STM32G0 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、コードやデータを保護する各種手段について説明します。

概要

- 目的:
  1. 組込みのファームウェアとデータの読み書き保護を以下の領域に提供する
     - Flashメモリ
     - バックアップ·レジスタ
  2. 重要なファームウェアの安全な実行を実現する

アプリケーション側の利点

- STM32の組込みソフトウェアの知的財産を保護
- JTAGインタフェースまたはその他可能な外部攻撃手段を通じたコードのハッキングや読出しを防止
- 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)
- セキュア·アプリケーション(セキュアブートまたはセキュア·ファームウェア·アップデートなど)を開発可能

life.augmented

メモリ保護は、さまざまな目的で設計されています。
たとえば、読出し保護は、外部アクセスを通じた組込みソフトウェアコードの読出しを防止したり、開発者の知的財産を保護します。
書込み保護は、ソフトウェアやデータの更新手順で負荷オーバーフローによって特定の Flash セクタが偶発的に消去されることを防ぎます。

STM32G0 マイクロコントローラには、Flash 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複数の機能が搭載されています。
これらの代表的なメモリ保護に加え、STM32G0 はまた、重要なファームウェアの安全な実行を確保するための新しいメカニズムも導入しています。

後続のスライドでは、これらすべての保護機能について説明します。

主な機能

3

- **読出し保護(RDP)**
  - 外部アクセスに対してFlashメモリとバックアップ･レジスタをグローバルに保護
  - ブートがユーザFlashメモリ内からではない場合に、メモリとレジスタをSWDアクセスから保護
  - 保護なしから完全かつ永続的な保護までの、3つのRDPレベルを定義
- **商用コード読出し保護(PCROP)**
  - ソフトウェアIP読出し／書込みアクセスに対してFlashメモリ領域を保護
  - PCROP属性を備えた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	なし
書込み	なし
実行	**あり**

life.augmented

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。
RDP：読出し保護
PCROP：商用コード読出し保護
WRP：書込み保護機能
セキュアユーザメモリ保護は STM32G0 マイクロコントローラの新機能です。コードとデータの保護に加え、重要なアプリケーションの安全な実行を確実にします。

読出し保護(RDP)は、Flash メモリ、オプションバイト、バックアップレジスタに対する外部読出しアクセスを防ぐグローバルなメカニズムです。
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実行可能です。
RDP 保護の 3 つのレベルは、まったく保護を提供しないレベル 0 から完全かつ永続的な保護を備えたレベル 2 まで定義されています。
保護レベルについては、後続のスライドで説明します。

PCROP はコード読出しに対するメモリアクセス保護です。これは、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 3rd パーティコード(トロイの木馬)を実行している CPU によって行われる読出しおよび書込みアクセスは禁じられます。

主な機能

- **書込み保護（Write protection: WRP）**
  - 書込み／消去／プログラム･アクセスに対するFlashメモリ･セクタの保護
  - 書込み保護属性を持つFlashメモリ･コードは、不要な書込みや消去操作から保護される

リクエスト	アクセス許可
読出し	あり
書込み	**なし**
実行	あり

- **セキュア･ユーザ･メモリ保護**
  - 重要なファームウェアを実行するための、特定のアクセス･メカニズムによるFlashメモリ領域の保護
  - 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
  - コードはその他のプロセスの実行前に実行される

リクエスト	アクセス許可
セキュア読出し	あり
非セキュア読出し	なし
セキュア書込み	あり
非セキュア書込み	なし
セキュア実行	あり
非セキュア実行	なし

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。
セキュアユーザメモリは、特定の保護メカニズムを搭載したFlash メモリ領域で、コードとデータの保護に加えて、重要なファームウェアの安全な実行を確保します。
すべての保護メカニズムは STM32G0 オプションバイトを介して設定できます。

読出し保護

保護レベル0および1

- RDPレベル0
  - 保護は設定されておらず、すべての操作（読出し／書込み／消去）が Flashメモリ、SRAM、バックアップ･レジスタで許可されている。
  - オプション･バイトは変更可能。
- RDPレベル1
  - デバッグ･ポートが接続されている場合やRAMまたはシステムFlashメモリ･ブートローダからのブート中は、Flashメモリやバックアップ･レジスタへのアクセス（読出し、消去、プログラム）は一切実施できない。
    - 読出しまたは書込みリクエストの場合は、バスエラーが生成される。
  - ユーザFlashメモリからブートする場合は、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される。
  - オプション･バイトは変更可能で、レベル0への保護レベルの解除は可能であるが、これにより、Flashメモリとバックアップ･レジスタの全体が消去される。

life.augmented

最下位の RDP レベル（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。Flash メモリとバックアップレジスタに対するすべての読出しまたは書込み操作は（書込み保護が設定されていない場合）、すべてのブート設定（Flash ユーザブート、デバッグまたは RAM からのブート）で可能です。
オプションバイトはこのレベルでも変更可能です。
レベル 0 は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 Flash メモリとバックアップレジスタに対して設定されます。
このレベルでは、保護されたメモリは、ユーザ Flash メモリからブートされる場合にのみアクセス可能です。
デバッガアクセスが検出されるか、ブートがユーザ Flash メモリ領域に設定されていない場合には、保護されたメモリにアクセスすると、システムハードフォールトが生成され、次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。
オプションバイトはこのレベルでも変更できるため、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

レベル解除と保護レベル2

- レベル1からレベル0への保護レベルの解除
  - Flashメモリとバックアップ·レジスタの全体消去
    - 保護される領域（PCROPおよびセキュア·ユーザ·メモリ）は、その消去ポリシーに応じて変更されないままの場合がある
  - オプション·バイトとOTPバイトは消去されない
- RDPレベル 2
  - レベル1 によるすべての保護がアクティブで永続的
  - オプション·バイトが内部からも外部からも変更不能になる
  - SWDは無効
  - RAMやシステム·メモリ（ブートローダ）からのブートも許可されなくなる
  - ユーザFlash モリでのブートのみが許可され、Flashメモリとバックアップ·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

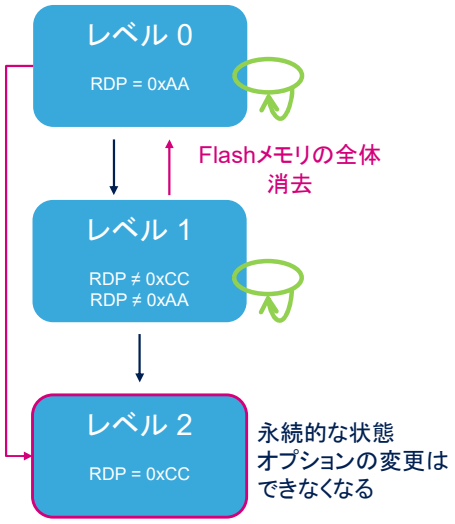
前のスライドでは、レベル 1 でオプションバイトを変更できることを確認しました。 その後、保護レベルをレベル 0 に変更することで、保護を解除することができます。
この保護レベルの解除により、Flash メモリとバックアップレジスタが全体消去されます。PCROP で保護されるか、セキュアユーザメモリとして設定されている Flash 領域は、その消去ポリシーの設定に応じて、消去または変更されないままにできます。

読出し保護レベル 2 はレベル 1 と同様の保護を提供しますが、その保護は永続的になります。オプションバイトは変更できないため、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、全体消去メカニズムによるレベル解除ができなくなります。このレベルは、開発ステージ完了時に最終製品でのみ考慮する必要があります。
バックドアが発生しないように、この保護は ST からの出荷時点でもバイパス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･バイトは変更可能
  - レベル1またはレベル2への遷移が可能
- レベル 1 / RDP ！=(0xAA|0xCC)
  - オプション･バイトは変更可能
  - ユーザFlashメモリ、バックアップ･レジスタ、SRAM2を全体消去し、レベル0へ遷移
  - 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･バイトは変更不能
  - 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ています。保護レベルを上げることは常に可能ですが、解除はレベル 1 とレベル 0 間でのみ可能です。その結果として、ユーザ Flash全体消去操作が生じます。
RDP レベルは 1 つのオプションバイトでコード化されます。レベル 0 は 0xAA 値でコード化され、レベル 2 は 0xCC 値でコード化され、レベル 1 は 0xAA または 0xCC 以外の値でコード化されます。

読出し保護

概要

領域	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	ユーザFlashメモリ以外でブートするとき、またはデバッグ·アクセスを検出したときのアクセス権
メインFlashメモリ	1	R/W/E	アクセスなし
	2	R/W/E	- (1)
システムFlashメモリ	1	R	R
	2	R	- (1)
オプション·バイト	1	読出し／書込み	読出し／書込み
	2	R	- (1)
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	- (1)
OTP	1	読出し／書込み	アクセスなし
	2	読出し／書込み	- (1)

(1):RDP2 では、ユーザ Flash メモリでのブートのみが許可される　　W:書込み　R:読出し　E:消去

life.augmented

この表は、前のスライドに見られるように、読出し保護（RDP）レベル、設定済みのブートモード、デバッグアクセス権に基づいて、Flash メモリとバックアップレジスタに対して許可されている各種アクセスをまとめたものです。

PCROP

9

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の保護
  - STや3rdパーティは、STM32マイクロコントローラに固有のソフトウェアIPを開発して販売これらのIPはさらなるアプリケーション開発に使用されるため、不正なコピーから保護される必要がある
  - PCROPの機能により、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）からの読出しに対してソフトウェアIPの保護が確保される
- PCROPの属性
  - PCROP領域は実行専用
    - 読出し／書込み／消去操作は許可されていない
    - PCROPコードは適切なオプション（armcc）「 –execute_only」を使用してコンパイルし、このメモリ属性に準拠するようにする必要がある。
  - RDPレベルに関係なく保護が有効

life.augmented

PCROP は商用コード読出し保護を意味します
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。ソフトウェアの知的財産（IP）を保護するために、コードをコピーしたり、読み出すことは禁じられています。PCROP の目的は、RDP レベルの設定に関係なく、3rd パーティソフトウェアの知的財産コードの機密性を悪意のあるユーザから保護することです。保護されているファームウェアは、Cortex®-M0+ コアによってのみ実行できます。その他すべてのアクセス（DMA、デバッグ、データ読出し、書込み、消去）は厳しく禁じられています。
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。例：「–execute_only」（Keil ツールの場合）。このオプションを指定しないと、定数は、リテラルプールと呼ばれる読出し専用セクションで関数によってインタリーブされます。
Cortex-M0+ MPU では、実行のみのアクセス許可はサポートしていません。

PCROP

10

設定／設定解除

- 設定
  - 2 つの PCROP 領域を定義可能
  - PCROP 領域は 512 バイト単位で定義され、512 バイトからフルバンクまで設定可能
  - 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
- リセット
  - PCROP を無効化する唯一の方法はレベル 1 からレベル 0 へのRDP レベルの解除
    - このレベル解除は Flash メモリの全体消去操作をトリガする
  - 追加のオプションビット（PCROP_RDP）で、RDP 保護がレベル 1 からレベル 0 に変更された場合、消去する PCROP 領域を選択できる

life.augmented

Flash メモリの商用コード読出し保護領域は、オプションバイトを通じて定義されます。

2 つの PCROP 領域を定義できます。各領域は 512 バイト単位で設定されており、512 バイトからフルバンクまで設定できます。
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、不要なセクタ書込み操作や消去操作に対する保護を提供します。

レベル 1 からレベル 0 への RDP レベル解除によってのみ PCROP 保護を解除できます。RDP 解除を実行すると、このメカニズムにより、Flash メモリの全体消去がトリガされます。
PCROP_RDP オプションビットに応じて、RDP 保護をレベル 1 からレベル 0 に変更すると、PCROP 領域が消去されます。

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

- 書込み保護属性
  - 保護されたセクタは消去またはプログラムできない
- 設定／リセット
  - 保護は Flash メモリのページごと(2 KB)に個別に設定される
  - 保護はオプションバイトレジスタで設定される
  - 書込み保護は RDP レベル 0 とレベル 1 でリセット可能
    - RDP レベル 2 では変更できない
  - 書込み保護されているセクタがある場合、RDP レベル解除メカニズムは機能しない
    - RDP レベル解除と Flash メモリの全体消去の前に書込み保護を解除する必要がある

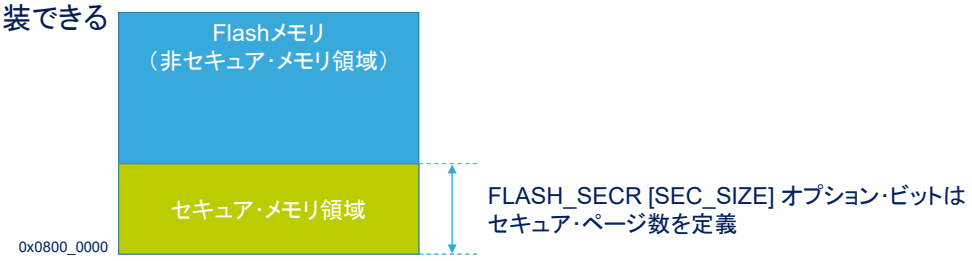
life.augmented

書込み保護は不要な消去や偶発的な消去からコードと不揮発データを保護します。
この保護は Flash メモリでのみ利用可能です。書込み保護は選択した Flash メモリセクタにのみ設定できます。
STM32G0 マイクロコントローラには、2 KB のセクタが 64 個あります。
セクタが保護されている場合、消去やプログラムはできません。
セクタへの書込みアクセスを試行すると、Flash メモリエラーが生じます。
少なくとも 1 つのセクタが書込み保護されている場合は、Flash メモリの全体消去は実行できません。この保護は最初に解除する必要があります。

セキュア·メモリ領域

概要

- セキュア·メモリ領域の主な目的は、望ましくないアクセスからFlashメモリの特定の領域を保護することである
  - これにより、セキュア·キー·ストレージやセーフブートなどのソフトウェアのセキュリティ·サービスを実装できる

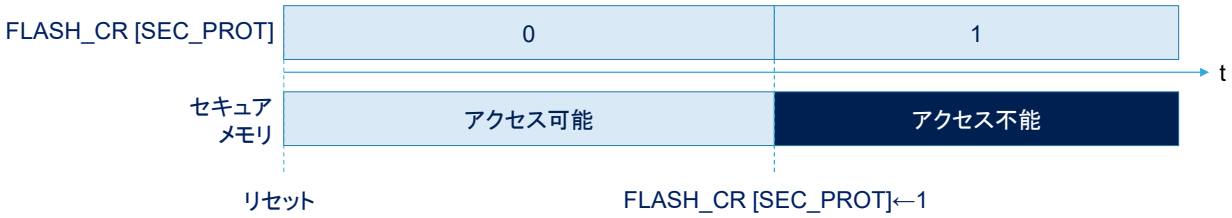


  - FLASH_SECR[SEC_SIZE] オプション·ビットが0の場合は、セキュア·メモリは実装されない
  - このフィールドはRDPレベル0でのみ変更可能

life.augmented

セキュアメモリの目的は、ブート時に使用できるコードとデータを格納することです。これらのコードとデータは、ブートプログラムが制御ビットをセットするとアクセスできなくなります。
通常の使用例では、セキュアメモリに含まれる暗号キーを使用して、Flash メモリに存在するソフトウェアイメージの認証と、可能な場合には復号化を実行します。認証プログラムと復号化プログラムもセキュアメモリに格納されます。
オプションビットはセキュアメモリのサイズをページ単位で設定するために使用します。ベースアドレスは常に 0x0800_0000 で、Cortex-M0+ リセットベクタに対応しています。
オプションバイトの SEC_SIZE フィールドがゼロの場合は、セキュアメモリは実装されません。
このフィールドは、RDP レベル 0 でのみ変更できます。

セキュア·メモリ領域



- デフォルトでは、リセット後に、セキュア·メモリにアクセス可能
  - SEC_PROTビットがFLASH_CRレジスタにセットされると、次のリセットまで、セキュア·メモリにアクセスできなくなる
  - リセットでのみSEC_PROTビットをクリア可能

ソフトウェアで FLASH_CR レジスタに SEC_PROT ビットをセットすると、セキュアメモリはアクセスできなくなります。
Flash メモリイメージの認証および復号化の実行に使用されるセキュアブートの場合、SEC_PROT ビットは、認証に成功したときに、イメージの最初の命令に分岐する直前に 1 にセットされます。
SEC_PROT ビットがセットされると、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。

セキュア·メモリ領域

- セキュア·メモリの内容は、PCROPページとオーバーラップしている場合でも、RDPをレベル1からレベル0に変更すると消去される

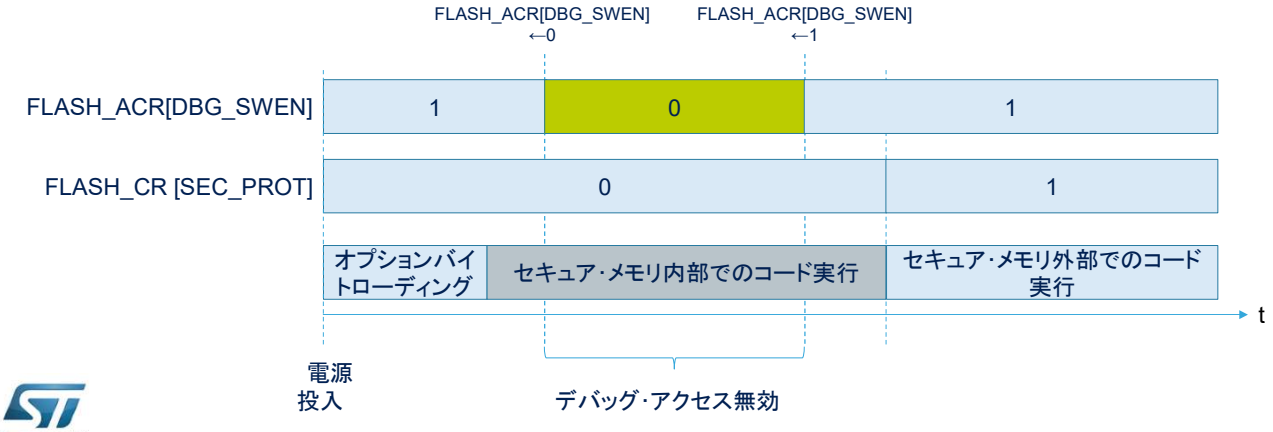
セキュアメモリサイズ（SEC_SIZE[6:0]）	セキュアメモリ？	PCROP_RDP	消去されるページ
0	いいえ	1	すべて（全体消去）
0		0	PCROPを除くすべて
>0	はい	1	すべて（全体消去）
>0		0	セキュア·メモリ領域外にあるPCROPを除くすべて

- PCROP_RDPビットはRDPレベルがレベル1からレベル0に下がった場合にPCROPを保持するかどうかを制御する。
  =0：PCROPは消去されない
  =1：PCROPは消去される

もちろん、セキュアメモリ領域にあるコードはセキュアメモリの一部を消去しようとする場合があります。
さらに、Flash 読出し保護（RDP）レベルをレベル 1 からレベル 0 に変更すると、セキュアメモリの消去がトリガされます。
セキュアメモリ領域にあるコードはまた、商用コード読出し保護（PCROP）領域にマッピングすることにより、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 に変更すると、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。セキュアメモリアドレス範囲外にある PCROP 領域のコンテンツのみが保持されます。

コア·デバッグ·アクセスの無効化

- コアへのデバッグ·アクセスは、セキュア·メモリ領域で機密コードを実行したり機密データを処理するために、一時的に無効化可能



life.augmented

侵入型デバッグを使用した Cortex-M0+ の制御は、DBG_SWEN 制御ビットを適切にプログラミングすることにより、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、その後、認証に成功したら、このビットを 1 にセットして侵入型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

16

- STM32G0ブート・メモリ:
  - 内蔵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、信頼のチェーンを構築するため、FLASH_SECR レジスタのBOOT_LOCKオプション・ビットでは、他のブート・オプションにかかわらず、システムをメインFlashメモリから強制ブートできる
  - また、BOOT_LOCKビットはいつでもセットできる
  - このビットをリセットするための条件:
    - RDPをレベル0にセットする、または
    - RDPレベル1がセットされている状態でレベル0に変更し、Flashメモリ全体消去を実行する

life.augmented

STM32G0 では、組込み SRAM からのブート、システムメモリからのブート、メイン Flash メモリからのブートという 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のセキュアブートの実行は、ブート領域が Flash メモリであることを意味します。他のブート領域を無効にするには、BOOT_LOCK オプションビットを FLASH_SECR レジスタでセットする必要があります。
このオプションビットは無条件にセットできます。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 に変更され、Flash メモリ全体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

17

- 次のペリフェラルに関連するトレーニングを参照:
  - STM32G0 - Flashメモリ

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