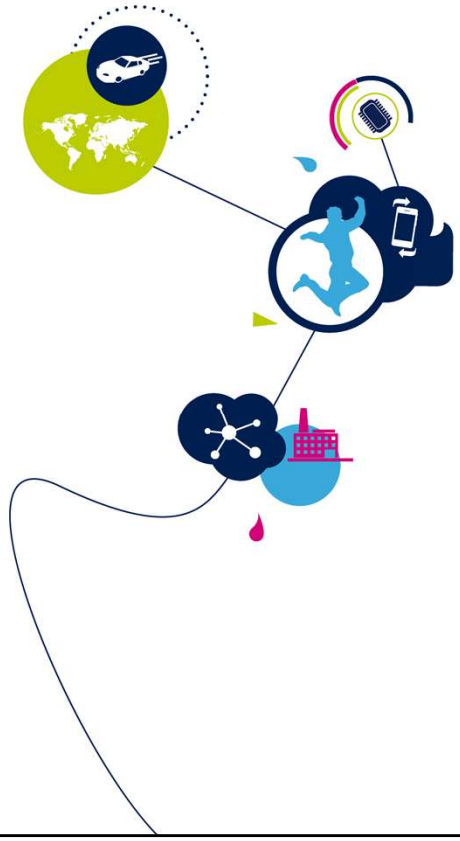
STM32G4 – Flash

内蔵Flashメモリ

0.1版



こんにちは、STM32G4マイクロコントローラファミリや、すべての製品に含まれている組み込みフラッシュメモリのプレゼンテーションへようこそ。

概要

- STM32G4は、デュアルバンク·アーキテクチャを備えた最大512KBのFlashメモリを内蔵
- Flashメモリ·インタフェースは、すべてのアクセス(読出し、プログラミング、削除)、メモリ保護、セキュリティ、およびオプション·バイト·プログラミングを管理

アプリケーション側の利点

- 高性能で低消費電力
- 書込み中読出し機能
- 小さな消去粒度
- 短いプログラミング時間
- デュアルバンク·ブート
- セキュリティと保護

life.augmented

STM32G4マイクロコントローラは、デュアルバンクアーキテクチャを備えた最大512キロバイトのフラッシュメモリを内蔵しています。
フラッシュメモリインタフェイスは、すべてのメモリアクセス(読出し、プログラミング、および削除)だけでなく、メモリ保護、セキュリティ、オプションバイトを管理します。
このフラッシュ メモリ インタフェイスを使用するアプリケーションは、低電力アクセスと共にその高パフォーマンスという利点を活用できます。それは書込み中での読出(RWW)サポート、消去の単位が小さく、プログラミング時間も短く、デュアルバンクブートを可能にします。
コードとデータ、読出しや書込みアクセスに対して、さまざまなセキュリティと保護メカニズムを備えています。

STM32G43X/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)
サイズ	128 KB	512 KB	
バンク数	1	1	2
データ幅	64 ビット	128 ビット	64 ビット
ページ サイズ	2キロバイト	4キロバイト	2キロバイト
フラッシュ構成	64ページ	128ページ	128ページ
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領域 (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のフラッシュメモリの実装に関する相違点をハイライトしています。
フラッシュ メモリのサイズは、カテゴリ 2 の場合は 128 KB、カテゴリ 3 の場合は 512 K バイトです。
DBANK オプション・ビットに応じて、カテゴリー 2 のバンクの数は 1、カテゴリー 3 の場合は 1、または 2 です。書込み中読出し機能 (RWW) は、デュアルバンク アーキテクチャがアクティブな場合にのみサポートされます。これにより、一方のバンクをプログラミングまたは削除し、もう一方のバンクからのコードを実行できます。
最小の消去の単位を提供するページ サイズは、カテゴリ 2 では 2 KB、カテゴリ 3 はシングル バンクの場合は 4 KB、デュアル バンクの場合は 2 KB です。
ページ数はカテゴリ 2 の場合は 64 ページ、カテゴリ 3 の場合は 128 ページです。
保護機能に関しては、カテゴリ2のマイクロコントローラは2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4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があります。

主な機能

- ページ消去、バンク消去、マス消去
- 高速消去(22ms)と高速プログラミング時間(ダブルワードで82µs)
- 2つのプログラミング モード:
  - 標準(メインメモリおよびOTP用)
  - 高速 (メインメモリのみ)
    - フラッシュのベリファイ確認無しでプログラム 64 ダブルワード
- エラーコード訂正 (ECC): 64bitダブルワードで8bit
  - シングルビット·エラーの検出と訂正、マスク可能な割込みによる通知
  - ダブルビット·エラーの検出と通知、NMIによる通知

フラッシュ メモリは、ページ消去、バンク消去、およびマス消去をサポートします。
ページ、バンク、またはマス消去の操作は22msしか必要とされず、ダブルワードの場合、プログラミング時間は82 µsです。
高速プログラミングモードは、64個のダブルワードを連続して書き込み、ページプログラミング時間を短縮して、各ダブルワードアクセスのフラッシュのベリファイを確認する必要をなくし、さらに、ダブルワード書き込みごとに高電圧の立ち上がり時間と立ち下がり時間を回避します。
プログラムするダブルワードに 8 ビット ECC コードが追加されます。読み取り時にチェックされ、シングルビットエラーを検出して修正し、ダブルビットエラーを検出します。
修正できないエラーが発生した場合、フラッシュ メモリ コントローラは、マスク不可割り込み (NMI) を Cortex®-M4 に通知します。

主な機能

- ART Accelerator™ (命令キャッシュ、データ･キャッシュ、プリフェッチ･バッファ)は周波数に対して線形の性能を実現
- 保護:
  - 書込み保護領域
  - 独自仕様コード読出し保護領域
  - WPR領域, 2つのPCROP領域, 2セキュリティ保護可能なメモリ領域
  - デュアルバンク･モード: バンクごとに2 WPR 領域、バンクごとに1つの PCROP 領域、バンクごとに1つのセキュリティ保護可能なメモリ領域

適応型 リアルタイム メモリ アクセラレータ(ART Accelerator)は、命令キャッシュ、データ キャッシュ、プリフェッチ バッファを備えており、周波数に対して線形のパフォーマンスを実現します。
また、Vcore パワードメインに属する電力消費の低減にも貢献します。
以下の保護メカニズムがサポートされています。

- 不要な書き込み操作から保護するために使用される書き込み保護領域。
- 独自仕様コード読出し保護領域(またはPCROP):フラッシュメモリの一部を第三者からのアクセスから保護することができます。
- 保護領域は実行専用であり、命令コード域として STM32 CPU のみ読み取り可能ですが、他のすべてのアクセス (DMA、デバッグ、および CPU データとしての読み取り、書き込み、消去) は厳しく禁止されています。
- セキュリティ保護可能なメモリ領域は、新しいリセットが発生しない限り、ブート時に 1度だけ実行できるコード領域を定義します。

Flashメモリの構成(1/2)

Flashメモリは次のように構成されている:

- 64 ページまたは128 ページを含むメインメモリ·ブロック
  - シングルバンクを持つ Cat 3デバイスの場合、ページサイズは4KB
    - 各ページは、512バイトの8行で構成される
  - Cat2デバイスとデュアルバンクを備えたCat 3マイクロコントローラの場合、ページ·サイズは2KB
    - 各ページは、256バイトの8行で構成される
- 情報ブロックは次を含む:
  - ST ブートローダ用に予約済みのシステムメモリ
  - ユーザ·データに使用する1KB(128ダブルワード)の OTP(ワンタイム·プログラマブル)領域
    - OTP 領域のデータは消去不能、ダブルワードを1回だけ書き込める
  - ユーザ設定のオプション·バイト

life.augmented

メインメモリは、マイクロコントローラのカテゴリに応じて64または128ページが含まれます。
シングルバンク アーキテクチャを持つカテゴリ 3 の場合、ページ サイズは 4 KB、各ページは 512 バイトの 8 行で構成されます。
デュアルバンク アーキテクチャを持つカテゴリ 3 とカテゴリ 2 の場合、ページ サイズは 2 KB で、各ページは 256 バイトの 8 行で構成されます。
メイン フラッシュ メモリに加えて、STM32G4 は:

- ST ブートローダを含む 28 K バイトのシステム メモリ
- 消去または変更してはならないユーザー データを格納するために使用できる 1 K バイトの OTP メモリ。ダブルワードの1つのビットを"0"に設定すると、ダ ブルワード全体はオールゼロ以外の値を書き込めなくなります。
- システムオンチップ内のIPを設定するためのデフォルト設定を含むオプションバイト。これらは、電源投入リセット後に自動的にロードされます。

Flashメモリの構成(2/2)

Flash領域		Flashメモリ·アドレス (Cat 3、デュアルバンク)	サイズ	名前
メイン メモリ	バンク 1	0x0800_0000 – 0x0800_07FF	2 KB	ページ0
		…	…	…
		0x0803_F800 – 0x0803_FFFF	2 KB	ページ127
	バンク 2	0x0804_0000 – 0x0804_07FF	2 KB	ページ0
		…	…	…
		0x0807_F800 – 0x0807_FFFF	2 KB	ページ127
インフォメーション ブロック		0x1FFF 0000 – 0x1FFF_6FFF	28 KB	システム メモリ
		0x1FFF 7000 – 0x1FFF_73FF	1 KB	OTP エリア
		0x1FFF 7800 – 0x1FFF_787F	48 B	オプション バイト

オペレーション	粒度
プログラミング	8バイト
高速プログラミング	512バイト行
消去	マス、バンク、ページ
セキュリティ保護可能なメモリ	ページ
書込み保護	
読込み保護	グローバル
独自仕様コード読出し保護領域	クワッドワード(Cat 3 シングルバンク) もしくは、ダブルワードアライメント

life.augmented

左の表は、メインフラッシュメモリの領域のデュアルバンクアーキテクチャを持つカテゴリ3マイクロコントローラと、インフォメーションブロックに基づくメモリ構成を詳述しています。右の表は、フラッシュ メモリへのオペレーションを詳しく示しています。

- プログラミングは8バイトのダブルワードで行われる
- 高速プログラミングは512バイトの行で行われます
- 消去は、グローバルに (大量消去) するか、バンクまたはページの単位で行われます。
- セキュリティ保護可能なメモリはページ上に配置されます。
- 書込み保護はページごとに行われます
- 読取り保護はグローバル単位です
- 独自仕様コード読出し保護領域は、クアッドワードまたはダブルワードのいずれかの整列されたプログラム可能な開始アドレスと終了アドレスに基づいています。

Flashデュアルバンク

書込み中の読出し、およびデュアルバンクブート機能

- ユーザ·オプションのバイト·オプション DBANK は、デュアルバンク·モードを選択
- デュアルバンク・ブート機能を備えたデュアルバンクFlashメモリ
  - ユーザ·オプション·バイトのオプション BFB2
    - BFB2 = 1,有効なバンクに応じて、バンク2またはバンク1からデバイスが起動
    - BFB2 = 0,バンク1のみでのデバイスが起動
- 書込み中の読出し
  - デュアルバンク機能により、一方のバンクから読み取り、もう一方のバンクをプログラミング/消去することが可能
    - Flashメモリがプログラムが書かれているときにコード実行が停止されない
  - 同じバンクでデータをプログラミング/消去する場合: AHBは、プログラム/消去操作が進行中で停止

life.augmented

DUALBANK (DBANK) オプションは、カテゴリー 3 デバイスに対してシングル・バンクまたはデュアル・バンクのいずれかを選択するために使用されます。
フラッシュ メモリは、2 つのバンクをサポートするように設定でき、書込み中の読出し機能とデュアル バンク ブート機能を備えており、バンク 1 またはバンク 2 から起動できます。

ユーザ オプションバイトの BFB2 オプションは、デュアルバンク ブート モードを選択するために使用されます。BFB2 オプションが設定されている場合、デバイスは有効なバンクに応じてバンク 2 またはバンク 1 から起動します。BFB2 オプションをオフにすると、デバイスは常にバンク 1 から起動します。

Flash読出しアクセス

170MHz で 213DMIPS

- 適応型 リアルタイム·アクセラレータ (ART Accelerator™) は、Flashメモリのアクセス時間に関係なく、周波数に対して線形パフォーマンスを実現

ウェイト状態(WS) (フラッシュ 遅延)	HCLK (MHz)		
	V_{CORE} レンジ 1 ブースト·モード	V_{CORE} レンジ 1 ノーマル·モード	V_{CORE} レンジ 2
0 WS	≤ 34	≤ 30	≤ 8
1 WS	≤ 68	≤ 60	≤ 16
2 WS	≤ 102	≤ 90	≤ 26
3 WS	≤ 136	≤ 120	-
4 WS	≤ 170	≤ 150	-

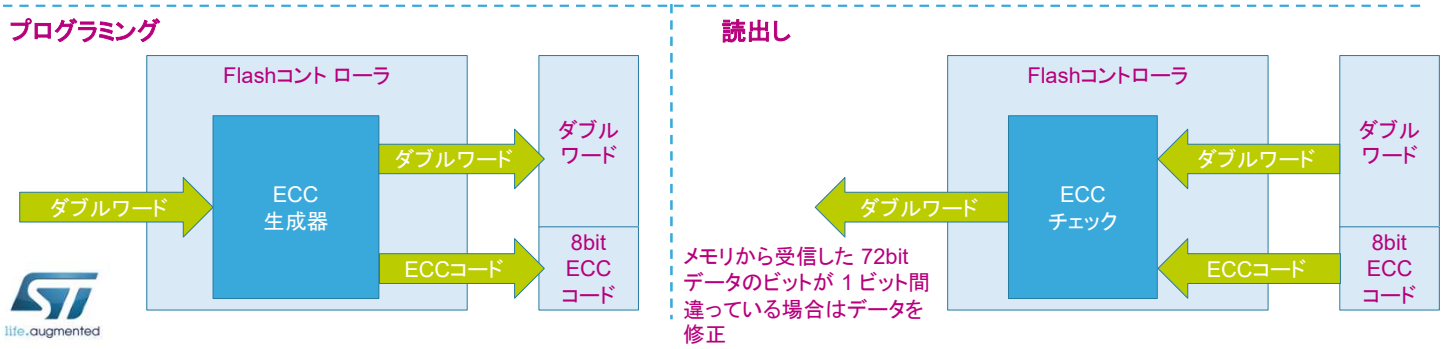
life.augmented

フラッシュ メモリを読み取るためには、クロック周波数に応じて、読出しアクセスに挿入されるウェイト状態の数を設定する必要があります。待機状態の数も電圧スケーリング範囲によって異なります。レンジ 1 では、フラッシュ メモリは 4 つのウェイト状態で最大 170 MHz にアクセスできます。0 のウェイト状態で 34 MHz までアクセスできます。レンジ 2 の場合、26 MHz まで、ウェイト状態が 2 です。適応型リアルタイムアクセラレータ、ARTアクセラレータにより、プログラムはクロック周波数に依存しない0待ち状態で実行することができます。これは周波数170 MHzに対して、213 Dhrystone MIPSのベンチマークの結果に関連してほぼ線形性能を提供します。

Flashメモリの機能(1/2)

堅牢なメモリの完全性と安全性

- **ECC** (エラー コード訂正): 64bitワードの場合、8bitの長さ
  - シングルビット·エラー訂正: FLASH_ECCRで設定された ECCC ビット、オプションの割込み生成
  - ダブルビット·エラー検出: ECCD ビットセット FLASH_ECCR => NMI
  - **FLASH_ECCRレジスタにエラー·アドレスが保存**



フラッシュ メモリ ワード データは 72 ビット幅で、各ダブル ワード (64 ビット) ごとに 8 ビットが追加されます。ECC メカニズムは以下をサポートします

- 1ビットのエラー検出と修正
- 2ビットのエラー検出

1 ビットのエラーが検出されて修正されると、ECCC フラグ (ECC 訂正) がフラッシュ ECC レジスタにセットされます (FLASH_ECCR)。また割込みを生成できます。
2 ビットのエラーが検出されると、Flash ECC レジスタ (FLASH_ECCR) に ECCD フラグ (ECC 訂正) がセットされます。この場合、NMI が生成されます。

Flashメモリの機能(2/2)

堅牢なメモリの完全性と安全性

- プログラミングの単位は64bit(実際は8bit ECCを含む72bit)
  - シングルバンクの Cat 3デバイスの場合は 144bit (72bit x2)
- 2 つのプログラミング・モード:
  - 標準(メインメモリおよびOTP用)
  - 高速 (メインメモリのみ)
    - Flashメモリのベリファイを確認せずに64ダブルワードでプログラム

life.augmented

高速プログラミングにより、256 バイトの行をプログラミングが出来ます。通常のプログラミングは 8 バイト単位となります。

高速プログラミングの主な目的は、ページ単位のプログラミング時間を短縮することです。高速モードでは、アドレス位置の内容はプログラミング前に チェックされません。ダブルワードごとの電圧の上げ下げを節約できます。

プログラミング/消去時間

短いプログラミングと消去時間&小さいページサイズ
→データ EEPROM エミュレーションの利点

パラメータ	標準値
64bitプログラミング時間	82µs
1 行 (256B) のプログラミング時間	標準モード: 2.61ms 高速モード: 1.91ms
1 ページ (2KB) のプログラミング時間	標準モード: 20.91ms 高速モード: 15.29ms
バンク・プログラミング時間	標準モード: 2.68s 高速モード:1.96s
ページ (2 KB) の消去時間	22.02ms
マス消去時間	22.13ms

- プログラム操作と消去操作は、電圧スケーリングのレンジ1でのみ可能

高速プログラミングは、標準モードプログラミングより3分の1高速です。
512K バイトの消去操作のマス消去時間は、ページ消去とほぼ同じ時間を要します。

行 (64ダブルワード) 高速プログラミング

- 高速プログラミングでプログラムできるのは**メインメモリ**のみ
  - OTP バイトもオプション・バイトも不可
- プログラミング前に、ハードウェアによる Flashロケーションの検証はしない
- 64のダブルワードは連続して書く必要がある
  - すべてのプログラミングのため、Flashメモリには高電圧が維持される
  - 連続した2つのダブルワード書込みリクエスト間の**最長時間**は、プログラミング時間（50µs前後）で規定される=> ただし、割込みは無効にする
- Flash クロック周波数（HCLKS）は少なくとも8MHzとする必要がある

life.augmented

高速プログラミングと標準プログラミングでは

- メインフラッシュメモリのどこにでも位置する8バイトのダブルワードの代わりに512バイトがプログラムされる
- 8 バイトのプログラミングは、検証手順により信頼性が高い

2つの連続したダブルワードの間の最大時間は約50 µsであることに注意してください。この遅延の後に 2 番目のダブルワードが到着すると、高速プログラミングは中止され、エラーフラグがセットされます。したがって、この遅延を超えないように、割込みを無効にする必要があります。

プログラミング·モード：標準vs高速

	プログラミング·モード	
	標準	高速
対象	メインメモリ+ OTPエリア	メインメモリのみ
粒度	8バイト	256バイト
固有の制限	なし	アドレス位置のチェックなし フラッシュクロック周波数 ≥ 8 MHz 割込み禁止
256バイトのプログラムに要する時間	2.61 ms	1.91 ms

このスライドは、標準プログラミングモードと高速プログラミング モードの比較を示しています。

Flashメモリ保持

- デザイン上の期待値

耐久性	40℃～+105° Cで最低10000回書き換え
データ保持	55° Cで10000回書き換え後30年85° Cで10000回書き換え後15年105° Cで10000回書き換え後10年 85° Cで1000回書き換え後30年105° Cで1000 回書き換え後15年125° Cで1000回書き換え後 7年

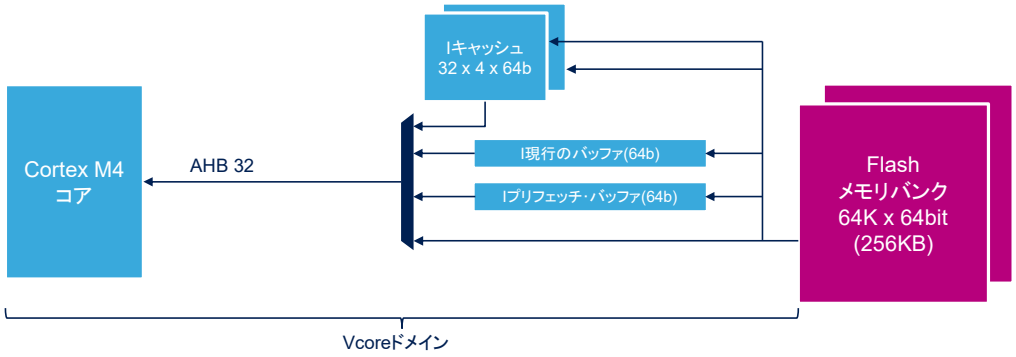
それぞれプログラム/消去の操作は、フラッシュメモリセルを劣化させます。
プログラム/消去サイクルを何度も行うとメモリセルは、メモリエラーを引き起こし、機能しなくなる可能性があります。
耐久性とは、フラッシュメモリが信頼性に影響を与えることなくサポートできる消去/プログラミングシーケンスの最大数です。

データ保持は、指定された期間、特定のデータ パターンを保持すると定義されます。
保持は、プログラム/消去サイクルの数と温度によって異なります。

適応型リアルタイム･メモリア･クセラレータ (ART Accelerator™)

優れたパフォーマンスと低消費電力

- **命令キャッシュ:** 32ラインの4x64bit（1Kバイト）、命令用
- **データ･キャッシュ:** 8ラインの4x64bit（256バイト）、リテラルプール用
- **プリフェッチ･バッファ:** 64ビット1ライン
- 最高のトレードオフ　キャッシュ･サイズ、パワー、パフォーマンス



life.augmented

ART アクセラレータは、優れた性能を発揮し、動的消費電力を低減します。
1 K バイトの命令キャッシュ、256 バイトのデータ キャッシュ、およびプリフェッチ バッファで構成されます。
命令キャッシュには 32 ラインの 4 つのダブルワードが含まれ、データ･キャッシュには 8 ラインの 4 つのダブルワードがあります。
命令キャッシュ･メモリ･ラインがすべて満杯になると、LRU (最も使用されにくい) ポリシーを使用して、命令メモリ･キャッシュ内で置き換えるラインを判別します。
この機能は、ループを含むコードの場合に特に有益です。
このアーキテクチャは、キャッシュ サイズ、消費電力、パフォーマンスの間で最良のトレードオフを実現するために選択したものです。
キャッシュミスが発生する度に、キャッシュは要求されたダブルワードによってのみ更新されます。そうすることで、フラッシュへのアクセスを制限し消費電力を抑えることができます。ライン内の4ダブルワード は全て有効であるとは限りません。
キャッシュミスの場合、Cortex M4コードはフラッシュメモリから直接命令を取得します。
並行して、64bit のラインが有効化された現行バッファと有効化されていれば命令キャッシュにコピーされます。従って、次のシーケンシャルアクセスは現行バッファから直接行なわれます。
プリフェッチが有効な場合、さらに64bit のフラッシュメモリアクセスが行なわれ、プリフェッチバッファはシーケンシャルデータで満たされます。
データが現行バッファにある場合、CPUは現行バッファを読み出します。
その次のシーケンシャル読出 しはプリフェッチバッファにて行なわれ、同時に現行バッファにコピーされるため、次のシーケンシャル データを格納するためのスペースが確保できます。
データが現行バッファになく、プリフェッチバッファにあればそこから読み出されます。
プリフェッチバッファになければ、キャッシュヒットしている場合、命令キャッシュから読み出されます。
そうでない場合、フラッシュアクセスが行なわれます。

ARTの基本

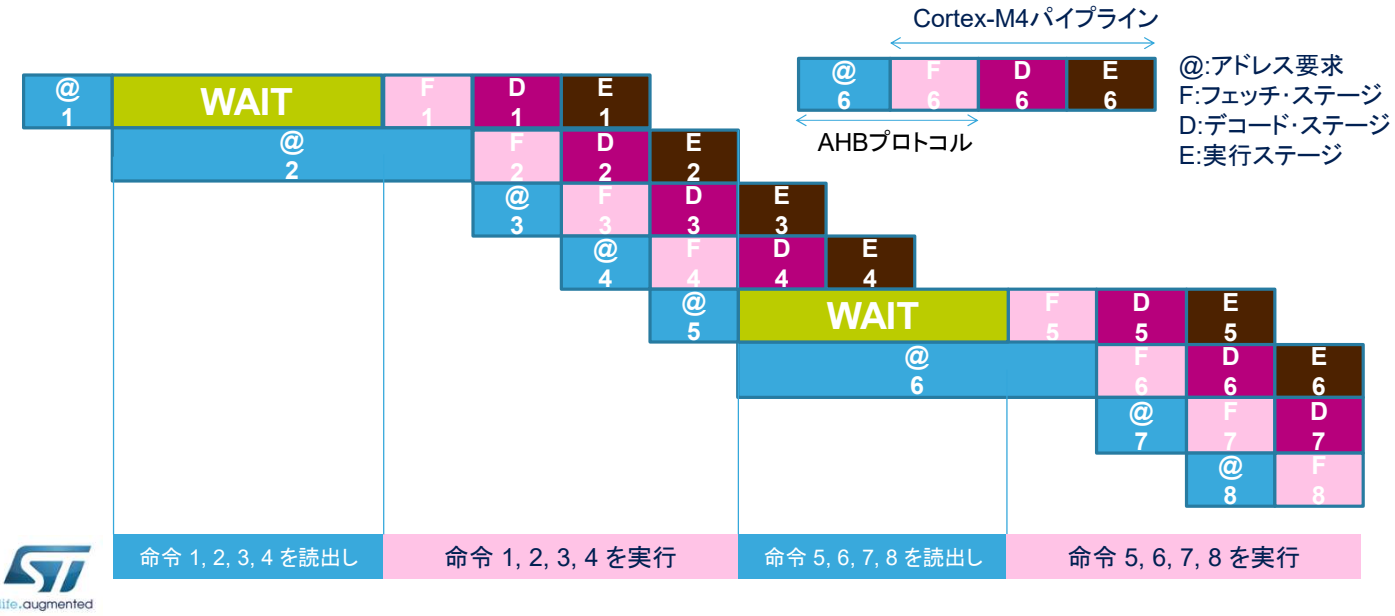
消費電力とパフォーマンスの結果は、アプリケーション･コードに依存
ほとんどの場合、キャッシュが ON かつプリフェッチが OFF の条件でエネルギー効率は最高

- プリフェッチがON：ARTの命令キャッシュは分岐キャッシュのように動作
  - キャッシュは処理フロー内で分岐／ジャンプが発生するたびに更新
  - シーケンシャル･アクセスは、現行命令バッファ＋プリフェッチバッファにより発行
  - プリフェッチ･バッファがアクセスされるたびに、その内容が現行命令バッファに転送され、プリフェッチバッファを満たす新しいFlashアクセスが行われる
    - したがって、キャッシュ内容は変更されない
- プリフェッチがオフ（リセット値）：ARTのキャッシュは普通のキャッシュのように動作
  - プリフェッチバッファが無効なので、シーケンシャルアクセスでもキャッシュ･コンテンツが変更される

life.augmented

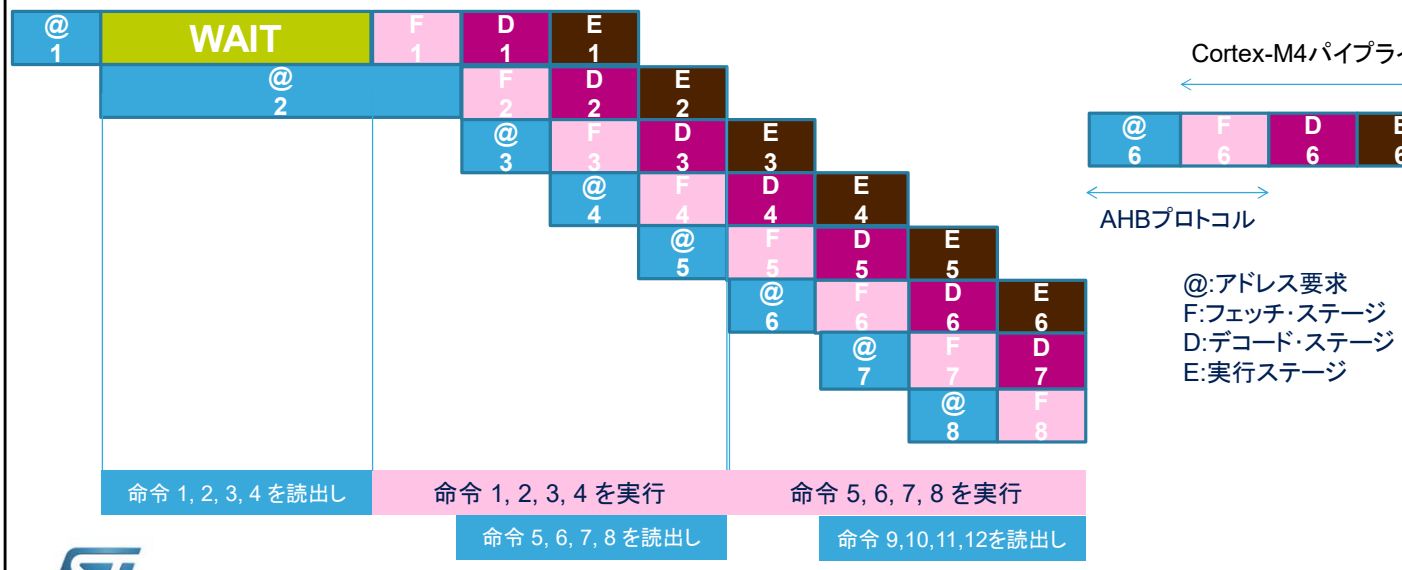
命令キャッシュは、プリフェッチバッファが有効か無効かによって動作が異なります。
プリフェッチバッファが有効な場合、ART の命令キャッシュは分岐キャッシュのように動作します。
キャッシュは処理フロー内で、分岐、または、ジャンプが発生するたびに変更されます。
シーケンシャルアクセスは現行命令バッファとプリフェッチバッファにより発行されます。プリフェッチ バッファがアクセスされるたびに、その内容は現行命令バッファに転送され、プリフェッチバッファにデータを満たすための新しい フラッシュアクセスが行なわれます。この場合、キャッシュの内容は変更されません。
プリフェッチバッファが無効になっている場合、ART 命令キャッシュは普通のキャッシュのように動作します。
プリフェッチバッファは無効なので、シーケンシャルアクセスでもキャッシュの内容が変更されます。
消費電力とパフォーマンスのトレードオフは、アプリケーションごとに評価し、プリフェッチバッファの有効、無効を判断する必要があります。
ほとんどのアプリケーションでは、プリフェッチバッファを有効にすることでパフォーマンスが若干向上しますが消費電力が増えます。
一般的に、フラッシュ アクセスの数が減るため、キャッシュが有効になり、プリフェッチ バッファが無効になっている場合、一般的に最適なエネルギー効率が提供されます。

シーケンシャル16bit命令の実行(3WS)
プリフェッチ無し



本スライドは、フラッシュメモリへのアクセスに3ウェイトステート必要な場合で、プリフェッチ無効時にシーケンシャル16ビット命令の 実行に必要なサイクル数を示しています。各フラッシュアクセスにより64ビットまたは4 命令を取得できます。これにより、各フラッシュアクセスにおいて、4 命令ごとに3ウェイトステートが挿入されます。

シーケンシャル16bit命令の実行(3WS)
プリフェッチ有効



本スライドは、フラッシュメモリへのアクセスに3ウェイトステートが必要な場合で、プリフェッチ有効時にシーケンシャル16ビット命令の実行に必要なサイクル数を示しています。。各フラッシュアクセス後に、次のフラッシュアクセスを行ないプリフェッチバッファを満たすことができます。
従って、現行バッファから全ての命令がフェッチされた後、次のシーケンシャル命令はプリフェッチバッファより読み出され、命令フローが順番に処理される限り、ウェイトステートは挿入されません。

Flashメモリの保護(1/2)

アプリケーションでの必要性に応じた柔軟なFlashメモリ保護機能

- 読出し保護(RDP)
  - SRAMからのブート時、ブートローダの選択時、またはデバッグ･インタフェース（JTAG/SWD）によるFlash/SRAM/バックアップ･レジスタへのアクセスを禁止
- 独自仕様コード保護(PCROP)
  - 読出し、または書込みアクセスから特定のコード域を保護するために使用
    - コードの実行のみ可能
- 書込み保護(WRP)
  - 不要な書込みアクセスおよび消去から特定のコード領域を保護するために使用

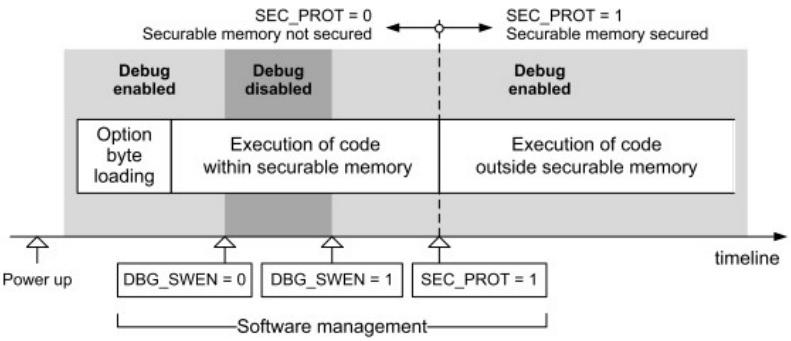
life.augmented

オプションバイトを使用して、複数のフラッシュメモリ保護オプションを設定できます。
読出し保護は、フラッシュメモリ、オプションバイト、内部CCM SRAMおよびバックアップレジスタの内容を、デバッガやソフトウェアの読み取りによって要求された読出しから保護することを目的としています。
フラッシュメモリからのブートのみが、これらのメモリの内容を読出すことを許可されます。
独自仕様コードの保護は、フラッシュメモリの一部を実行専用としてマークする方法です。この種のアクセス許可は、Cortex®-M4 コアに存在するメモリ保護ユニットではサポートされないことに注意してください。
PCROP 領域は、フラッシュ メモリの一部だけをサードパーティの読み取りから保護するのに役立ちます。
書込み保護により、フラッシュ メモリの一部が消去および再プログラムされるのを防ぐことができます。

Flashメモリの保護(2/2)

アプリケーションでの必要性に応じた柔軟なFlashメモリ保護機能

- セキュリティ保護可能なメモリ領域
  - アクティブ化すると、セキュリティ保護可能なメモリ領域へのアクセス (フェッチ、読出し、プログラミング、消去) が拒否され、バス·エラーが発生
- コアデバッグ·アクセスの無効化
  - セキュリティ保護可能なメモリ領域でコードを実行する際のデバッグ·アクセスの時間的な無効化



life.augmented

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フラッシュ メモリの特定の部分を保護することです。これにより、イメージ認証を担当するセキュアキーストレージやセキュア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。
プロセッサがセキュリティ保護可能なメモリを出ると、フラッシュメモリのこの部分にはアクセスできなくなります。
保護可能な領域は、デバイスをリセットすることによってのみ保護を解除できます。
セキュリティ保護可能なメモリ領域のサイズは、ページ上で調整されます。
さらに、セキュリティ保護可能なメモリから実行されたコードは、デバッグアクセスを一時的に無効にする可能性があります。

ユーザ･オプション･バイト

- ユーザ･オプション･バイトは次の場合に読み込まれる
  - 電源リセット後（BOR または STANDBY/SHUTDOWN の終了）
  - Flash制御レジスタ（FLASH_CR）のOBL_LAUNCH ビットがセットされたとき

オプション	説明	コメント
BOR_LEV[2:0]	ブラウンアウト･リセットの閾値レベル	STM32G4の新機能
nRST_STOP; nRST_STDBY; nRST_SHDW	STOP/STDBY/SHUDOWN モード終了時のリセットの生成／リセットの不生成	STM32F3と同じ
WWDG_SW; IDWG_SW IWDG_STOP; IWDG_STDBY	ハードウェア／ソフトウェア･ウィンドウのウォッチドッグ／独立型ウォッチドッグ STOP/STANBY モード時の、独立型ウォッチドッグのカウンタ停止の有無	STM32F3と同じ
BFB2	デュアルバンク･ブートの有効化/無効化	STM32G4の新機能
DBANK	128 ビットデータ読取り幅のシングルバンク･モードと 64bitデータ読取り幅のデュアルバンク･モード間の選択	STM32G4の新機能
nBOOT1	ブート設定 (BOOT0ピンと一緒に)	STM32F3と同じ
nSWBOOT0	オプション･ビット nBOOT0 から取得された BOOT0 または PB8/BOOT0 ピンから	STM32G4の新機能
nBOOT0		STM32G4の新機能
CCM SRAM_RST	システムリセット時、CCM SRAM 消去	STM32G4の新機能
SRAM_PE	SRAM1 および CCM SRAM パリティ･チェックを使用可能	STM32F3と同じ

オプションバイトは、Cortex®-M4を起動する前に、システムオンチップを早期に設定するために使用されます。これらは 48 バイトあります。
電源リセット後、またはFLASH_CR レジスタに OBL_LAUNCH ビットのセットに応じて、自動的に読み込まれます。この機能は、デバイスをリセットせずに新しい設定を適用するために必要です。
このスライドと次の 2 つのスライドでは、オプションバイトの各種フィールドについて説明します。

ユーザ・オプション・バイト

オプション	説明	コメント
BOOT_LOCK	設定すると、メインFlashメモリから強制的にブートする	STM32G4の新機能
SEC_SIZE1[7:0] SEC_SIZE2[7:0]	バンク 1 の確保可能なメモリ領域のサイズ バンク 2 の確保可能なメモリ領域のサイズ	STM32G4の新機能 STM32G431 はSEC_SIZE2なし
IRHEN	内部リセット・ホルダ・イネーブル・ビット	STM32G4の新機能
NRST_MODE	PG10/NRST 機能選択	STM32G4の新機能

life.augmented

Bootlock は、他のブート オプションに関係なく、システムをメイン フラッシュ メモリから強制的に起動させます

ユーザ･オプション･バイト(セキュリティ)

オプション	説明	コメント
RDP[7:0]	読出し保護レベル	STM32F3と同じ
PCROP1_STRT[14:0] PCROP1_END[14:0] PCROP2_STRT[14:0] PCROP2_END[14:0]	バンク 1 PCROP エリア開始オフセット アドレス バンク 1 PCROP エリア終了オフセット アドレス バンク 2 PCROP エリア開始オフセットアドレス バンク 2 PCROP エリア終了オフセット アドレス	STM32G4の新機能
PCROP_RDP	RDP レベルが低下した場合に保持される PCROP 領域	STM32G4の新機能
WRP1A_STRT[6:0] WRP1A_END[6:0] WRP1B_STRT[6:0] WRP1B_END[6:0] WRP2A_STRT[6:0] WRP2A_END[6:0] WRP2B_STRT[6:0] WRP2B_END[6:0]	バンク 1 書込み保護領域 A 開始 オフセット･アドレス バンク 1 書込み保護領域 A 終了 オフセット･アドレス バンク 1 書込み保護領域 B 開始 オフセット･アドレス バンク 1 書込み保護領域 B 終了 オフセット･アドレス バンク 2 書込み保護領域 A 開始 オフセット･アドレス バンク 2 書込み保護領域 A 終了 オフセット･アドレス バンク 2 書込み保護領域 B 開始 オフセット･アドレス バンク 2 書込み保護領域 B 終了 オフセット･アドレス	STM32F3では、書き込み保護は2ページの単位で実装され、2ページごとに1つのオプション･ビットがある

life.augmented

読出し保護レベルにより、フラッシュメモリ全体の読出し保護が可能:

- レベル0: 保護なし
- レベル1:読出し保護
- レベル2:デバッグ不可

レベル 0 からレベル 1、部分的または一括消去を意味するレベル 1 からレベル 0、レベル 0 からレベル 2、レベル 1 からレベル 2 までの遷移がサポートされます。

- PCROPA_STRTとPCROPA_ENDは、独自のコード読出し保護アドレス範囲 A を定義します。
- PCROPB_STRTとPCROPB_ENDは、独自のコード読出し保護アドレス範囲 B を定義します。
- PCROP_RDPは、RDP 保護がレベル 1 からレベル 0 に変更されたときに PCROP 領域を消去するか、または消去しないかの選択を行うことができます。

割込み

割込みイベント	説明
操作終了	1つまたはそれ以上の Flash メモリの操作（プログラム／消去）が正常に完了すると ハードウェアによってセット
操作エラー	Flash メモリの操作（プログラム／消去）が 正常に完了しなかったときに、ハードウェアによってセット
読出しエラー	読み取るアドレスがFlashの読取り保護領域に属している場合はハードウェアによってセット(PCROP保護)。
書出しエラー	消去/プログラムされるアドレスがFlashメモリの書き込み保護された部分(WRP、PCROPまたはRDPレベル1)に属している場合、ハードウェアによってセット
サイズ･エラー	プログラムまたは高速プログラム･シーケンス中に、アクセスのサイズがバイトまたはハーフワードである場合に、ハードウェアによってセット。ダブルワード･プログラミングのみ可能
プログラミング･エラー	プログラムされるダブルワード･アドレスが、書き込むデータが0x0000_0000の場合を除いて、プログラミング前に0xFFFF_FFFFとは異なる値が含まれている場合に、ハードウェアによってセット
プログラミング･シーケンスエラー	Flashメモリへの書き込みアクセスが実行される場合、ハードウェアによってセット PGまたはFSTPGが以前に設定されていない間にコードを記述 以前のプログラミング･エラーにより、PROGERR、SIZERR、PGAERR、WRPERR、MISSERR または FASTERR が設定されている場合も、ハードウェアによってセット

フラッシュ メモリ コントローラは、このスライドと次のスライドに示されているように多くの割込みソースをサポートしています。
操作が正常に終了すると、割込みをアサートできます。
プログラム/消去操作中にエラーが発生した場合、割込みをアサートすることもできます。
保護違反によっても割込みが発生する可能性があります。
サイズ エラーは、プログラムするデータがワードアラインドでない場合に発生します。
プログラムの操作が、事前にフラッシュ メモリを消去していないときに、エラーが発生します。

割込み

割込みイベント	説明
プログラミング･アライメントエラー	通常プログラミングの場合、同じダブルワード(64bit) Flashメモリにデータを含めることができない場合、または高速プログラミング中にページの変更がある場合、ハードウェアによってセット
高速プログラミング中のデータミス･エラー	新しいデータが時間内に存在しない場合は、ハードウェアによってセット
高速プログラミング･エラー	高速プログラミングシーケンス(FSTPGによってアクティブ化)がエラーのために中断された場合、ハードウェアによってセット
オプションの有効性エラー	読み取ったオプションがユーザーによって設定されたものではない場合がある
ECC訂正	1bitの ECCエラーが検出され、修正された場合、ハードウェアによってセット
マスク出来ない割込み (NMI)	
ECC検出	2bitのECCエラーが検出された場合、ハードウェアによってセット

プログラミングのアライメント エラーは、通常プログラムの操作を開始する前に完全なダブル ワードが指定されていない場合、または高速プログラミング操作を開始する前に完全な行が記述されていない場合に発生します。
高速プログラミング シーケンス中にデータが時間内に書き込まれていない場合、高速プログラミング中のデータミスエラーが発生します。
シングルビット ECC エラーが検出され修正されると、割込みをアサートできます。
ダブルビット ECC エラーが検出されると、NMI がアサートされます。

低電力モード

SRAMからのコード実行時の消費電力の最適化

- RUN／低電力RUN、SLEEP／低電力SLEEPの各モード時に、Flashへのクロッ ク供給をゲートオフできる
  - Flashクロックは、リセットおよびクロック･コントローラ（RCC）で設定
  - Flashクロックはデフォルトで有効
- SLEEP／低電力SLEEPモード時のFlashメモリをパワーダウン･モードに設定で きる
- RUN／低電力RUNモード時のFlashメモリをパワーダウン･モードに設定できる

フラッシュメモリからのコードを実行していない場合、フラッシュメモリ分の消費電力を下げることができます。
フラッシュクロックは、RUN／低電力 RUN モード時にゲートオフすることができます–またSLEEP／低電力 SLEEP モード時にも、フラッシュクロックをゲートオフすることができます。フラッシュクロックはリセットおよびクロックコントローラにより設定します。フラッシュクロックはデフォルトで有効です。
SLEEP／低電力 SLEEP モード時のフラッシュメモリをパワーダウンモードに設定できます。
コードが SRAM から実行されているとき、RUN／低電力 RUNモード時のフラッシュメモリもまたパワーダウンモードに設定できます。
クロックのゲーティングおよびフラッシュメモリをパワーダウンモードに設定することで、消費電力を大幅に低減できます。

低電力モード

モード	説明
RUN	有効 コードが SRAM から実行され、Flashメモリがパワーダウン·モードの場合、Flashクロックを無効にできる
SLEEP	有効 SLEEPモード時にFlashクロックを無効にできます。Flashメモリをパワーダウン·モードにすることができる
低電力 RUN	有効 コードが SRAMから実行され、Flashメモリがパワーダウン·モードの場合、Flashクロックを無効にできる
低電力 SLEEP	有効 低電力 SLEEPモード時にFlashクロックを無効にできます。Flashメモリをパワーダウンモードにすることができる
STOP 0/STOP 1	Flashメモリ のクロック·オフ ペリフェラル·レジスタの内容は保持され、Flashメモリは、パワーダウン·ードにすることができる
STANDBY	パワーダウン状態 Flashメモリ·インタフェースは、STANBY モード終了後に再び初期化する必要がある
SHUTDOWN	パワーダウン状態 Flashメモリインタフェースは、SHUTDOWN モード終了後に再び初期化する必要が ある

life.augmented

フラッシュ メモリ モジュールは、次の低電力機能をサポートします。

- クロック・ゲーティング
- フラッシュメモリのパワーダウンモード
- モジュール全体への電力ゲーティング:フラッシュメモリとコントローラ

RUN、SLEEP、低電力RUN 、低電力SLEEPスリープモードではクロックのゲーティング、パワーダウンモードがサポートされています。SRAMからコードを実行する際に使用できます。

STOP0 と STOP1 では、クロックはゲートされ、フラッシュ メモリはパワーダウン モードに入ります。

SHUTDOWNモードでは、フラッシュメモリとコントローラの両方に対して、フラッシュメモリモジュールの電源がゲートされます。クロックをゲーティングし、フラッシュメモリをパワーダウンモードに設定すると、消費電力が大幅に削減されます。

Flashメモリのパフォーマンス

3.36Coremark / MHz

- ARTアクセラレータにより、Flashメモリのパフォーマンスは周波数に対してほぼ線形的に変化
- 3.36 CoreMark / MHz (シングルバンク、キャッシュオン、プリフェッチオン) => 571CoreMark @ 170MHz

	ART オン I-キャッシュ オン D-キャッシュオン プリフェッチオン		ART オン I-キャッシュ オン D-キャッシュ オン プリフェッチ オフ		ART オフ	
	デュアルバンク	シングルバンク	デュアル バンク	シングル バンク	デュアル バンク	シングル バンク
CoreMark / MHz	3.26	3.36	3.23	3.32	1.05	1.47

life.augmented

ここでは、EEMBC CoreMarkベンチマークを実行しながら、170 MHzでのコード実行パフォーマンスを比較します。
コードが SRAM1 にあるデータを CCM SRAM で実行されると、最大パフォーマンスに達します。
170 MHz でフラッシュ メモリから実行すると、ART アクセラレータが有効の場合 CoreMark の最大パフォーマンスに達し、170 MHz で 7 つのウェイトを必要とするフラッシュ アクセス時間によるパフォーマンスの低下はほとんどありません。

関連ペリフェラル

- このペリフェラルにリンクされている他のペリフェラルのトレーニングを参照してください。
  - システム設定コントローラ (SYSCFG)
  - リセットおよびクロック・コントローラ(RCC)
  - 電源コントローラ(PWR)
  - 割込み (NVIC)
  - メモリ保護

フラッシュ メモリ モジュールは、次の他のモジュールとの関係を持っています。

- システム設定コントローラ(SYSCFG)
- リセットおよびクロックコントローラ(RCC)
- 電源コントローラ(PWR)
- 割込み(NVIC)
- メモリ保護

参照

- 詳しくは、以下の関連資料を参照してください。
  - AN2606: STM32 microcontroller system memory boot mode – Application note

詳しくは、STM32 マイクロコントローラのシステムメモリブート モードに関するアプリケーションノート、AN2606 を参照してください。