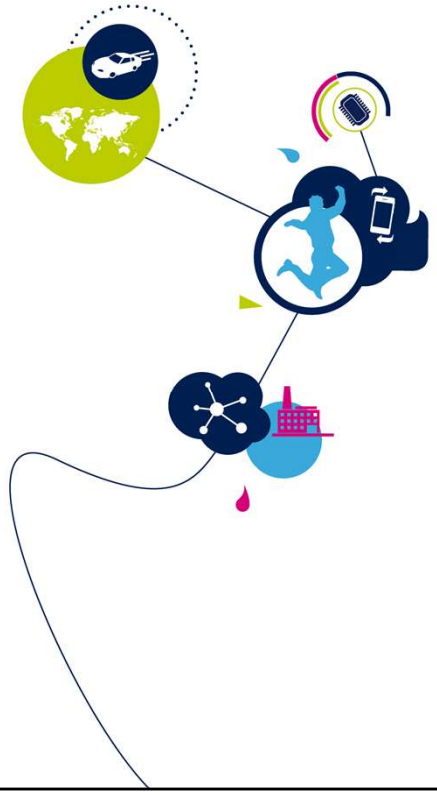
STM32H7 - MEMPROTECT

システム･メモリ保護

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
     - バックアップ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。
例えば、リードプロテクトは、外部からのアクセスによる組込みソフトウェアのコードの流出を防ぎ、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Flashセクタが誤って消去されることを防ぎます。
STM32H7マイクロコントローラは、Flashメモリ、バックアップSRAM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、STM32H7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、バックアップSRAM（4キロバイト）、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JTAG/SW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領域の保護
  - PCROP属性を持つFlashコードは実行のみ可能
- **書込み保護(WRP)**
  - Flash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
- **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

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機能は、STM32H7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することが可能です。
読み出し保護(RDP)は、Flashメモリ、4Kバイトのバックアップ SRAM、バックアップレジスタへの外部からのリードアクセスを防止するグローバルなメカニズムです。
外部アクセスとは、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。

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Flash領域です。
すべての保護メカニズムは、STM32H7オプションバイトを介して設定可能です。

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、バックアップ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、バックアップSRAM、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 読取りリクエストや書込みリクエストがあった場合、バスエラーが発生
  - 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、 バックアップ・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。Flash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(Flashユーザーブート、デバッグ、RAMからのブートなど)でバックアップ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Flashメモリ、バックアップ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、Flash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Flash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、バックアップ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
  - JTAG、SWV(シングルワイヤ·ビューワ)、ETM、バウンダリー·スキャンが無効(JTAGヒューズ)
  - 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、バックアップSRAM、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

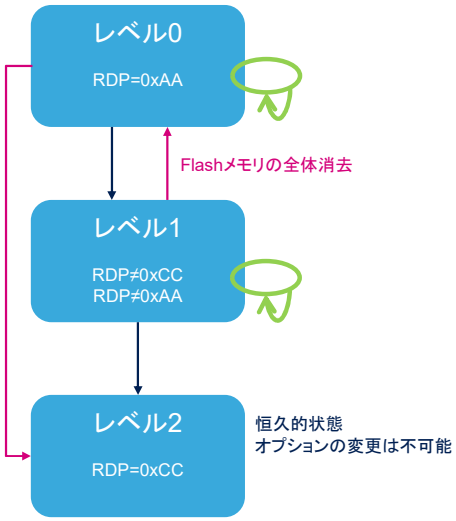
life.augmented

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、Flashメモリ、バックアップ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・メモリとして構成されたFlash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、バックアップ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



life.augmented

このスライドは、各読み出し保護レベル間で可能な遷移を示しています。保護レベルを上げることはいつでも可能ですが、レベル1とレベル0の間では、ユーザーFlashの完全消去という結果を伴う回帰しかできません。
RDPのレベルは1つのオプションバイトでコード化されており、レベル0は0xAA、レベル2は0xCC、レベル1は0xAAまたは0xCC以外の値でコード化されています。

読出し保護

サマリ

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	BootがユーザFlashメモリにないとき、または デバッグ･アクセスが検出され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Flasメモリ	1	R	R
	2	R	-(1)
オプション･バイト	1	R/W	R/W
	2	R	-(1)
バックアップSRAM& バックアップ･レジスタ	1	R/W	アクセスなし
	2	R/W	-(1)

(1):RDP2では、ユーザーFlashでの起動のみ可能

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(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、Flashメモリ、バックアップSRAM、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(1/2)

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
  - Cortex-M7コアのみがPCROPエリアからコードを実行することができ、Cortex-M4コアはPCROPエリアへのアクセス（読取り/書込み/実行）はできない
  - RDPレベルに関係なく保護が有効

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ためには、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。例えば、以下のようになります。"-execute_only"(Keilツール用)

PCROP(2/2)

設定/設定解除

- 設定
  - 各Flashバンクに1つのPCROPエリアを定義可能
  - PCROP領域は、8つのFlashワード（256バイト）の粒度で定義されており、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
- 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の全消去の操作をトリガ

life.augmented

Flash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。

バンクごとに1つのPCROPエリアを定義できます。各エリアは256バイトの粒度で設定され、512バイトからバンク全体まで設定できます。
これらの領域は、データバスを介したアクセスに対して保護されています。コード実行のために保護されたセクタにアクセスできるのは、Cortex-M7コアの命令バスだけです。
PCROP機能で保護されているセクタは、書込みアクセスに対しても保護されており、意図しないセクタの書込みや消去操作から保護されます。

PCROP保護の解除は、RDPのレベルをレベル1からレベル0に回帰させることでのみ実行可能です。このメカニズムが実行されると、Flashメモリの完全な大量消去が行われます。

Flashメモリの書込み保護

10

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
  - Flashメモリのセクタ(128Kバイト)ごとに独立した保護設定が可能
  - 保護はオプション・バイト・レジスタで設定
  - RDPレベル0およびレベル1では、ライトプロテクトのリセットが可能
    RDPレベル2では変更できない
  - 書込み保護されたセクタがある場合、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Flashメモリでのみ使用できます。書込み保護は、選択したFlashメモリセクタのみに設定できます。
STM32H7マイコンでは、1バンクあたり128Kバイトの8セクタが定義されています。
ページが保護されている場合、セクタ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、Flashメモリエラーが発生します。
少なくとも1つのセクタが書き込み禁止の場合、Flash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。

セキュア・ユーザ・メモリ

11

イントロダクション

- セキュアなアプリケーションの中には、強力なセキュリティ要件を持つものがある
  1. コードとデータ保護
     - 機密性またはアルゴリズムの知的財産
     - 秘密データまたは非公開データ(鍵)
  2. 安全な実行
     - アプリケーションの実行を保証:バイパスしない
     - 他のプロセスからのコードの中断や、中間の感覚的なデータへのアクセスを防ぐ
- セキュリティ保護されたアプリケーション例
  - 起動メモリの整合性チェック
  - 特定のペリフェラルから初期化ファームウェア
  - セキュリティ保護されたファームウェアの更新

life.augmented

STM32H7セキュア・ユーザ・メモリ

- セキュア・ファームウェア用の設定可能なFlashエリア保護
- コードとデータの保護
- 安全な実行
  - 実行のプリエンプションを保証
  - 他のプロセスからの分離実行

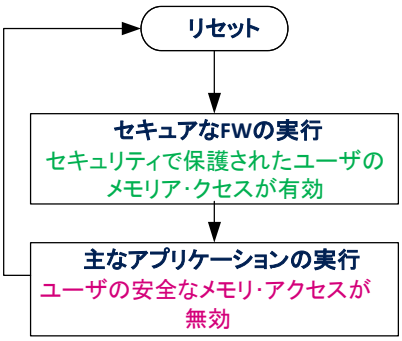
この機能は特定の部品番号でのみ使用可能

セキュアアプリケーションの中には、安全な実行だけでなく、データやコードの保護を必要とするものがあります。このようなセキュアなアプリケーションの例としては、セキュアなファームウェアのアップデートや、特定の起動手順を用いたユーザーセキュアブートなどがあります。これらのアプリケーションは、暗号鍵などの秘密データを操作する可能性があり、機密データにアクセスする可能性のある悪意のあるプロセスによってその実行が中断されてはなりません。STM32H7は、このようなアプリケーションの開発を可能にするセキュア・ユーザ・メモリ保護機能を導入しています。
セキュア・ユーザ・メモリは、Flashメモリの一部として設定可能です。この領域は、リセット後に一度だけアクセス可能で、他のプロセスよりも先に機密性の高いファームウェアを実行することができます。一度閉じた領域は、いかなる手段でもアクセスできないようになっています。

セキュア・ユーザ・メモリ

保護メカニズム

- セキュア・ユーザ・メモリへアクセス
  - 保護領域内のコードとデータは、システム・リセット後にのみアクセス可能
  - デバイスは、他のアプリケーションよりも先に実行されるセキュアなファームウェアで起動
    このファームウェアを実行できるのは、Cortex-M7コアのみ
  - 実行されると、セキュア・ファームウェアはセキュア・ユーザメモリへのアクセスを無効にし、メイン・アプリケーションにジャンプする
  - セキュア・ユーザ・メモリは、次のシステム・リセットが行われるまでアクセスできない
  - 読み取り、書き込み、実行のいずれのアクセスも禁止セキュア・ユーザ・メモリは、Cortex-M4コアやデバッグポートからは絶対にアクセスできない



life.augmented

セキュア・ユーザメモリへのアクセスは、システムリセット後に許可されます。セキュアファームウェアはこの領域に組み込まれており、ブートアドレスが正しく設定されていれば、メインのユーザーアプリケーションの前に実行されます。
保護された領域は、ファームウェアの実行中、オープンのままになります。完了すると、ファームウェアはこの領域を閉じ、メインアプリケーションにジャンプします。保護領域は次回のシステムリセットまで閉じられ、セキュアなファームウェアとそのデータにはアクセスできなくなります。
セキュアなユーザーメモリは、Cortex-M4コアやデバッグポートからは決してアクセスできません。

セキュア・ユーザーメモリ

STM32H7セキュア・アクセス・モード

- STM32H7の高度なセキュリティ機能は、特定のデバイス・コンフィギュレーション・モードで利用可能：セキュア・アクセス・モード
  - このモードでは、
    - STルート・セキュリティ・サービス(RSS): システムFlashに組み込まれたセキュリティ保護されたサービス
    - セキュア・ユーザ・メモリ設定
  - セキュア・アクセス・モードのセット / リセット
    - セキュア・アクセス・モードはオプション・バイト・レジスタによって制御
    - デバイスでセキュア・アクセス・モードをアクティブにする方法に制限はない
      システムがリセットされると、モードはアクティブになる
    - デバイスで使用可能な保護コードがなくなった場合にのみ、セキュア・アクセス・モードをリセット可能
      (セキュアユーザー領域とPCROP領域)
- セキュア・ユーザ・メモリの設定は、セキュア・アクセス・モードでのみ可能

life.augmented

セキュア・アクセス・モードは、特定の部品番号でのみ使用可能

STM32H7は、セキュア・アクセス・モードと呼ばれる特定のモードで利用できる高度なセキュア・サービスを提供します。このモードでは、別のモジュールおよびセキュア・ユーザーメモリ機能で詳しく説明されている、STルートセキュアサービス(RSS)にアクセスできます。これらのセキュアサービスは、システムFlashメモリに組み込まれています。

このモードは、オプションバイトによって設定されるデバイスコンフィギュレーションです。このモードは無制限に設定することができますが、Flashメモリに保護された領域がなくなっていない限り、設定を解除することはできません。この場合、デバイスのセキュアアクセスモードをリセットする前に、Flashのマス消去が必要になります。

セキュア・ユーザ・メモリ

セット / リセット

- セキュア・ユーザ・メモリの設定は、セキュア・アクセス・モードでのみ可能
- セット
  - 各バンクに1つのセキュア・ユーザ・メモリを設定可能（サイズ変更可能）
  - 各エリアのサイズは512バイトからフルバンクまで256バイトの粒度で設定可能
  - 初期化のためにルート・セキュア・サービスが呼び出される:RSS_resetAndInitializeSecureAreas
- リセット
  - セキュア・ユーザ・エリアを消去するには、Flashマスイレーズまたはバンク消去を行う必要がある
    - Flashマスイレーズは、RDPレベル1からRDPレベル0へのレベル回帰がトリガーとなる
    - バンク消去は、Flashコントロール・レジスタによってトリガされる

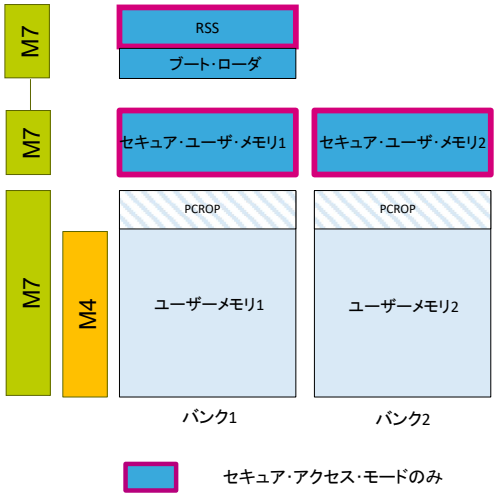
life.augmented

セキュア・アクセス・モードに入ると、セキュア・ユーザーメモリの設定が可能になります。
セキュア・ユーザーメモリは、Flashバンクごとに1つ設定できます。領域は512バイトから全バンクまで、256バイト単位で設定できます。保護の初期化には、専用のルートセキュアサービスを呼び出す必要があります。
セキュア・ユーザーメモリは，Flashマスイレーズまたはバンクイレーズによってリセットすることができます。Flashマスイレーズは，RDP1からRDP0へのRDPレベル回帰がトリガーとなります。

Flash保護

概要

アクセスタイプ	コア	Protected Area/SW	セキュリティモード	アクセス
実行	CM7	PCROP	任意	はい
		セキュアユーザソフトウェア	セキュアアクセス	はい (*)
		ルートセキュアサービス	セキュアアクセス	はい (*)
	CM4	PCROP	任意	いいえ
		セキュアユーザソフトウェア	セキュアアクセス	いいえ
		ルートセキュアサービス	セキュアアクセス	いいえ
読出しアクセス	CM7	PCROP	任意	いいえ
		セキュアユーザソフトウェア	セキュアアクセス	はい (*)
		ルートセキュアサービス	セキュアアクセス	はい (*)
	CM4	PCROP	任意	いいえ
		セキュアユーザソフトウェア	セキュアアクセス	いいえ
		ルートセキュアサービス	任意	いいえ
デバッグアクセス	CM7	PCROP	任意	いいえ
		セキュアユーザソフトウェア	セキュアアクセス	いいえ
		ルートセキュアサービス	セキュアアクセス	いいえ
	CM4	保護された領域	任意	いいえ



life.augmented

(*): リセット後、コードが完了するまでの間のみ付与されるアクセス権

このスライドでは、Flashメモリの保護機能の違いについてまとめています。
保護された領域は、Cortex-M7コアが特定の動作に従ってアクセスすることしかできません。
ルートセキュリティサービスとセキュアユーザーメモリは、セキュアアクセスモードでのみアクセス可能です。
Cortex-M4コアおよびデバッグポートは、保護された領域へのアクセスが禁止されています。

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ご参照ください。
  - STM32H7- Flashメモリ
  - STM32H7- ルートソース·サービス

life.augmented

メモリアーキテクチャ、オプションバイト、Flash操作については、
Flashメモリトレーニングをご参照ください。