OPT	NBRSD	SNBRSA	Res.	BRSD	SBRSA	SBRV			

* OPTR：オプション·レジスタ（Options Register）
* SFR：セキュア Flash レジスタ（Secure Flash Register）
* SRRVR：セキュア RAM/リセット·ベクタ·レジスタ（Secure Ram and Reset Vector Register）

- Cortex-M0+ セキュリティが有効であれば、セキュア·ユーザ·オプションに Cortex-M0+ から排他書込みが可能
  - 非セキュアな Cortex-M4 からは、セキュア·ユーザ·オプションを読み出してセキュリティ設定を確認可能

life.augmented

デバイスの起動時にセキュアな Flash レジスタにロードされるセキュア·ユーザ·オプションによって Cortex-M0+ セキュリティが制御されます。
セキュア·ユーザ·オプションはセキュアな Cortex-M0+ でのみ変更できます。これは、セキュアな Cortex-M0+ ソフトウェアの更新に伴う各種パラメータの変更です。
非セキュアな Cortex-M4 では、セキュア·ユーザ·オプションに読出しアクセスしてセキュリティ設定を確認できます。

セキュア･ユーザ･オプション 1/2

- セキュア･ユーザ･オプションで扱うメモリのセキュリティ
- Flash メモリのセキュリティ
  - セキュリティの有効化（FSD）➔Cortex-M0+ セキュリティのグローバル有効化
  - セキュアな Flash の開始アドレス（SFSA）
    - このウォーターマークの開始アドレスから Flash メモリの先頭まで Flash メモリはセキュアな状態
- RAM のセキュリティ
  - RAM のセキュリティの有効化（BRSD：バックアップ SRAM2）（NBRSD：非バックアップ SRAM1）
  - セキュアな RAM の開始アドレス（SBRSA：バックアップ SRAM2）（SNBRSA：非バックアップ SRAM1）
    - このウォーターマークの開始アドレスから RAM の先頭まで RAM はセキュアな状態
- セキュリティ環境の有効化（ESE）
  - このビットを読み出すことで、セキュリティが有効であることを判断可能
  - このビットを書き込むと、RDP を解除するときにセキュリティも解除可能

life.augmented

7

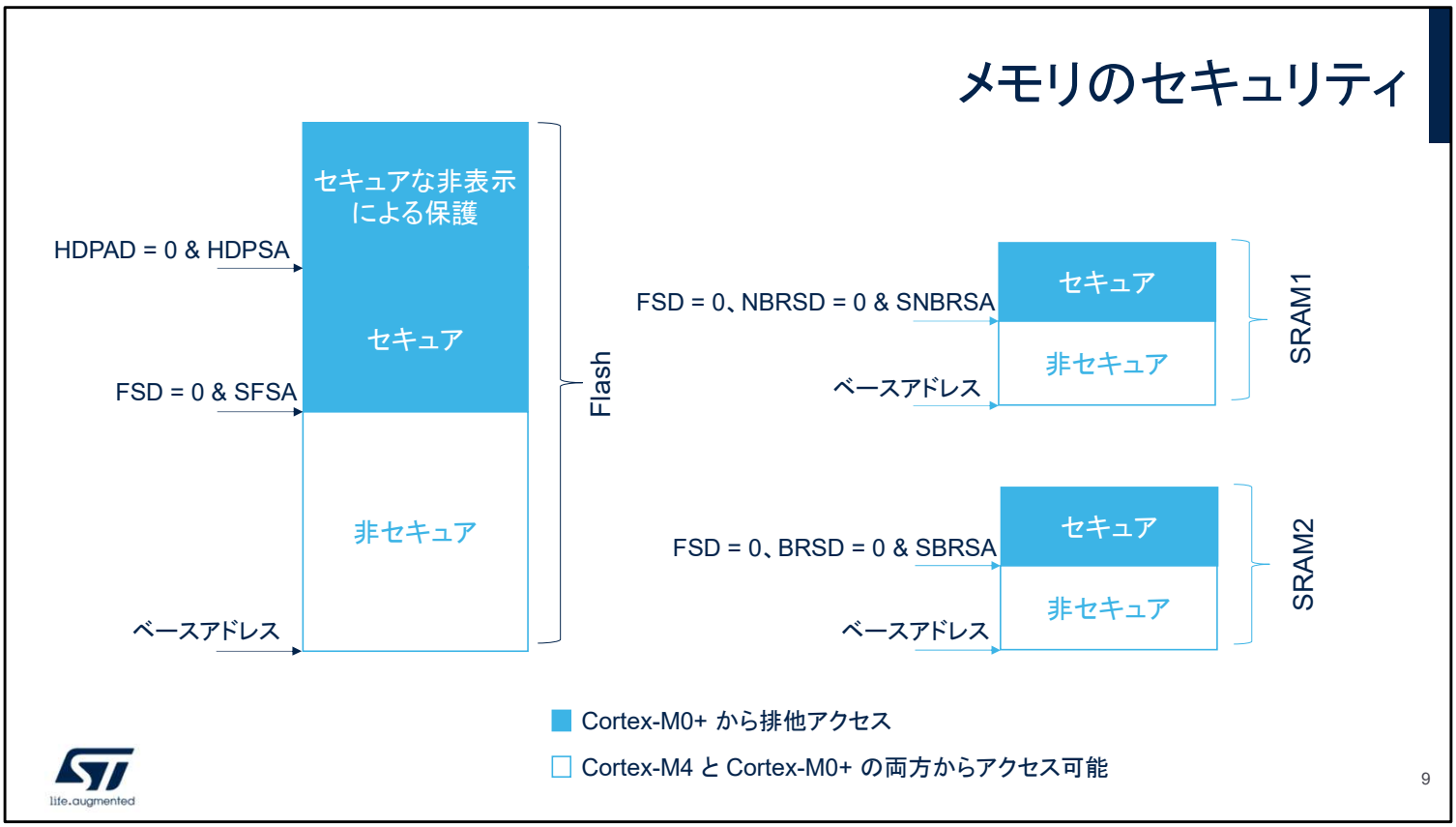
メモリのセキュリティは、セキュア･ユーザ･オプションで有効化して設定します。
Flash セキュリティのディスエーブル･ビット（FSD）で、グローバルな Cortex-M0+ セキュリティが有効になります。
セキュア Flash 開始アドレス（SFSA）で、Flash メモリのセキュアな領域（ウォーターマーク）が始まるアドレスを定義します。
バックアップ RAM セキュリティのディスエーブル･ビット（BRSD）ではバックアップ SRAM2 のセキュリティを制御します。セキュアバックアップ RAM 開始アドレス（SBRSA）では、バックアップ SRAM2 のセキュアな領域（ウォーターマーク）が始まるアドレスを定義します。
非バックアップ RAM セキュリティのディスエーブル･ビット（NBRSD）を使用して、SRAM1 のセキュリティを有効にします。
セキュア非バックアップ RAM 開始アドレス（SNBRSA）では、SRAM1 のセキュアな領域（ウォーターマーク）が始まるアドレスを定義します。
セキュリティ環境の有効化ビット（ESE）を読み出すと、デバイスがセキュアかどうかの情報が得られます。このビットに書き込むと、RDP の解除と同時にセキュリティを解除できます。

セキュア･ユーザ･オプション 2/2

- Flash メモリの秘匿保護
  - 秘匿保護の無効化（HDPAD）
  - 秘匿保護の開始アドレス（HDPSA）
    - この開始アドレスから Flash メモリの終端まで Flash メモリは秘匿保護状態
    - この秘匿保護領域は、あらゆるセキュア･ブートとセキュア･ファームウェア･アップデート機能で使用
- デバッグ･セキュリティの無効化（DDS）
  - このビットで Cortex-M0+ へのデバッグ･アクセスを無効化
- CPU2 のブート･ロック（C2BOOT_LOCK）
  - このビットで Cortex-M0+ のブート･モードをロック

life.augmented

Flash メモリの秘匿保護無効化ビット（HDPAD）では、Cortex-M0+ のセキュアな Flash 領域で秘匿保護領域を有効化します。秘匿保護開始アドレスで、Flash メモリの秘匿保護領域が始まるアドレスを定義します。この領域には、セキュア･ブートとセキュア･ファームウェア･アップデートが置かれます。この秘匿保護は、Cortex-M0+ をリセットすると実行され、次回のリセットまで保持されます。
デバッグ･セキュリティの無効化ビット（DDS）では、セキュアな Cortex-M0+ とセキュアなすべてのリソースへのデバッグ･アクセスを制御します。
CPU のブート･ロック･ビットを使用して、Cortex-M0+ のブートに対する信頼の基点を作成できます。セキュア･ブートやセキュア･ファームウェア･アップデートで効果的です。



メモリの後部は、Cortex-M0+ による排他アクセス向けにセキュリティで保護できます。
セキュア Flash メモリ開始アドレスで始まる Flash メモリの後部は、Flash セキュリティディスエーブル･ビットを「0」に設定している場合にセキュリティで保護されています。
セキュアバックアップ RAM 開始アドレスで始まるバックアップ SRAM2 の後部は、Flash セキュリティディスエーブル･ビットとバックアップ RAM セキュリティディスエーブル･ビットの両方を「0」に設定している場合にセキュリティで保護されています。
セキュア非バックアップ RAM 開始アドレスで始まる SRAM1 の後部は、Flash セキュリティのディスエーブル･ビットと非バックアップ RAM セキュリティのディスエーブル･ビットの両方を「0」に設定している場合にセキュリティで保護されています。
どの RAM もセキュリティで保護せず、Flash メモリのみをセキュリティで保護することもできます。しかし、Cortex-M0+ ソフトウェアで使用する Flash メモリと RAM の両方をセキュリティで保護することをお勧めします。
秘匿保護ディスエーブルと秘匿保護開始アドレスにより、Flash 領域に秘匿保護領域を定義できます。

セキュリティとメモリ消去

- Flash ページの消去
  - セキュアなページはセキュアな Cortex-M0+ でのみ消去可能
- Flash 全体の消去
  - Flash メモリ全体の消去は、Cortex-M0+ によるリクエストでのみ可能
  - 非セキュアな Cortex-M4 による Flash 全体の消去リクエストは拒否される
- RDP 解除に起因する Flash の消去
  - 複数ページの消去は、非セキュアな Flash メモリ領域でのみ可能
- ESE と RDP 解除に起因する Flash 全体の消去
  - Flash 全体の消去と SRAM2 の消去により、セキュアな Flash と非セキュアな Flash を消去可能

life.augmented

STM32WL5 マイクロコントローラでは、Cortex-M4 ソフトウェアと Cortex-M0+ ソフトウェアの両方で 1 つの Flash メモリを使用します。非セキュアな Cortex-M4 コアによるセキュアな Flash メモリ・ページの消去は、Cortex-M0+ セキュリティによって禁止されています。Cortex-M4 の Flash 全体の消去操作は拒否されるので、Cortex-M4 ソフトウェアを消去するには複数ブロック消去を使用する必要があります。
読出し保護（RDP）をレベル 1 からレベル 0 に解除すると、Flash メモリのうち、非セキュアな部分のみが消去されます。セキュアな 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 に解除すると同時に ESE=0 にした場合のみ、Flash メモリ全体が消去され、セキュリティが解除されます。この場合は、セキュアであるかどうかに関係なく、すべてのソフトウェアが消去されます。

Cortex-M0+ のブート･リセット･ベクタ

- Cortex-M0+ のブート･リセット･ベクタは、セキュアなブート･リセット･ベクタ（SBRV）オプションでプログラム
  - ワード境界で整列した値
- セキュアな CPU2 オプション（C2OPT）による選択に従い、Flash メモリまたは SRAM から Cortex-M0+ をブート可能
- 生産時の Cortex-M0+ ではブート･リセット･ベクタを Flash メモリの中間に設定

life.augmented

Cortex-M0+ のブート･リセット･ベクタは、セキュア･ブート･リセット･ベクタのオプションとセキュアな CPU2 のオプションでプログラムします。 生産時の Cortex-M0+ では、ブート･リセット･ベクタが Flash メモリの中間に設定されます。セキュア･モードでは、セキュアな Cortex-M0+ 側でのみ Cortex-M0+ のブート･リセット･ベクタを変更できます。

デバッグの無効化

- セキュア・オプションで扱うデバッグ・アクセス

- セキュア・ユーザ・オプションで扱うデバッグ・アクセス
- デバッグ・セキュリティの無効化オプション（DDS）で制御
  - デバッグ・ポートから Cortex-M0+ へのアクセスを無効化
- セキュア・モードと非セキュア・モードでデバッグの有効化と無効化が可能
  - デバッグ・アクセス制御とセキュリティは相互に独立
  - セキュア・モードでは、セキュアな Cortex-M0+ 側でのみデバッグ・アクセスを変更可能

life.augmented

12

Cortex-M0+ のデバッグ・アクセスは、デバッグの無効化オプション・ビットで制御します。このアクセスはセキュリティから独立していて、セキュア・モードと非セキュア・モードの両方で有効化と無効化が可能です。セキュア・モードでは、セキュアな Cortex-M0+ 側でのみデバッグ・アクセス制御を変更できます。

Sub-GHz 無線のセキュリティ

- **セキュア･オプションで扱う Sub-GHz 無線アクセス**

- セキュア･ユーザ･オプションで扱う Sub-GHz 無線アクセス
- SUBGHZSPISD オプションで制御
  - Sub-GHz 無線へのアクセスを制御できるようにして、セキュアな Cortex-M0+ から排他アクセス
  - リセット時点からセキュリティ設定を適用

life.augmented

Sub-GHz 無線シリアル･ペリフェラル･インタフェースのセキュリティ無効化ユーザ･オプションにより、Sub-GHz 無線アクセスをセキュリティで保護できます。Sub-GHz 無線をセキュリティで保護して Cortex-M0+ からの排他アクセスを実現します。有効にすると、リセットの時点から Sub-GHz 無線アクセスがセキュリティで保護されます。

セキュアなペリフェラルの設定

- ペリフェラルのセキュリティはレジスタ·ビットで処理
- ペリフェラルのセキュリティを GTZC_TZSC で設定
  - 実行時にペリフェラルをセキュリティで保護可能
  - セキュアな CM0+ と非セキュアな CM4 との間で必要に応じてペリフェラルを共有
  - FSD でセキュリティを有効にしている場合にのみペリフェラルのセキュリティを利用可能
    - AES、PKA、ハードウェア乱数発生器
- DMA チャネルのセキュリティを DMA で設定
  - 実行時に DMA チャネルをセキュリティで保護可能
  - セキュアな CM0+ と非セキュアな CM4 との間で必要に応じて DMA チャネルを共有

life.augmented

Cortex-M0+ ファームウェアによって、AES アクセラレータ 1、公開鍵アクセラレータ、ハードウェア乱数発生器の各ペリフェラルを実行時にセキュリティで動的に保護できます。
Cortex-M0+ ファームウェアによって、DMA チャネルを実行時にセキュリティで動的に保護できます。
非セキュアな Cortex-M4 では、ペリフェラルのセキュリティ·ステータスに関する情報を読み出して取得できます。

特権による保護

- GTZC_TZSC のレジスタ·ビットで特権による保護を処理
  - 特権で保護したリソースを特権がないアクセスから保護可能
- 特権で保護したウォーターマークがメモリごとに 1 つ存在
- セキュリティで保護したリソースのみを特権で保護可能
  - メモリ、Sub-GHz 無線アクセス、AES、PKA、ハードウェア乱数発生器、DMA チャネル

life.augmented

特権による保護によって、特権があるアクセスによる排他アクセスが実現します。メモリごとにウォーターマークが 1 つあるので、特権で保護した部分と特権で保護していない部分にメモリを分割できます。
セキュリティで保護可能なペリフェラルも特権で保護できます。
特権による保護は実行時に有効化できます。

セキュア･ファームウェア･インストール/アップデート

- セキュア･ファームウェア･インストール機能でセキュアなファームウェアをインストール可能
  - システム･メモリから利用可能（Flash に関するモジュールを参照）
- セキュア･ファームウェア･アップデート機能は、秘匿保護されたセキュアな Flash 領域にインストール可能
- セキュアな Cortex-M0+ はすべての RDP レベルでユーザ･オプションを更新可能

life.augmented

16

STM32WL5 では、システム･メモリにセキュア･ファームウェア･インストール（SFI）ファームウェアが事前プログラムされています。
これにより、あらゆる Cortex-M0+ ソフトウェアをセキュリティで保護してインストールできます。
それ以降のファームウェア更新では、秘匿保護されたセキュアな Flash 領域にセキュア･ファームウェア･アップデート機能をインストールできます。
すべての読出し保護（RDP）レベル（0、1、2）でセキュアな Cortex-M0+ ソフトウェアの更新が可能です。

セキュリティ上の不正アクセス

- セキュアなリソースへの不正アクセスがあると、セキュアな Cortex-M0+ が通知を受領
- Cortex-M0+ が有効であれば、不正アクセスによって Cortex-M0+ があらゆる動作モードからウェイクアップ
- Cortex-M0+ ファームウェアが適切な措置を実行
- 不正なアクセスの情報を以下から取得
  - 特権で保護されたセキュアな、Flash、SRAM1、SRAM2 の各メモリ領域
  - 特権で保護されたセキュアな、DMA、DMAMUX、SUBGHZSPI、AES、PKA、ハードウェア乱数発生器の各ペリフェラル
  - GTZC と PWR でのセキュリティと特権の制御

life.augmented

特権で保護されたセキュアなリソースへの不正アクセスがあると、セキュアな Cortex-M0+ に通知されます。Cortex-M0+ ファームウェアによって適切な措置が実行されます。不正アクセスによって、リセットを含むあらゆる動作状態から Cortex-M0+ がウェイクアップします。

Cortex-M4 イベント

措置	CM4 で生成されるイベント
セキュアなメモリ領域から Cortex-M4 が実行をフェッチ	バス·エラー
特権で保護されたメモリ領域から、Cortex-M4 が特権のない実行をフェッチ	バス·エラー
セキュアな Flash メモリ領域に Cortex-M4 が読出しアクセス	ゼロ値の読出し
セキュアな RAM メモリ領域に Cortex-M4 が読出しアクセス	ゼロ値の読出し
セキュアなペリフェラル·レジスタに Cortex-M4 が読出しアクセス	ゼロ値の読出し

life.augmented

このスライドでは、Cortex-M0+ のセキュリティ機能によって Cortex-M4 コアに発生するイベントを挙げています。セキュアなメモリ領域から Cortex-M4 でどのような命令をフェッチしてもバス·エラーが生成されます。セキュアな領域からの読出しに対してはデータ値としてゼロが返されます。非セキュアな Cortex-M4 コアで読み出すことができるのは、セキュリティ設定のユーザ·オプションとペリフェラルのセキュリティ設定ビットのみです。

Cortex-M0 +イベント

措置	CM0+ で生成されるイベント
Cortex-M4 によるセキュリティ上不正なアクセス	ウェイクアップおよび割込み
特権で保護されたメモリ領域から Cortex-M0+ が特権のない実行をフェッチ	バス･エラー

life.augmented

このスライドでは、Cortex-M0+ のセキュリティ機能によって Cortex-M0+ に発生するイベントを挙げています。セキュアなリソースに対する Cortex-M4 の不正アクセスがあると、不正アクセス･イベントが生成されて Cortex-M0+ に送られます。

関連ペリフェラル

- この機能に関連する以下の各トレーニングを参照
  - STM32WL5 の Flash メモリ･インタフェース
    - セキュア･ユーザ･オプション
  - STM32WL5 のグローバル TrustZone 設定（GTZC）
    - ペリフェラルのセキュリティ･ビット
    - セキュリティ違反となる不正アクセスに対する制御
  - STM32WL5 電源コントローラ（PWR）
    - セキュリティ違反となる不正アクセスに対するウェイクアップ制御
  - DMA および DMAMUX
    - セキュアな DMA チャネル

life.augmented

このトレーニングのほか、Flash メモリ･インタフェース、グローバル TrustZone コントローラ、電源コントローラ、DMA および DMAMUX に関する各モジュールも有用です。