STM32WL MEMPROTECT

メモリ保護機能

レビジョン 1.0

STM32 システム・メモリ保護のプレゼンテーションへようこそ。ここでは、外部と内部からの攻撃からコードとデータを保護する手段をいくつか取り上げます。

概要

- 内部組込みソフトウェアとデータの読み書き保護を以下の領域に提供
  - Flash メモリ
  - SRAM1 および SRAM2
  - バックアップ·レジスタ
- Cortex-M0+ のコードとデータをユーザ·アプリケーションから保護

アプリケーション側の利点

- STM32 の内部組込みソフトウェアの知的財産を保護
- JTAG インタフェースなどを通じた外部攻撃によるコードのハッキングと読出しを防止
- 不必要な消去や偶発的な消去からコードとデータを保護(ローダや較正データなど)
- ファームウェア、SFI、SBSFU のセキュアな実行を実現

life.augmented

2

ソフトウェア·プロバイダは、悪意のあるユーザや侵入攻撃から自社ソフトウェアの知的財産を保護する必要があります。STM32WL5 マイクロコントローラには、この目的のために、Flash メモリ、SRAM1、SRAM2、バックアップ·レジスタに置かれたコードとデータを保護する機能をいくつか備えています。JTAG デバッガ、エンドユーザのコード、SRAM に潜むトロイの木馬のコードによるコードとデータの読出しや書込みを、これらの機能で防止できます。

Cortex-M0+ コアで実行されているアプリケーション·ファームウェアを対象として、新たな専用の保護メモリ機能が用意されています。この CPU は、保護されているセグメントに排他アクセスできます。

主な機能

- Cortex-M0+ セキュリティ
  - Flash メモリ、SRAM1、SRAM2 の上位部分を保護して Cortex-M0+ からの排他アクセスを実現
- 読出し保護(RDP)
  - レベル 0:読出し保護なし
  - レベル 1:メモリ読出し保護
  - レベル 2:チップ読出し保護
- 商用コード読出し保護(PCROP)
  - 設定可能な 2 つの Flash メモリ領域
- 書込み保護(WRP)
  - Flash メモリあたり 2 つの領域を設定可能

- ユーザ・アプリケーションからワイヤレス・スタックおよび SFI と SBSFU のコードとデータを保護
- JTAG インタフェースからのアクセスや Flash メモリ以外からのブートがあった場合に Flash メモリにあるコードを保護
- Flash メモリのコードは実行専用で、読出し不可
- 不必要な書込み操作や消去操作から Flash メモリのコードを保護

life.augmented

3

コードを保護するために以下の手段が用意されています。

- Cortex-M0+ のセキュアな Flash メモリ、SRAM1、SRAM2 アプリケーション・ファームウェア、セキュア・ファームウェア・インストール、セキュア・ブート、セキュア・ファームウェア・アップデートなどの Cortex-M0+ コードとデータに、Cortex-M4 で実行されているユーザ・アプリケーションからアクセスできないようにします。
- RDP:読出し保護(ReaDout Protection)
  すべての Flash メモリ領域に JTAG からアクセスできないようにします。
- PCROP:商用コード読出し保護(Proprietary Code ReadOut Protection)
  悪意のある 3rd パーティ・コード(トロイの木馬)を実行している CPU から、設定可能な Flash メモリ領域に読出しアクセスできないようにします。
- WRP:書込み保護機能
  偶発的または悪意による書込み操作と消去操作を防止します。

Cortex M0+ セキュリティ、RDP、PCROP、WRP は、STM32WL5 のオプション・バイトで設定できます

Cortex-M0+ セキュリティ(1/2)

- Cortex-M0+ セキュリティ
  - Cortex-M4 とデバッグ･アクセスからコードとデータを保護
- 以下のコード、揮発性データ、不揮発性データを保護
  - Cortex-M0+ のアプリケーション･ファームウェア
  - SFI（セキュア･ファームウェア･インストール）
  - SBSFU（セキュア･ブート、セキュア･ファームウェア･アップデート）

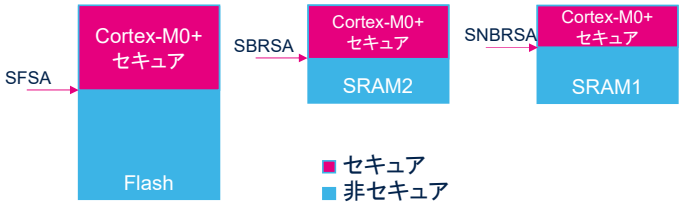
この機能の詳細については、以下の該当トレーニング･モジュールを参照
- STM32WL5 システムの CM0+ セキュリティ
- STM32WL5 セキュリティのルート･セキュリティ･サービス（RSS）

life.augmented

Cortex-M0+ セキュリティの各機能は、Cortex-M4 コア上で実行されているユーザ･アプリケーションから、Cortex-M0+ コア上で実行されているファームウェアのコードとデータを保護します。
これにより、セキュア･ファームウェア･インストール（SFI）、セキュア･ブートのセキュア･ファームウェア･アップデート（SBSFU）、Cortex-M0+ のアプリケーション･ファームウェアを確実にセキュアな状態で実行できるほか、これらのファームウェアへのデバッグ･アクセスも防止できます。
Cortex-M0+ アプリケーション･ファームウェアをインストールするときに、Cortex-M0+ セキュリティの各機能が有効になります。
Cortex-M0+ セキュリティの保護機能、SFI、SBSFU の詳細については、このトレーニングで紹介している該当のモジュールを参照してください。

Cortex-M0+ セキュリティ(2/2)

- Flash、SRAM1、SRAM2 の各メモリに関連する保護
  - Flash メモリの上位部分：Flash ページで整列した境界に従い、SFSA オプション･バイトで設定
  - SRAM1 と SRAM2 の上位部分：1 KB の粒度により、それぞれ SBRSA オプションと SNBRSA オプションで設定



- 保護領域のセキュリティは、Cortex-M0+ アプリケーション･ファームウェアのインストールまたは更新の際に設定

life.augmented

5

Cortex-M0+ セキュリティは、Flash、SRAM1、SRAM2 の各メモリの上位部分を保護します。各領域のサイズは、Cortex-M0+ アプリケーション･ファームウェアのインストールまたは更新の際に設定されます。
セキュアな Flash メモリの開始アドレス（SFSA）は、保護されている Flash メモリの下位境界です。このアドレスは、Flash ページの粒度で整列されます。
SRAM2 のセキュアなバックアップ RAM の開始アドレス（SBRSA）と SRAM1 のセキュアな非バックアップ RAM の開始アドレス（SNBRSA）は、それぞれ SRAM2 と SRAM1 の保護されている領域の下位アドレスです。それぞれのサイズは 1 KB の粒度で設定できます。

読出し保護（RDP）

読出し保護機能について詳しく説明します。

読出し保護(1/3)

- 読出し保護レベル 0(保護なし、工場出荷時設定)
  - Flash メモリ、SRAM2、バックアップ・レジスタに対するすべての操作(読出し、書込み、消去)が可能
  - 両方の CPU でオプション・バイトを変更可能
- 読出し保護レベル 1
  - ユーザ Flash メモリからブートするブート・モードを選択していて(Boot0 = 0)、デバッガからのアクセスが検出されていない場合(JTAG なし):
    - Flash メモリ、SRAM2、バックアップ・レジスタに対するすべての操作(読出し、書込み、消去)が可能オプション・バイトを変更可能
  - ユーザ Flash メモリからブートするブート・モードを選択していない場合(Boot0 = 1)、またはデバッガからのアクセスが検出された場合(JTAG):
    - Flash メモリ、SRAM2、バックアップ・レジスタに対するすべての操作(読出し、書込み、消去)をブロック(ハード・フォールトを生成)オプション・バイトを変更可能

life.augmented

7

STM32WL5 の読出し保護機能には、SRAM2、Flash メモリ、バックアップ・レジスタのすべてに対する 3 段階の保護レベルが用意されています。

- レベル 0 では保護が機能しません。これは工場出荷時のデフォルト設定です。SRAM2、Flash メモリ、バックアップ・レジスタに対する読出し、書込み、消去の各操作が許可されています。レベル 0 ではオプション・バイトを変更できます。PCROP と Cortex-M0+ のセキュリティ・ルールが適用されることに留意してください。
- レベル1 では、Flash メモリとバックアップ・レジスタに対して読出し保護が機能します。また、STM32 ファミリでの新しい機能として SRAM2に対しても読出し保護が機能します。

デバッガからのアクセスが検出された場合、または Flash メモリ領域からブートするブート・モードを設定していない場合は、Flash メモリ、バックアップ・レジスタ、SRAM2 のどれにアクセスしてもシステム・ハード・フォールトが生成されます。その結果、次回のパワーオン・リセットまですべてのコード実行がブロックされます。レベル 1 でもオプション・バイトを変更できます。

読出し保護(2/3)

- 読出し保護レベル 2 (JTAG ヒューズ)
  - レベル 1 によるすべての保護がアクティブ
  - RAM からのブートとシステム・メモリ(ブートローダ)からのブートは不可(ユーザ Flash メモリからのブートのみが可能)
  - JTAG インタフェースは無効。JTAG/SWD によるデバッグとプログラミングは不可能(JTAG が無効状態)
    - デバッグとプログラミングができないためFAR(不良解析)でできることが制限される。
  - ユーザ Flash メモリからのブート・モードを選択した場合
    - Flash メモリ、バックアップ・レジスタ、SRAM2 に対するすべての操作(読出し、書込み、消去)が可能
  - オプション・バイトは内部的にも外部的にも変更不可(レベル 2 の状態で固定)

life.augmented

レベル 2 では、SRAM2、Flash メモリ、バックアップ・レジスタに対してレベル 1 と同様の保護が機能します。ただし、レベル 1 との間には次の 3 つの大きな相違点があります。

1. JTAG/SWD デバッガ接続が無効になります(バックドアが発生しないようにするため)
2. Boot0 と Boot1 の設定に関係なく、ブート・モードはユーザ Flash メモリからのブートに恒久的に固定されます。レベル 2 に設定すると元に戻すことはできません。
3. RDP と WRP をはじめとして、すべてのオプション・バイトは変更できなくなります。

読出し保護(3/3)

- RDP の解除
  - RDP レベル 2 は半恒久的で、インストールされているセキュアな Cortex-M0+ ファームウェア以外では解除不可
  - RDP レベル 1 は、次の手順で解除してレベル 0 に戻すことが可能
    - Flash メモリの部分的消去
      - メモリのユーザ使用部分を消去
        - 設定されている消去ポリシーに応じて PCROP 領域を削除
      - メモリのセキュアな部分は変更せずに保持
        - Cortex-M0+ セキュリティはアクティブな状態で保持
        - ワイヤレス·スタックと RSS は消去から除外
    - バックアップ·レジスタ全体と SRAM2 の非セキュアな部分を消去

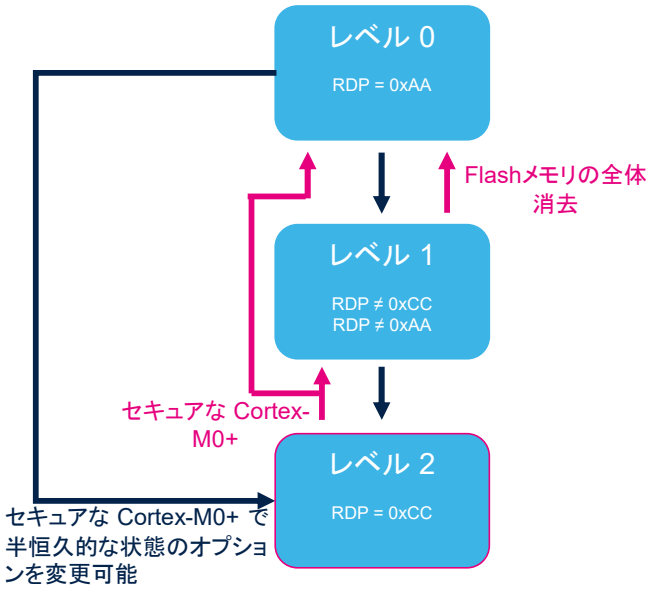
life.augmented

RDP の保護レベルは、現在の保護レベルが「1」の場合に変更できます。RDP レベル 2 は半恒久的で、インストールされているセキュアな Cortex-M0+ ファームウェアでのみ元のレベルに戻すことができます。
RDP の保護レベルを「1」から「0」に変更すると、Flash メモリの非セキュアな領域、SRAM2、バックアップ·レジスタが自動的に消去されます。Flash メモリのセキュアな部分はこの影響を受けず、セキュリティは変化しません。

RDP レベルの遷移スキーム

- レベル 0
  - オプション･バイトは変更可能
  - レベル 1 またはレベル 2 に遷移可能
- レベル 1
  - オプション･バイトは変更可能
  - レベル 0 またはレベル 2 に遷移可能
    - レベル 0 → ユーザ Flash メモリ、バックアップ･レジスタ、SRAM2 の全体消去
- レベル 2
  - セキュアな Cortex-M0+ でのみオプション･バイトを変更可能
  - インストールされているセキュアな Cortex-M0+ ファームウェアでレベル 0 またはレベル 1 に遷移可能

注：ユーザ Flash メモリ、バックアップ･レジスタ、SRAM2 は全体消去されない



読出し保護の各レベル間で可能な遷移について説明します。
すでに触れたように、STM32WL5 マイクロコントローラには 3 段階の RDP レベルが用意されています。

1. レベル 0 では、メモリからの読出しが保護されませんが、オプション･バイトは変更できます。
   レベル 0 のデバイスは、レベル 1 またはレベル 2 へ移行できます。
2. レベル 1 では、デバッグ･アクセスが有効な場合にメモリからの読出しを保護できます。
   レベル 1 のデバイスは、レベル 0 またはレベル 2 へ移行できます。
   レベル 0 に解除すると Flash メモリが全体消去されます。
3. レベル 2 ではレベル 1 と同様の読出し保護が得られますが、JTAG/SWD のデバッグ･アクセスが自動的に無効になります。
   レベル 2 は半恒久的な状態であり、他の RDP レベルへの解除は、インストールされているセキュアな Cortex-M0+ ファームウェアでのみ可能です。
   レベル 2 から解除する場合の注意事項：ハードウェアによる全体消去はできません。読出し保護レベルを解除する前に機密情報を消去するには、インストールされているセキュアな Cortex-M0+ ファームウェアを使用する必要があります。

アクセス･ステータスと RDP レベルとの関係

領域			保護 RDP レベル	ユーザ Flash メモリからブートする場合のアクセス権限	ユーザ Flash メモリからブートしない場合またはデバッグ･アクセスが検出された場合のアクセス権限
Flash メモリ	メイン･メモリ	非セキュア	1	R/W/E（CPU1 と CPU2）	アクセスなし
			2	R/W/E（CPU1 と CPU2）	-
		セキュア	1	R/W/E（CPU2）	アクセスなし
			2	R/W/E（CPU2）	-
	システム･メモリ		1	R	R
			2	R	-
	オプション･バイト	非セキュア	1	R/W/E	R/W/E
		すべて	2	R（CPU1）、R/W/E（CPU2）	-
	バックアップ･レジスタ		1	読出し／書込み	アクセスなし
			2	読出し／書込み	-
	SRAM2	非セキュア	1	R/W/E（CPU1 と CPU2）	アクセスなし
			2	R/W/E（CPU1 と CPU2）	-
		セキュア	1	R/W/E（CPU2）	アクセスなし
			2	R/W/E（CPU2）	-

W：書込み
R：読出し
E：消去

life.augmented

11

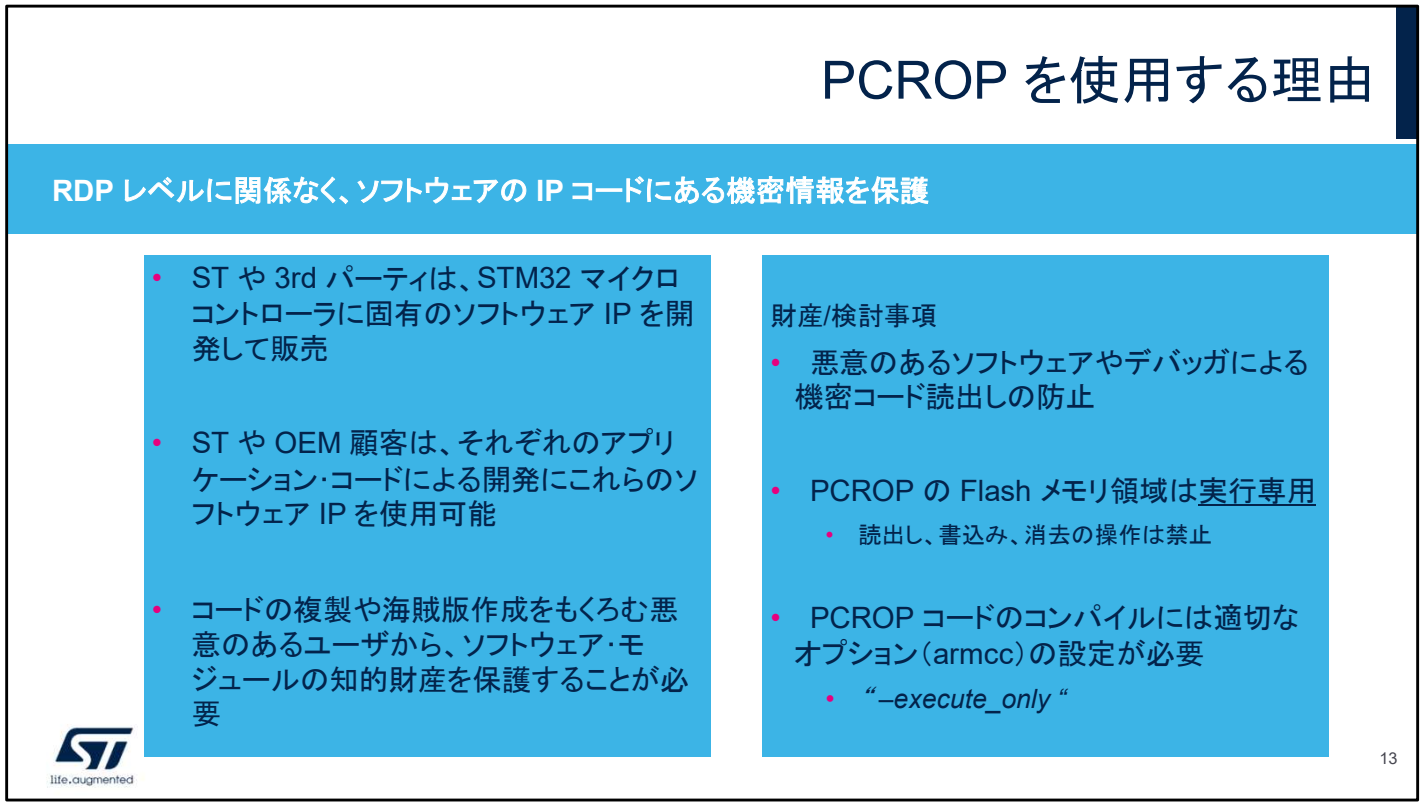
この表は、読出し保護（RDP）レベル 1 とレベル 2、設定されているブート･モード、およびデバッグ･アクセスに応じて、Flash メモリ、バックアップ･レジスタ、SRAM2 へのアクセスとして許可される形態を、ここまでの説明に従って示したものです。まとめると次のようになります。

- RDP をレベル 0 に設定すると読出し保護機能はアクティブにならず、すべてのメモリを読み出すことができ、また変更できます。**セキュアなメモリとオプション･バイトへはセキュアな CPU2 からのみアクセスできます。**
- RDP がレベル 0 以外の場合は次のようになります。

ユーザ Flash メモリからブートするようにデバイスを設定している場合：
→ ユーザ Flash メモリ、バックアップ･レジスタ、SRAM2 に対しては、RDP レベルに関係なく、読出しと変更ができます。
→ システム Flash メモリは読出し専用です。
→ RDP をレベル 2 に設定している場合、CPU1 ではオプション･バイトについて読出しだけできます。セキュアな CPU2 では、オプション･バイトの読出しと書込みができます。
ユーザ Flash メモリからブートするようにデバイスを設定していない場合、またはデバッグ･アクセスを検出しない場合：
→ システム Flash メモリを除き、ほとんどすべてのメモリにアクセスできません。システム Flash メモリに対してはレベル 1 で読出しのみができます。オプション･バイトはレベル 1 で読み出すことができ、また変更できます。

商用コード読出し保護（Proprietary code readout protection: PCROP）

商用コード読出し保護（PCROP）の詳細と RDP との違いについて説明します。



PCROP は、商用コード読出し保護（Proprietary Code ReadOut Protection）の略です。
PCROP を使用する理由は次のとおりです。
商用コード読出し保護とは、基本的に、3rd パーティのソフトウェアにある知的財産コードの機密を、RDP レベルの設定に関係なく保護する手段です。
3rd パーティは、STM32 マイクロコントローラに使用できる自社固有のソフトウェア IP を開発し、販売できます。OEM 製造元は、それぞれのアプリケーション·コードを開発する際に、このようなソフトウェア IP を使用できます。商用コード読出し保護は、3rd パーティ IP の機密を保護するうえで効果的であり、悪意のあるユーザからソフトウェアの知的財産を保護します。
言い換えると、PCROPによって、悪意のあるソフトウェアやデバッガによる機密コードの読出しを防止できます。
保護領域は実行専用です。STM32 CPU のみから命令コードとしてアクセスでき、その他すべてのアクセス（DMA、デバッグ、CPU によるデータ読出し、書込み、消去）は厳格に禁止されています。つまり、保護されているコードのコンパイルには、固有のコンパイラ·オプションを使用する必要があります。
例：“–execute_only”（Keil ツール向け）

PCROP の設定と制約

- 設定と制約
  - PCROP の領域はオプション･バイトの設定で定義
  - Flash ページの半分の粒度で 2 つの保護領域を設定可能
  - PCROP 領域のサイズは大きくすることができるだけで、小さくすることは不可
  - PCROP を非アクティブにする方法は RDP をレベル 1 からレベル 0 に遷移することのみ
- オプション･ビット PCROP_RDP
  - このビットを有効にすることで、RDP をレベル 1 からレベル 0 へ遷移するときに PCROP 領域の消去を防止。このビットを有効にしないと、Flash メモリは全体消去。

life.augmented

Flash メモリの商用コード読出し保護領域はオプション･バイトで定義します。
STM32WL5 デバイス上では PCROP 機能が向上します。現在は、2 つの独立した PCROP 領域を別々に設定できます。それぞれに Flash ページの半分の粒度で開始アドレスと終了アドレスを定義します。設定した PCROP 領域のサイズは大きくすることのみが可能です。
定義した PCROP 領域に対する保護機能を無効にするには、RDP の保護レベルを「1」から「0」に変更する以外にありません。これによって、Flash メモリ領域が消去されます。

RDP レベルを解除した場合に PCROP 領域を消去するためのポリシーは、PCROP_RDP オプション･ビットで定義します。オプション･バイトの PCROP_RDP ビットを設定すると、PCROP 領域のコードが失われないので、保護は解除されません。

PCROP の「実行専用」の意味を詳しく説明します。
PCROP は RDP のサブステートです。PCROP の設計では、PCROP で保護されている Flash メモリ領域を、STM32 上で実行されている他のコードからは読み出せないようにしています。この点は、保護のターゲットが外部である RDP と異なります。
PCROP を有効にすると、AHB によって命令バスの動作のみが許可されるので、コードの実行のみが可能です。データ･バスからは、保護されている Flash メモリ領域にアクセスできません。
開発段階が終了すれば、PCROP を有効にしたまま RDP をレベル 1 に設定できます。この場合、外部からのアクセスは読出し専用に制限されます。ただし、特定セクタの PCROP 設定は、この領域のコードを読み出そうとするすべてのマスタに引き続き適用されます。

書込み保護

STM32WL5 の書込み保護設定について詳しく説明します。

Flash への書込み保護

- 設定と制約
  - 書込み保護領域をオプション･バイトで定義
  - STM32WL5 では、Flash ページのページ粒度で 2 つの WRP 領域を設定可能
  - RDP がレベル 2 でなければ、オプション･バイトの変更によって WRP 領域のサイズをいつでも変更可能、セキュアな Cortex-M0+ のみは RDP がレベル 2 でも WRP を変更可能
- 特性
  - 定義されて有効になっている WRP 領域に対しては書込み操作と消去操作が禁止

life.augmented

16

Flash メモリの書込み保護機能は、Flash メモリの定義済み領域に対する不必要な書込みアクセスを防止するように設計されています。この領域には、セキュア･ブート、セキュア･ファームウェア･アップデートや変化しない較正定数などを配置します。
書込み保護領域はオプション･バイトで定義します。最大で 2 つの独立した書込み保護領域を Flash メモリに定義できます。この 2 つの Flash メモリ領域のそれぞれは、Flash ページの粒度による開始アドレスと終了アドレスで定義します。
RDP がレベル 2 でなければ、書込み保護領域のサイズはいつでも変更できます。セキュアな Cortex-M0+ のみは、RDP がレベル 2 でも WRP を変更できます。
消去操作は書込み保護領域に対する書込み操作として扱われるので、許可されません。

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
    - Flashメモリのアーキテクチャ
  - STM32WL5 システムの CM0+ セキュリティ
    - Cortex-M0+ 機能の説明と設定
  - STM32WL5 のセキュリティ･サービス
    - SFI、SBSFU の各機能の説明

life.augmented

17

このトレーニングのほか、これら 3 つのモジュールも有用です。