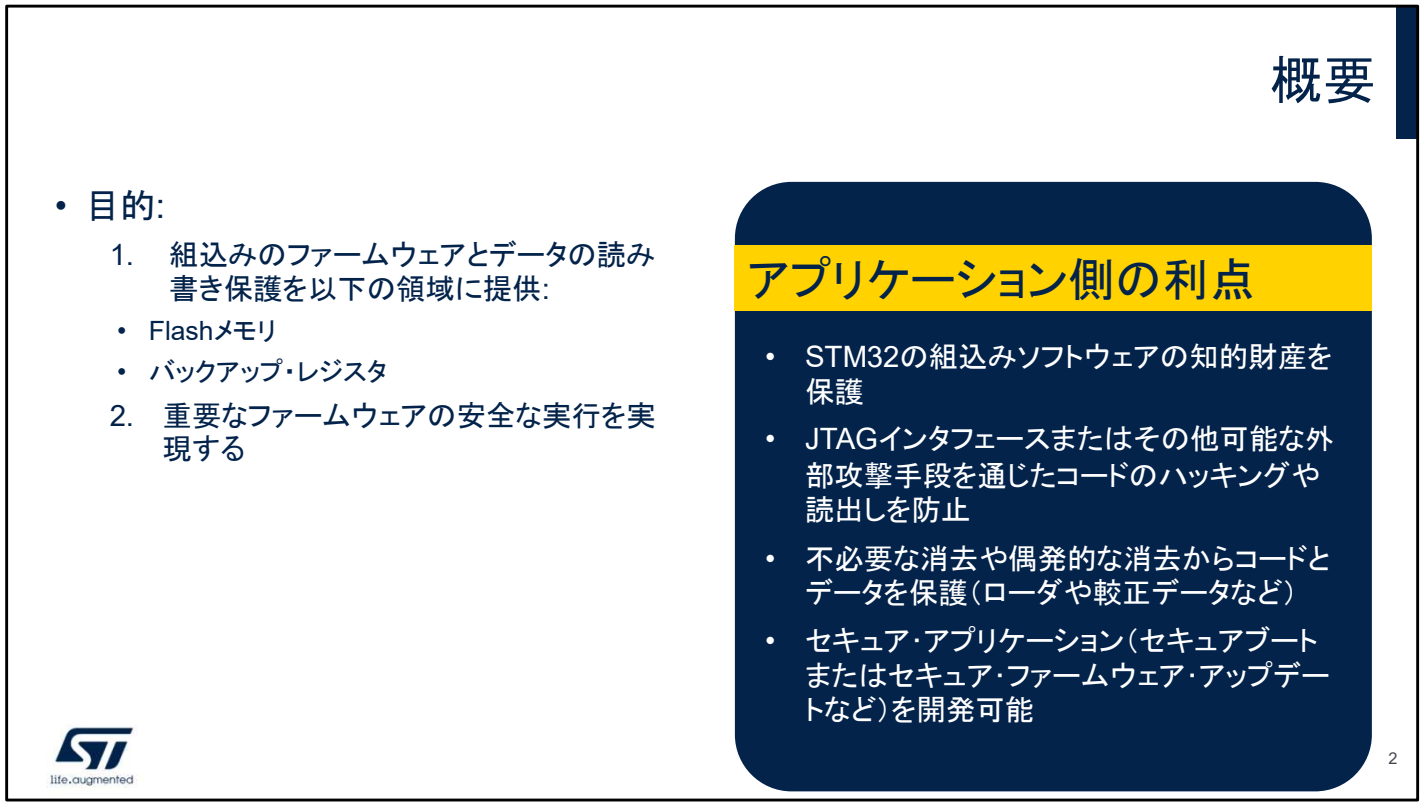
life.augmented

STM32C0-MEMPROTECT

システムメモリの保護

STM32C0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。



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。

STM32C0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、STM32C0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メカニズムも実装しています。

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

- **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

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。
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
安全なユーザーメモリ保護により、コードとデータの保護に加えて、機密アプリケーションの安全な実行が保証されます。

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（Writeprotection: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
- **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
読出し	あり
書込み	なし
実行	あり

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

4

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。
システムリセット後、保護可能なメモリ領域内のコードは、保護可能な領域が保護されるまでのみ実行でき、次のシステムリセットまでは実行できません。
これにより、安全なキーストレージやセーフ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できます。
すべての保護メカニズムはSTM32C0オプションバイトを介して設定できます。

主な機能

保護メカニズム	保護メモリ	粒度	リージョン数	リージョンサイズ
読出し保護	メインFlash オプションバイト SRAM	メインFlash全体	グローバル	グローバル
書込み保護	メインFlash	2KBページ	2	最初と最後のページで定義
独自仕様コード保護	メインFlash	512バイトサブページ	2	最初と最後のサブページで定義
セキュア保護可能なメモリ	メインFlash	2KBページ	1つ	ページ0から始まる0から15のページ数で定義

life.augmented

この表は、さまざまな保護メカニズムの機能をまとめたものです。

- 保護されるメモリの種類
- 保護の粒度
- 保護エリアの数
- 保護領域のサイズの定義

読出し保護

保護レベル0および1

- RDPレベル0（デフォルト）
  - 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

6

読出し保護は、RDPオプションバイトを設定し、システムリセットを適用して新しいRDPオプションバイトをリロードすることによってアクティブになります。
読出し保護には、保護なし（レベル0）から最大保護またはデバッグ不可（レベル2）までの3つのレベルがあります。
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メ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

7

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

8

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、メインFlash全体消去操作が生じます。
RDPオプションバイトは、補完バイトによって保護されます。
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	R
	2	R/W/E	-(1)
システムFlashメモリ（ブートローダ）	1	R	R
	2	R	-(1)
オプションバイト	1	R/W/E	R/W/E
	2	R	-(1)
バックアップレジスタ	1	R/W	アクセスなし
	2	R/W	-(1)
OTP	1	R/W	アクセスなし
	2	R/W	-(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　　R:読出し　W:書込み　E:消去

life.augmented

9

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

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b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

10

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

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

11

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機能で保護されたページも書込みアクセスから保護され、不要なページ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（2KB）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

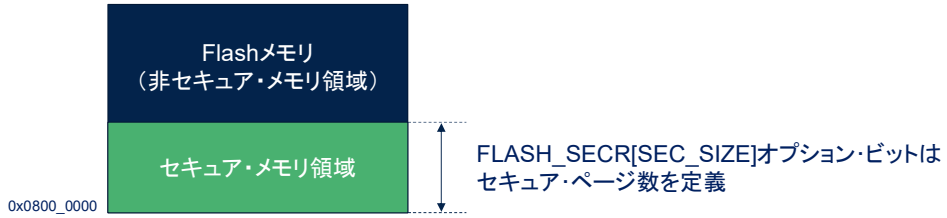
12

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。
この保護はメイン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。
STM32C0マイクロコントローラには、2KBのセクタが16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

13

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、セキュアメモリは無効になります。
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

life.augmented

14

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

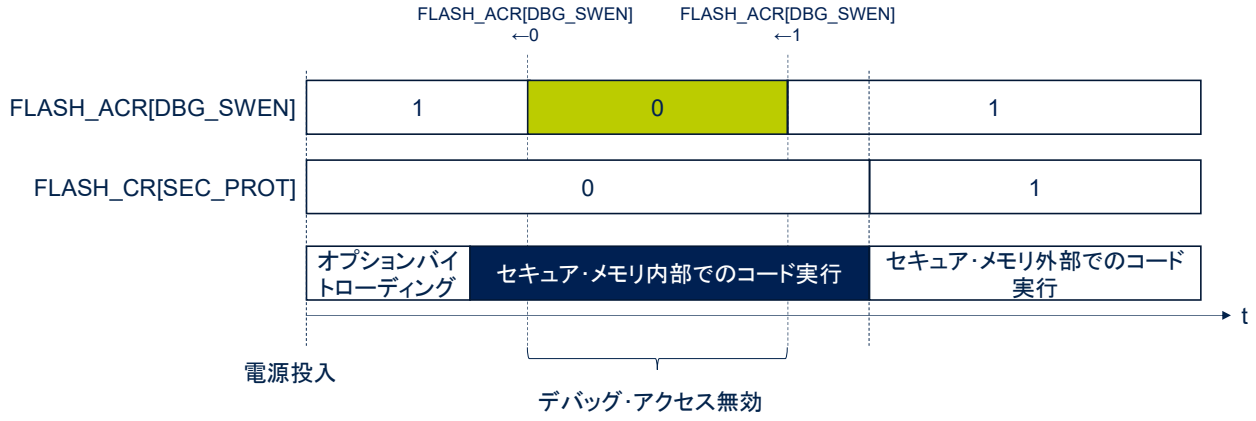
life.augmented

15

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

16

侵入型デバッグを使用したCortex-M0+の制御は、DBG_SWEN制御ビットを通じ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、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

- STM32C0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

STM32C0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。
いつでもBOOT_LOCKビットを設定できます。
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。

オプションバイト・ロード・フェイルセーフ

- このモジュールで提供されるすべてのメモリ保護は、オプションバイト（OB）に保存される
- OBのロード時に不一致が発生した場合
  - WRPオプションが一致しない場合、両方のWRPに「保護なし」が設定される
  - RDPオプションの場合、不一致の値はデフォルト値「レベル1」
  - PCROPの不一致がある場合、すべてのPCROPが「全メモリ保護」に設定される
  - BOOT_LOCKの場合、不一致の値は「メインFlashメモリから強制的に起動」
- これらの不一致値により、安全な構成が強制され、デバイスが永久にロックされる可能性がある
  - これを防ぐには安全な環境（安全な電源、保留中のウォッチドッグなし、クリーンなリセットライン）でのみオプションバイトをプログラム

life.augmented

オプションのバイトロード中、オプションはダブルワードで読み取られます。ワードとその補数が一致する場合、オプションワードがオプションレジスタにコピーされます。
ワードとその補数の比較が失敗すると、ステータスビットOPTVERRが設定されます。
不一致の値は、2番目の黒丸で示されているように、オプションレジスタに強制的に挿入されます。
オプションバイトのプログラミングが失敗すると（電源喪失やオプションバイト変更シーケンス中のリセットなどの何らかの理由で）、オプションバイトの不一致値がリセット後にロードされます。
これらの不一致値により安全な設定が強制され、デバイスが永久にロックされる可能性があります。
STM32C0は、オプションバイトの不一致の場合でもデバッグ機能が有効なままになるという新機能を実装しています。

関連ペリフェラル

- 次のペリフェラルに関連するトレーニングを参照:
  - STM32C0-Flashメモリ

life.augmented

19

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。

Our technology starts with You

Find out more at www.st.com

life.augmented

ありがとうございました。