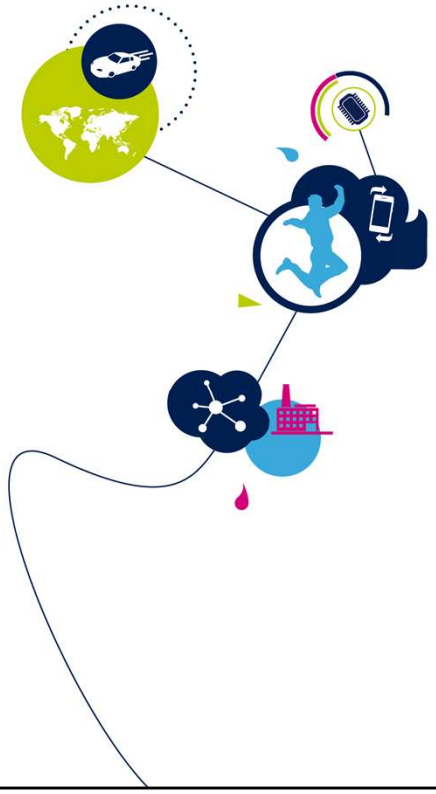
STM32G4 - MEMPROTECT

メモリ保護機能

1.0版



life.augmented

STM32 システムメモリ保護のプレゼンテーションにようこそ。
コードやデータを保護するさまざまな 手段について説明します。

概要

- 目的:
  1. 内部の組込みソフトウェアやそれに含まれるデータに読出しと書込みの保護を提供:
     - Flashメモリ
     - コア結合メモリ(CCM) SRAM
     - バックアップ·レジスタ
  2. 機密性の高いファームウェアの安全な実行を提供

アプリケーション側の利点

- STM32内の組込みソフトウェアの知的財産権を保護
- JTAGインタフェースその他の外部攻撃手段を通じたコードのハッキングやコードのダンプを防止
- 不要／偶発的な消去からコード／データを保護(ローダ、較正データ)
- セキュア·アプリケーションの開発 (セキュア·ブートまたはセキュア·ファームウェア更新)を可能に

life.augmented

メモリ保護は、さまざまな目的のために設計されています。
保護メモリは、フラッシュ メモリ、コア結合メモリ (または CCM) SRAM、およびバックアップ レジスタです。
たとえば、読取り保護は、外部アクセスを通じて埋め込みソフトウェアコードをダンプすることを防ぎ、開発者の知的財産を保護します。
書込み保護は、ソフトウェアまたはデータ更新手順でのオーバーフローによって、特定のフラッシュセクタが誤って消去されることを防ぎます。
STM32G4マイクロコントローラは、フラッシュメモリおよびバックアップレジスタにあるコードとデータを保護するためのいくつかの機能を提供します。
これらの典型的なメモリ保護に加えて、STM32G4は、機密性の高いファームウェアの安全な実行を保証する新しいメカニズムも導入しています。
以下のスライドでは、これらすべての保護機能について説明します。

主な機能

- **読出し保護(RDP)**
  - 外部アクセスに対してFlashメモリ、CCM SRAM、バックアップ·レジスタをグローバルに保護
  - ブートがユーザのFlashメモリ内からと異なる場合、メモリとレジスタはSWD/JTAGアクセスから保護
  - 保護なし、から永続的かつ完全な保護までの、3つのRDPレベルを定義
- **独自仕様コード読出し保護(PCROP)**
  - ソフトウェアIPの読出しおよび書込みアクセスに対するFlashメモリ領域の保護
  - PCROP属性を持つFlashメモリ·コードは実行のみ可能

保護はRDP レベルに依存

リクエスト	アクセス許可
読出し	不可
書込み	不可
実行	**可能**

life.augmented

コード保護のために以下の手段が提供されます。:
RDP: 読出し保護(ReaDout Protection)
PCROP:独自仕様コード読出し保護 (Proprietary Code ReadOut Protection)
WRP: 書込み保護(WRite Protection)
セキュアなユーザーメモリ保護は、STM32G4マイクロコントローラの新機能です。コードとデータ保護に加えて、機密性の高いアプリケーションを安全に実行可能です。
読み出し保護(RDP)は、フラッシュメモリ、オプションバイト、CCM SRAMとバックアップレジスタへの外部読み取りアクセスを防ぐグローバルメカニズムです。外部アクセスは、JTAGコネクタ、シリアルワイヤポート、またはSRAMに組み込まれたブートソフトウェアを使用してデータを取得しようとするアクセスです。
RDP保護の3つのレベルは、全く保護を提供しないレベル0から永続的かつ完全な保護を備えたレベル2まで定義されます。
保護レベルは、次のスライドで説明します。
PCROP は、コードダンプに対するメモリ アクセス保護です。コードの知的財産を保護するために使用されます。
保護されたファームウェアは実行可能なままですが、悪意のあるサードパーティコード(トロイの木馬など)を実行しているCPUによって実行される読み取りおよび書き込みアクセスを防止します。

主な機能

- **書込み保護(WRP)**
  - Flashメモリ·セクタによる書込み/消去/プログラム·アクセスに対する保護
  - 書込み保護属性を持つFlashメモリ·コードは、不要な書込みまたは消去の操作から保護される

リクエスト	アクセス許可
読出し	可能
書込み	**不可**
実行	可能

- **セキュア·ユーザ·メモリ保護**
  - 感度の高いファームウェア実行のため、特定のアクセス·メカニズムによるFlashメモリ領域保護
  - この領域のコードとデータはリセット後にのみアクセス可能
  - コードは他のプロセスの前に実行される
  - 実行されると、保護領域は閉じられ、次のリセットまでアクセス出来なくなる

リクエスト	アクセス許可
セキュア 読出し	可能
非セキュア 読出し	不可
セキュア 書出し	可能
非セキュア 書出し	不可
セキュア 実行	可能
非セキュア 実行	不可

life.augmented

書込み保護メカニズムは、偶発的または悪意のある書込み/消去操作を防ぎます。
セキュア・ユーザー・メモリは、コードおよびデータ保護に加えて、機密ファームウェアのセキュアな実行を保証する特定の保護メカニズムを備えたフラッシュ・メモリ領域です。
すべての保護メカニズムは、STM32G4オプションバイトを介して設定可能です。セキュア ブートが実行されると、次のリセットまで、ユーザー の安全なメモリにアクセスできなくなることに注意してください。

STMG43X/4XとSTM32G47X/8Xの違い

	STM32G43X/4X (カテゴリ2)	STM32G47X/8X (カテゴリ3)	
		FLASH_OPTR[DBANK]=0 (シングルバンク)	FLASH_OPTR[DBANK]=1 (デュアルバンク)
バンク数	1	1	2
ページ サイズ	2キロバイト	4キロバイト	2キロバイト
書込み保護領域 (WRPs)	2	4	2 / バンク
独自仕様コード読出し保護 (PCROPs)	1	2	1 / バンク
セキュリティ保護可能なメモリ領域	1	2	1 / バンク

このスライドでは、カテゴリ2マイクロコントローラと呼ばれるSTM32G43X/4Xと、カテゴリ3マイクロコントローラと呼ばれるSTM32G47X/8Xの実装されたフラッシュメモリに関する違いについてハイライトします。
DBANK オプション・ビットに応じて、カテゴリ2 のバンクの数は1つ、カテゴリ3 の場合は 1つ、または 2つ です。
最小の消去の粒度になるページ サイズは、カテゴリ 2 では 2 キロバイト、カテゴリ 3 はシングル バンクの場合は 4 キロバイト、デュアル バンクを持つカテゴリ 3 の場合は 2 キロバイト です。
保護機能に関して、カテゴリ2のマイクロコントローラは1つの書込み保護領域、1 PCROPおよび1つのセキュリティ保護可能なメモリ領域を有し、カテゴリー3のマイクロコントローラには2つの書込み保護領域、2つのPCROPsおよび2つのセキュリティ保護可能なメモリ領域を持ちます。

読出し保護

保護レベル 0 および 1

- RDPレベル0
  - 保護が設定されておらず、Flashメモリ、CCM SRAM、およびバックアップ·レジスタですべての操作(読出し/書込み/消去)が許可されている
  - オプション·バイトの変更が可能
- RDPレベル1
  - デバッグ·ポートが接続されている間、または RAM もしくはシステムFlashメモリ·ブートローダから起動した場合、Flashメモリおよびバックアップ·レジスタへのアクセス (読出し/消去/プログラム) は実行できない
    - 読出しまたは書込みリクエストでバス·エラーが生成
  - ユーザがプログラムしたFlashメモリから起動するとき、ユーザ·コードから保護されたメモリへのアクセスが許可
  - オプション·バイトの変更は可能で、レベル0への保護レベルへの変更は可能だが、Flashメモリ、CCM SRAM、バックアップ·レジスタが全消去される

life.augmented

最下位の RDP レベル 0 が設定されている場合、デバイスは保護されません。フラッシュ メモリ上のすべての読出しまたは書込み操作 (書込み保護が設定されていない場合) は、すべてのブート構成 (フラッシュ ユーザー ブート、デバッグ、RAM からのブートなど) で CCM SRAM とバックアップ レジスタを実行できます。
オプション・バイトもこのレベルで変更可能です。
レベル 0 は工場出荷時のデフォルト レベルです。
レベル 1 では、読出し保護はフラッシュ メモリ、CCM SRAM、およびバックアップ レジスタに設定されます。
このレベルでは、保護されたメモリは、フラッシュメモリのユーザーコードから起動するときにのみアクセス可能です。
デバッガからのアクセスが検出されるか、ブートがユーザーのフラッシュメモリ領域に設定されていない場合、保護されたメモリへのアクセスは、システムのハード フォルトを生成し、次の電源投入がリセットされるまですべてのコード実行をブロックします。
オプションバイトはこのレベルでは変更可能なため、保護を解除できます。このメカニズムについては、次のスライドで説明します。

読出し保護

レベル回帰と保護レベル 2

- レベル1 からレベル0 への保護レベルの回帰
  - Flashメモリ、CCM SRAM、バックアップ·レジスタの全消去
    - 保護領域(PCROP およびセキュア·ユーザ·メモリ)は、消去ポリシーに依存する
  - オプション・バイトおよび OTPバイトは消去されない
- RDPレベル2
  - レベル1によって提供されるすべての保護が、アクティブかつ永久
  - オプション·バイトは、内部から、または外部からも変更出来ない
  - SWD/JTAG は無効
  - RAM またはシステム·メモリ (ブート·ローダ) からのブートは許可されない
  - ユーザFlashメモリでのみブートが許可され、Flashメモリとバックアップ·レジスタ上のすべての操作(読出し/書込み/消去)が有効になる

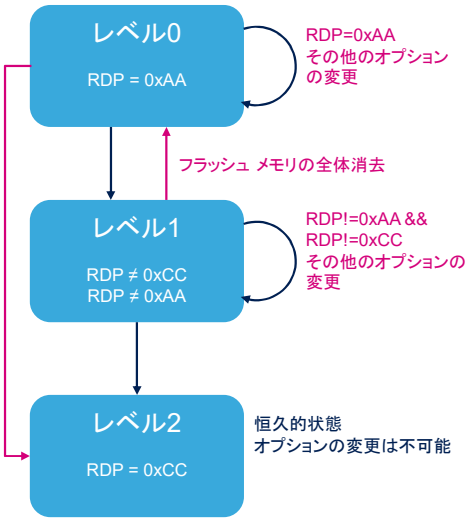
life.augmented

前のスライドでは、レベル 1 でオプションバイトを変更することが可能であることを確認しました。保護レベルをレベル 0 に変更することで、保護を解除できます。
この保護レベルの回帰により、フラッシュ メモリ、CCM SRAM、およびバックアップ レジスタが一括で全消去されます。
PCROP によって保護されるか、またはセキュア・ユーザー・メモリーとして構成されたフラッシュ領域は、消去ポリシーの設定に応じて消去または変更されないままにすることができます。
読み出し保護レベル 2 はレベル 1 と同じ保護を提供しますが、永久に保護されます。オプションバイトは変更できなくなるため、RDP 保護がこのレベルに設定されると、それを変更する方法はなく、全消去メカニズムによるレベル回帰は不可能になります。このレベルは、開発段階が完了した場合にのみ最終製品で考慮する必要があります。
この保護はST工場でも解除できないことに注意してください。

読出し保護

遷移スキーム

- レベル0 / RDP= 0xAA
  - オプション･バイトは修正可能
  - レベル1または2への遷移が可能
- レベル1 / RDP != (0xAA | 0xCC)
  - オプション･バイトは修正可能
  - ユーザFlashメモリ、バックアップ･レジスタ、CCM SRAMの全体消去でレベル0に移行
  - 永続的な保護(レベル2)への遷移が可能
- レベル2 / RDP = 0xCC
  - オプション･バイトが固定される
  - 他のレベルへの遷移不可能



このスライドでは、各読出し保護レベル間の可能な遷移を示します。保護レベルを上げることは常に可能ですが、回帰はレベル 1 とレベル 0 の間でのみ可能です。
RDP がレベル 1 からレベル 0 に遷移するように値 0xAA に再プログラムされると、フラッシュ メイン メモリの全体消去が実行されます。バックアップレジスタと CCM SRAM も消去されます。OTP 領域は、全体消去の影響を受けず、変更されません。
FLASH_PCROP1ERレジスタのビットPCROP_RDPがクリアされると、完全な一括消去は、PCROPによって保護されているページを除いて、PCROPがアクティブなバンクでの連続したページ消去である部分的な一括消去に置き換えられます。これは PCROP コードを保持するために行われます。
RDP レベルは 1 つのオプション バイトでコーディングされています。レベル 0 は 0xAA 値でコーディングされ、レベル 2 は 0xCC 値でコーディングされ、レベル 1 は 0xAA または 0xCC 以外の値でコーディングされます。

読出し保護

サマリー

エリア	保護レベル (RDP)	ユーザFlashメモリで ブートするときのアクセス権	RAM からのブートか、ブートローダまたはデバッガからの アクセスでブートした場合のアクセス権
メインFlashメモリ	1	R/W/E	アクセスなし
	2	R/W/E	N/A、ユーザFlashメモリ内での起動のみが許可される
システムFlasメモリ (ブートローダー)	1	R	R
	2	R	N/A、ユーザFlashメモリ内での起動のみが許可される
オプション・バイト	1	R/W/E	R/W/E
	2	R	N/A、ユーザFlashメモリ内での起動のみが許可される
バックアップ・レジスタ	1	R/W	アクセスなし
	2	R/W	N/A、ユーザFlashメモリ内での起動のみが許可される
CCM SRAM	1	R/W	アクセスなし
	2	R/W	N/A、ユーザFlashメモリ内での起動のみが許可される
OTP	1	R/W	アクセスなし
	2	R/W	N/A、ユーザFlashメモリ内での起動のみが許可される

W:書込み　R: 読出し　E:消去

life.augmented

この表は、前のスライドで見られるように、読出し保護 (または RDP) レベル、構成されたブート モード、およびデバッグ アクセスに従って、フラッシュ メモリとバックアップ レジスタに対して、認可されてるさまざまなアクセスの種類をまとめたものです。

PCROP

10

ソフトウェアIPコードの機密性を保護

- ソフトウェアの知的財産保護
  - STまたはサードパーティは、STM32マイコン用の特定のソフトウェアIPを開発および販売することが出来る
    - これらのIPは、さらなるアプリケーション開発のために使用され、不正コピーから保護する必要がある
  - PCROP機能により、内部(悪意のあるファームウェア)または外部Flashメモリ･アクセス(デバッグ･ポート)からのダンプに対するソフトウェアIP保護が保証される
- PCROP の特性
  - PCROP領域は実行専用
    - 読出し/書込み/消去の操作は許可されていない
    - PCROPコードは、このメモリ属性に準拠するために適切なオプション (armcc) “ –execute_only” を使用してコンパイルする必要がある
  - RDPレベルに関係なく保護が有効

life.augmented

PCROP は、独自のコード読み出し保護を意味します。
サードパーティは、STM32マイクロコントローラ用の特定のソフトウェアIPを開発および販売する場合があり、相手先ブランド機器メーカーは、独自のアプリケーションコードを開発する際に使用することができます。ソフトウェアの知的財産 (または IP) を保護するために、コードをコピーまたは読み取りしないでください。PCROP の目的は、サードパーティ製ソフトウェアの知的財産コードの機密性を、RDP レベルの設定に依存しない悪意のあるユーザーから保護することです。
保護されたファームウェアは Cortex®-M4 コアによってのみ実行できます。その他のアクセス(DMA、デバッグ、データの読出し、書込み、消去など)は厳しく禁止されています。
この制約に準拠するには、ファームウェアを適切なコンパイル オプションでコンパイルする必要があります。たとえば、「–execute_only」(Keil ツールの場合)。このオプションを指定しないと、リテラル プールと呼ばれる読み取り専用セクションの関数と定数がインターリーブされます。
Cortex-M4 MPU は、実行のみのアクセス許可をサポートしていません。

PCROP

11

設定/設定解除

- 設定
  - 各PCROP領域は、16バイトまたは32バイトからフルバンクまでの物理Flashバンクベース･アドレスに関連する開始ページオフセットと終了ページオフセットによって定義される
  - PCROP領域はオプション･バイト･レジスタを介して定義される
- 設定解除
  - PCROPを非アクティブ化する唯一の方法は、RDPレベルのレベル1 からレベル0 への回帰
    - この回帰レベルは、Flashメモリの全消去の操作をトリガ
  - 追加オプション･ビット (PCROP_RDP) を使用すると、RDP保護がレベル1からレベル0に変更されたときに、PCROP領域を選択して消去することが可能

life.augmented

フラッシュ メモリ内の独自のコード読出し保護領域は、オプション バイトを使用して定義されます。
各 PCROP 領域は、16 バイトまたは 32 バイトのフルバンクまでの物理フラッシュ バンクベース アドレスに関連する開始ページ オフセットと終了ページ オフセット、カテゴリ 2 デバイスの場合は 16 バイト、デュアル バンクを持つカテゴリ 3 デバイスの場合は 32 バイト、シングルバンクを持つカテゴリ 3 デバイスの場合は 32 バイトで定義されます。
これらの領域は、データ アクセスから保護されます。
PCROP 機能で保護されたセクタも書込みアクセスから保護され、不要なセクター書込み操作や消去操作に対する保護を提供します。

PCROP 保護は、RDP レベル回帰でレベル 1 からレベル 0 に対してのみ削除できます。このメカニズムを実行すると、フラッシュ メモリの完全な一括消去がトリガされます。
RDP 保護がレベル 1 からレベル 0 に変更されると、PCROP_RDPオプション･ビットに応じて、PCROP 領域は消去されます。

Flashメモリの書込み保護

不要な消去や偶発的な消去からコードとデータを保護

- 保護属性への書込み
  - 保護されたセクタは消去またはプログラムできない
- セット/リセット
  - 保護は、Flashメモリの各ページに対して個別に設定
  - 保護はオプション·バイト·レジスタで設定
  - 書込み保護は RDPレベル0およびレベル1でリセット可能
    - RDPレベル2では変更できない
  - 書込み保護されたページがある場合、レベル回帰メカニズムは機能しない
    - 書込み保護は、レベル回帰によるFlashメモリの一括消去の前に削除する必要がある

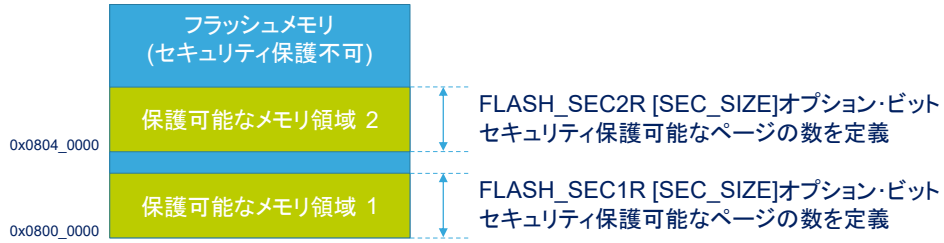
life.augmented

書込み保護により、コードや不揮発性データを不要な消去や偶発的な消去から保護します。
この保護はフラッシュ メモリでのみ使用できます。書込み保護は、選択したフラッシュ メモリ ページのみに設定できます。
ページが保護されている場合、ページを消去またはプログラムすることはできません。セクタへの書込みアクセスを試みると、フラッシュ メモリ エラーが発生します。
少なくとも 1 つのページが書き込み禁止の場合、フラッシュ メモリの一括消去は実行できません。保護を最初に削除する必要があります。

セキュリティ保護可能なメモリ領域

イントロダクション

- セキュリティで保護可能なメモリ領域の主な目的は、望ましくないアクセスからFlashメモリの特定の部分を保護するため
  - これにより、安全なキー・ストレージや安全なブートなどのソフトウェア・セキュリティ・サービスを実装可能



  - FLASH_SECiR[SEC_SIZE] オプション・ビットが0の場合、セキュリティ保護可能なメモリは実装されない
    - このフィールドはRDPレベル0でのみ変更可能

life.augmented

セキュリティで保護可能なメモリの目的は、ブート時に使用できるコードとデータを格納し、ブート プログラムがコントロール ビットを設定するとアクセスできなくなることにあります。
通常のユースケースは、セキュリティ保護可能なメモリに含まれる暗号キーを使用して、フラッシュ メモリに存在するソフトウェア イメージの認証と、場合によっては復号化を実行する場合にあります。認証プログラムと復号化プログラムも、セキュリティ保護可能なメモリに格納されます。
オプション ビットは、セキュリティ保護可能なメモリのサイズをページ単位で設定するために使用できます。Base アドレスは、Cortex-M4 リセット ベクターに対応する、セキュリティ保護可能なメモリ領域 1 に対して常に0x0800_0000になります。
セキュリティ保護可能なメモリ領域 2 はアドレス 0x0804_0000 から始まります。
オプションバイトのSEC_SIZEフィールドがゼロの場合、セキュリティ保護可能なメモリは実装されません。
このフィールドは RDP レベル 0 でのみ変更可能です。

セキュリティ保護可能なメモリ領域

- 既定では、リセット後、セキュリティ保護可能なメモリにアクセス可能
  - SEC_PROTiビットがレジスタ FLASH_CRに設定されると、次のリセットまで、確保可能なメモリ番号# iにアクセスできなくなる
  - リセットのみがSEC_PROTiビットをクリア可能

life.augmented

ソフトウェアがFLASH_CRレジスタにSEC_PROTiビットを設定すると、セキュリティ保護可能なメモリ番号 #i はアクセスできなくなります。
イメージ認証と復号化を実行するために使用されるセキュアブートの場合、SEC_PROTi ビットは、認証が成功したときに、イメージの最初の命令に分岐する直前に 1 に設定されます。
SEC_PROTiビットが設定されると、ソフトウェアでクリアすることはできません。このビットをクリアする唯一の方法は、リセットすることです。

セキュリティ保護可能なメモリ領域

- セキュリティ保護可能なメモリの内容は、PCROPページと重なっていても、RDPレベル1からレベル0に変更すると消去される

セキュリティ保護可能なメモリ･サイズ (SEC_SIZE[6:0])	セキュリティ保護可能なメモリ?	PCROP_RDP	消去されるページ
0	NO	1	すべて (全(マス)消去)
0		0	PCROP以外のすべて
>0	YES	1	すべて (全(マス)消去)
>0		0	PCROP以外すべての セキュリティ保護可能なメモリ領域

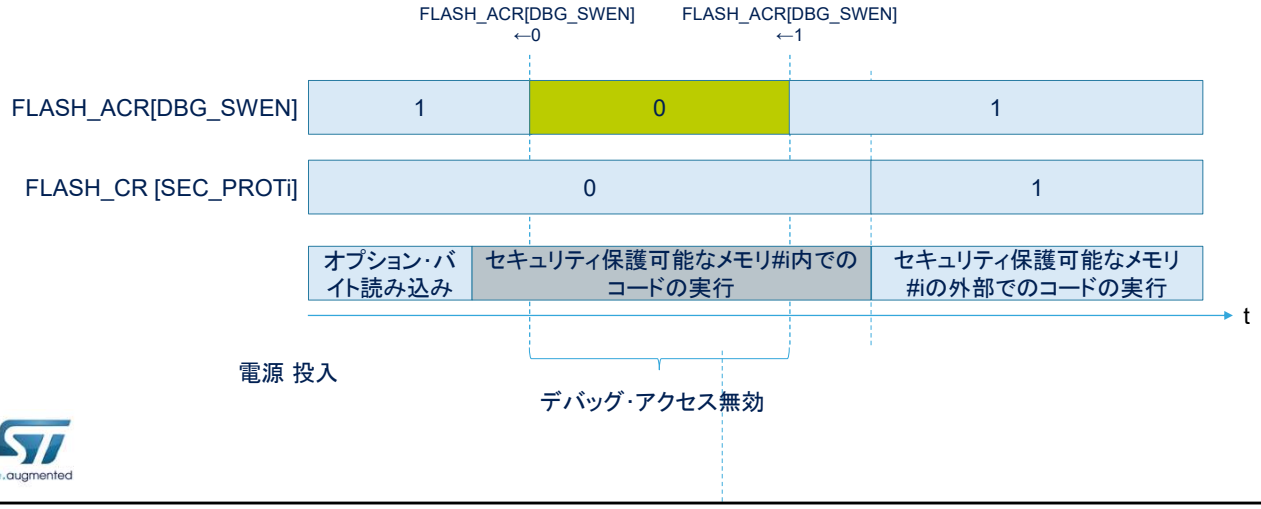
  - PCROP_RDPのレベルがレベル 1 からレベル 0 に回帰した場合に PCROP を保持するかどうかをビット制御
    =0: PCROP は消去されない
    =1: PCROP は消去される

life.augmented

もちろん、セキュリティ設定可能なメモリに存在するコードは、一部またはセキュリティ保護可能なメモリを消去する場合があります。
さらに、フラッシュ読出し保護レベルをレベル 1 からレベル 0 に変更すると、セキュリティ保護可能なメモリの消去がトリガされます。
セキュリティ保護可能領域に存在するコードは、独自仕様コード読出し保護(または PCROP) 領域にマッピングすることで、読出しおよび書込みアクセスから保護することもできます。
RDP レベルをレベル 1 からレベル 0 に回帰すると、PCROP_RDP ビットの値にかかわらず、これらの PCROP 領域が消去されます。セキュリティで保護可能なメモリ アドレス範囲の外側にある PCROP 領域の内容だけが保持されます。

コア·デバッグ·アクセスの無効化

- 機密コードの実行や、セキュリティ保護可能なメモリ領域での機密データの操作を行う場合、コアへのデバッグ·アクセスは一時的に無効にすることが可能



life.augmented

デバッガを使用しての Cortex-M4 を制御することは、DBG_SWEN制御ビットを適切にプログラミングすることによって一時的に無効にすることができます。
たとえば、セキュア ブートでは、認証/復号化を実行する前にこのビットをクリアし、認証が成功した後にこのビットを 1 つに設定して、デバッガによるデバッグを再度有効にできます。

Flashメモリからの強制ブート

- STM32G4ブート・メモリ:
  - 組み込み型SRAM
  - システム・メモリ (ブートローダ)
  - メインFlashメモリ
- セキュリティを強化し、信頼のチェーンを確立するために、FLASH_SECRレジスタのBOOT_LOCKオプション・ビットでは、他のブート・オプションに関係なく、システムがメインFlashメモリから強制的に起動することを許可する
  - BOOT_LOCKビットを設定することは常に可能
  - このビットをリセットする条件:
    - RDPはレベル0に設定されている。もしくは
    - RDPはレベル1に設定されており、レベル0が要求され、完全なマス消去が実行された時

life.augmented

STM32G4では、組み込みSRAMから起動、システムメモリから起動、メインフラッシュメモリから起動する3つの異なるブートモードを選択できます。
セキュア・メモリからセキュア・ブートを実行すると、ブート領域はフラッシュ・メモリーになります。他のブート領域を無効にするには、FLASH_SECRレジスタでBOOT_LOCKオプションビットを設定する必要があります。
このオプション ビットは常に設定できます。ただし、RDP レベルが 0 の場合、または RDP がレベル 1 からレベル 0 に回帰され、完全なマス消去が発生した場合にのみ、リセットが可能です。

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資料を参照してください。
  - STM32G4- Flashメモリ

メモリアーキテクチャ、オプションバイト、フラッシュメモリの操作の詳細については、フラッシュメモリのトレーニングを参照してください。