STM32WL5 - Flash

内蔵 Flash メモリ

レビジョン 1.0

STM32WL5 Flash メモリのプレゼンテーションへようこそ。
STM32WL5 Flash メモリの特徴をすべて説明します。

概要

- STM32WL5は、最大256KBのシングルバンクFlashメモリを内蔵
- Flashインタフェースは、すべてのアクセス（読出し、プログラム、消去）、メモリ保護、セキュリティ、およびオプション・バイトの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
- 小さい消去粒度
- 短いプログラミング時間
- セキュリティと保護

life.augmented

2

STM32WL5 は、最大 256 KB のシングルバンク Flash メモリを内蔵しています。
Flash メモリインタフェースは、すべてのメモリ・アクセス（読出し、プログラム、および消去）、メモリ保護、セキュリティ、およびオプション・バイトを管理します。
この Flash メモリ・インタフェースを使用するアプリケーションでは、低消費電力アクセスでありながら高性能という利点が得られます。消去の粒度が小さく、プログラミング時間も短くて済みます。
STM32WL5 Flash メモリは、コードとデータ、読出しと書込みのアクセスに対して、さまざまなセキュリティと保護のメカニズムを備えています。

主な機能

- 最大256KBのシングルバンクFlashメモリ
- 2KBのページ粒度
- 高速消去（22ms）と高速プログラミング（ダブルワードで82µs）
- 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）により、クロック周波数に比例する性能を実現
- エラーコード訂正（ECC）：64bitのダブルワードで8bit
  - シングルエラーの検出と訂正
  - ダブルエラーの検出と通知

life.augmented

STM32WL5 の Flash メモリは、さまざまな重要な機能を備えています。
最大 256 KB のシングルバンク Flash メモリを内蔵しています。
ページサイズに応じて消去粒度はわずか 2 KB です。
ページ消去、バンク消去、または全体消去の操作の所要時間はわずか 22 ms、ダブルワード 1 つのプログラミング時間はわずか 82 µs です。
適応型リアルタイムメモリ･アクセラレータは、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、クロック周波数に比例する性能を実現します。
Flash メモリは、64 ビットのダブルワードごとに 8 ビット長のエラー･コード訂正（ECC）をサポートしています。シングルエラーが検出され、訂正されます。ダブルエラーは検出されますが、訂正はされません。

Flashメモリの構成

- Flashメモリの構成:
- メインメモリ·ブロックは128ページで構成(1ページは2KB)、1ページは8行で構成(1行は256バイト)
- 情報ブロックの構成:
  - S ブートローダとSFI用にシステム·メモリを予約
  - ユーザデータ用に1KB(ダブルワード128個分)のOTP(一度だけプログラム可能な)領域
    - OTPエリアにはダブルワードを1回だけ書込み可能で、書き込んだデータは消去不能。ダブルワードの1つのビットを0に設定しただけで、そのダブルワード全体が書込み不能(すべて0x0の値は例外)
  - ユーザ設定のオプション·バイト

life.augmented

Flash メモリは 128 ページで構成されます(1 ページ は 2 KB)。
1 ページは 8 行で構成されます(1 行 は 256 バイト)。
メインメモリブロックに続いて、3 つの部分から成る情報ブロックがあります。
1 番目の部分は、ST のブートローダとセキュアファームウェアのインストール用に予約されているシステムメモリです。選択したデバイスはシステムメモリからブートし、ブートローダまたはセキュアファームウェアがインストールされます。
2 番目の部分は、一度だけプログラム可能な(OTP) 1 KB の領域です。OTP エリアは消去できず、ダブルワードを 1 回だけ書き込むことができます。ダブルワードの 1 つのビットを 0 に設定しただけで、そのダブルワード全体が書き込めなくなります。すべてのビットを 0 に設定したダブルワードは、この例外です。すでにプログラミングされているダブルワードのプログラミングは、すべてのビットをゼロにプログラミングする場合にのみ可能です。
3 番目の部分には、ユーザオプション設定用のオプション·バイトがあります。

Flashメモリの構成

Flash領域	Flashメモリ·アドレス	サイズ	名前
メイン·メモリ	0x0800 0000 ~ 0x0800 07FF	2KB	ページ0
	...	...	...
	0x0803 F800 ~ 0x0803 FFFF	2KB	ページ127
情報ブロック	0x1FFF 0000 ~ 0x1FFF 6FFF	28KB	システム·メモリ
	0x1FFF 7000 ~ 0x1FFF 73FF	1KB	OTPエリア
	0x1FFF 7800 ~ 0x1FFF 7FF	2KB	オプション·バイト

life.augmented

このスライドは、Flash メモリ·マップを示しています。メインメモリは 128 ページあり、ページ 0 から始まります。ソフトウェア手順でページを消去するときにページ番号を使用します。

堅牢なメモリの整合性と安全性

- ECC（エラーコード訂正）:64 ビットワードあたり 8 ビット
  - シングルエラー訂正:FLASH_ECCR の ECCC ビットがセットされ、必要に応じて割込みを生成
  - ダブルエラー検出:FLASH_ECCR の ECCD ビットをセット => NMI
  - FLASH_ECCR レジスタに障害発生元アドレスを保存
- プログラミングの粒度は 64 ビット（実際は 8 ビットの ECC を含む 72 ビット）
  - 2 つのプログラミングモード:
    - 標準（メインメモリと OTP 用）
    - 高速（メインメモリのみ）、Flash の位置を確認せずに 32 個のダブルワードをプログラミング

life.augmented

Flash メモリにはエラーコード訂正機能が組み込まれ、メモリの堅牢な整合性と安全性が確保されています。
ECC は、64 ビットワードあたり 8 ビットの長さです。シングルエラーが訂正されます。Flash の ECC レジスタの ECCC ビットがセットされ、割込みが有効であれば割込みが生成されます。ダブルエラーは検出されますが訂正されません。Flash の ECC レジスタの ECCD ビットがセットされ、ノンマスカブル割込みが生成されます。ECC エラーが検出されると、Flash の ECC レジスタに障害発生元アドレスが保存されます。
プログラミングの粒度は 64 ビットですが、実際は 8 ビットの ECC を含む 72 ビットです。プログラミングモードには、メインメモリと OTP で使用できる標準モードと、メインメモリ専用の高速モードの 2 つがあります。標準モードでは、プログラミングを開始する前に、Flash メモリのダブルワードが消去されていることが確認されます。高速モードでは、Flash の位置が確認されることなく、32 個のダブルワードがプログラミングされます。

プログラミング時間と消去時間

プログラミング時間と消去時間が短く、ページサイズが小さい
=> データEEPROMのエミュレーションに有利

パラメータ	標準値
64 ビットのプログラミング時間	82µs
ページ(2 KB)の消去時間	22ms
1 行(32 個のダブルワード)のプログラミング時間	標準モード:2.6ms 高速モード:1.9ms
1 ページ(2 KB)のプログラミング時間	標準モード:20.8ms 高速モード:15.2ms
Flash (256 KB)のプログラミング時間	標準モード:3s 高速モード:2s
全体消去時間	22ms

life.augmented

7

Flash メモリのプログラミング時間は、64 ビットのダブルワードでわずか 82 µs です。1 ページ(2 KB)をプログラムするには、標準モードで 20.8 ms、高速モードで 15.2 ms の時間を要します。Flash メモリ全体をプログラムするには、高速モードで 2 秒を要します。
ページの消去時間は 22 ms です。Flash メモリ全体の消去に必要な時間もわずか 22 ms です。
プログラミング時間と消去時間が短く、ページサイズが小さいので、データ EEPROM のエミュレーションに便利です。

行（64ダブルワード）の高速プログラミング

- メインメモリのみ高速プログラミングでプログラム可能
- プログラミングの前にHWでFlashの位置は確認されない
- 32個のダブルワードを連続で書き込む必要がある
  - すべてのプログラミングでFlashメモリに対してハイ電圧が維持される
  - プログラミング時間とは、2つのダブルワード書込みリクエスト間の最長時間（約20µs） => この期間は割込みの無効化が必要
- Flashのクロック周波数（HCLKS）は8MHz以上にする必要がある

life.augmented

高速プログラミングモードでは、標準プログラミングモードより短時間で 32 個のダブルワードをプログラムできます。
メインメモリのみ高速プログラミングモードでプログラムできます。
高速モードのプログラミングの前に、ハードウェアで Flash メモリのアドレス位置の内容が確認されることはありません。
32 個のダブルワードを連続で書き込む必要があります。すべてのプログラミングで Flash メモリに対してハイ電圧が維持されます。プログラミング時間とは、2 つのダブルワード書込みリクエスト間の最大時間です（約 20 µs）。したがって、割込みを無効にして、2 つのワード書込みリクエスト間の時間が 20 µs を超えないようにする必要があります。
高速プログラミングモードでは、Flash のクロック周波数を 8 MHz 以上にする必要があります。

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

	プログラミング·モード	
	標準	高速
対象	メインメモリと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	アドレス位置の内容確認なし Flash のクロック周波数は8MHz以上 割込み禁止
256バイトのプログラミングに要する時間	2.6ms	1.9ms

life.augmented

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との比較です。標準モードはメインメモリと OTP エリアのプログラミングに使用できます。高速モードは OTP のプログラミングには使用できません。標準モードでは 64 ビットダブルワード（8 バイト）をプログラミングできますが、高速モードでは 32 個の 64 ビットダブルワード（256 バイト）のみをプログラミングできます。高速モードでは、プログラミングの前にアドレス位置の内容は確認されません。また、Flash のクロック周波数は 8 MHz より高くする必要があり、CPU 割込みは禁止されています。256 バイトのプログラムに要する時間は、標準モードで 2.6 ms、高速モードで 1.9 ms です。

Flashメモリの保持

耐久性	-40 ~ +105℃で10,000サイクル以上
データ保持	55℃で10,000サイクル後30 年 85℃で10,000サイクル後15 年 105℃で 10,000サイクル後10 年 85℃で1,000サイクル後30年 105℃で1,000サイクル後15年 125℃で1,000サイクル後7年
サイクル保持	1 ppm

life.augmented

このFlash メモリは、最高 105 ℃で 10,000 サイクル以上の動作を保証します。データ保持は、55 ℃での 10,000 サイクル後 30 年、85 ℃での 10,000 サイクル後 15 年、105 ℃での 10,000 サイクル後 10 年、85 ℃での 1,000 サイクル後 30 年、105 ℃での 1,000 サイクル後 15 年、125 ℃での 1,000 サイクル後 7 年です。

Flashメモリ読出しアクセス

48MHzで60DMIPS

- 適応型リアルタイム・メモリ・アクセラレータ（ART Accelerator™）は、Flashメモリへのアクセス時間に関係なく、クロック周波数に比例する性能を実現

ウェイトステート（WS）（遅延）	HCLK（MHz）	
	V_{CORE} レンジ1	V_{CORE} レンジ2
0 WS	≤ 18	≤ 6
1 WS	≤ 36	≤ 12
2 WS	≤ 48	≤ 16

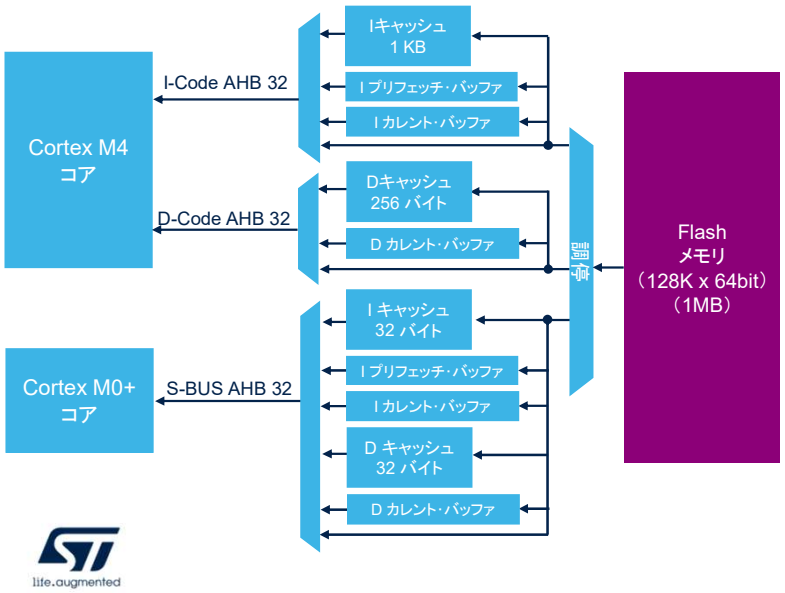
life.augmented

11

Flash メモリを読み出すには、読出しアクセスで挿入するウェイトステート数を、クロック周波数に応じて設定する必要があります。ウェイトステート数は、電圧スケーリングレンジにも依存します。レンジ 1 の場合、ウェイトステートが 2 つであれば最大 48 MHz、ウェイトステートがなければ最大 18 MHz で、それぞれ Flash メモリにアクセスできます。レンジ 2 の場合、ウェイトステートが 2 つであれば最大 16 MHz でアクセスできます。適応型リアルタイムメモリアクセラレータ（ART Accelerator）を使用すると、クロック周波数に関係なく、ウェイトステートなしでプログラムを実行できます。これにより、クロック周波数にほぼ正比例する性能が得られ、48 MHz では 60 Dhrystone MIPS を実現できます。

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

抜群の性能と低消費電力



- Cortex-M4
  - **命令キャッシュ** = 4 x 64bit x 32ライン(1KB)、命令用
  - **データキャッシュ** = 4 x 64bit x 8 ライン(256バイト)、リテラルプール用
  - **プリフェッチ·バッファ**
- Cortex-M0+
  - **命令キャッシュ** = 1 x 64bit x 4 ライン(32バイト)、命令用
  - **データキャッシュ** = 1 x 64bit x 4 ライン(32バイト)、リテラルプール用
  - **プリフェッチ·バッファ**
- キャッシュサイズ、電力、性能の間の最適なトレードオフ

12

ART Accelerator は抜群の性能を発揮し、動的な電力消費を削減します。Cortex-M4 の 1 KB の命令キャッシュ、256 バイトのデータキャッシュ、プリフェッチ·バッファ、および Cortex-M0+ の 32 バイトの命令キャッシュ、32 バイトのデータキャッシュ、プリフェッチ·バッファで構成されています。
Cortex-M4 の命令キャッシュは 4 個のダブルワード x 32 ラインで構成され、データキャッシュは 4 個のダブルワード x 8 ラインで構成されます。すべての命令キャッシュメモリラインが使用中の場合、LRU(最も長い時間使われていない)ポリシーを使用して命令メモリ·キャッシュの中で置き換えるラインを決定します。この機能は、コードにループが含まれる場合に特に有用です。
このアーキテクチャが選択されたのは、キャッシュサイズ、消費電力、および性能の間で最適なトレードオフを実現するためです。

Flash へのアクセスを制限して省電力を実現するために、キャッシュ·ミスが発生するたびに、要求されたダブルワードによってのみキャッシュが更新されます。1 ラインにある 4 個のダブルワードがすべて有効であるとは限りません。

キャッシュ·ミスが発生した場合、コードは Flash メモリから直接命令を取得します。64 ビット·ラインは、有効なカレント·バッファにコピーされるほか、有効な I キャッシュがあれば、そこにも同時にコピーされます。したがって、次のシーケンシャルアクセスはカレント·バッファから直接実行されます。
プリフェッチが有効な場合、プリフェッチ·バッファにシーケンシャルデータを格納するために、さらに 64 ビットの Flash メモリへのアクセスが発生します。

データがカレント·バッファに存在する場合、CPU はカレント·バッファを読み出します。次のシーケンシャル読出しはプリフェッチ·バッファで発生し、それがカレント·バッファにコピーされるので、次のシーケンシャルデータを格納する領域が得られます。

データがカレント·バッファに存在せず、プリフェッチ·バッファに存在する場合、プリフェッチ·バッファから読み出されます。プリフェッチ·バッファにも存在しない場合、命令キャッシュでヒットすれば、そこから読み出されます。ヒットしなければ、Flash へのアクセスが発生します。

Cortex-M4 の I-Code 命令、D-Code データ、Cortex-M0+ S-bus の命令とデータの間での Flash へのアクセス調停では、ラウンドロビン方式が使用されます。

ARTの基本

電力と性能の結果はアプリケーションコードに依存

キャッシュを有効･プリフェッチを無効にすると、ほとんどの場合、最良のエネルギー効率が実現

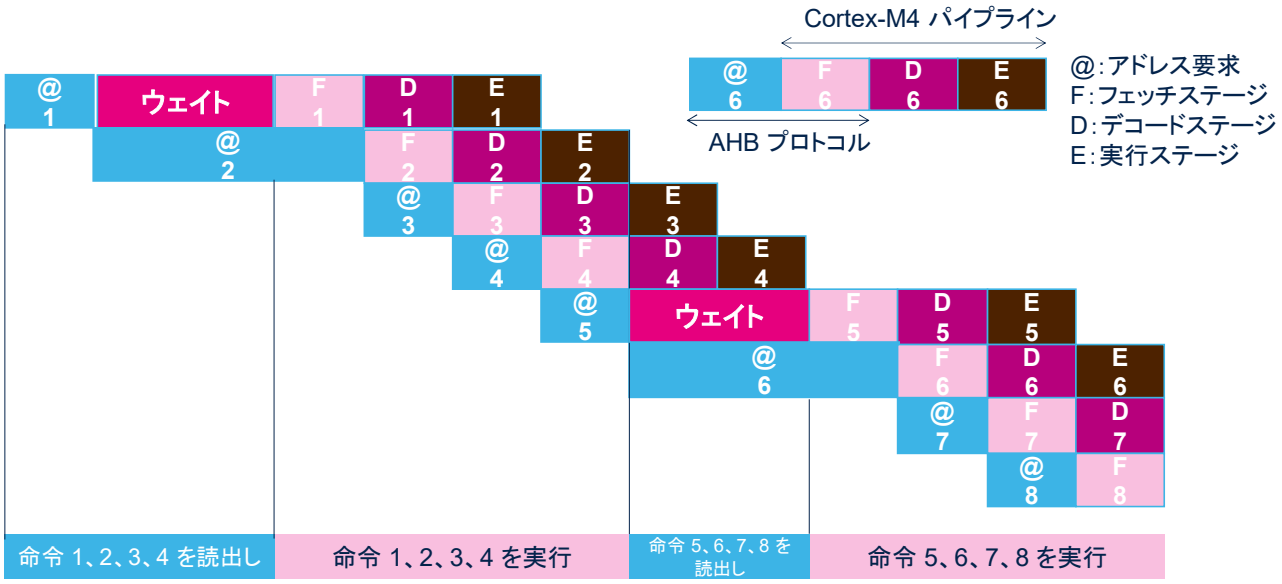
- プリフェッチが有効な場合：ART命令キャッシュは分岐キャッシュのように動作する
  - キャッシュは、実行フローで分岐やジャンプが発生するたびに変更される
  - 現在の命令バッファとプリフェッチ･バッファによってシーケンシャル･アクセスが発行される
  - プリフェッチ･バッファがヒットするたびに、その内容が現在の命令バッファに転送され、プリフェッチ･バッファに次の命令を配置するために新しい Flash アクセスが実行される
  - => キャッシュの内容が変更される
- プリフェッチが無効な場合（リセット値）：ART キャッシュは通常のキャッシュ同様に動作する
  - プリフェッチ･バッファを使用できないので、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る

life.augmented

13

命令キャッシュの動作は、プリフェッチ･バッファが有効かどうかによって異なります。
プリフェッチ･バッファが有効な場合、ART 命令キャッシュは分岐キャッシュのように動作します。このキャッシュの内容は、実行フローで分岐やジャンプが発生するたびに変更されます。現在の命令バッファとプリフェッチ･バッファによってシーケンシャルアクセスが発行されます。プリフェッチ･バッファがヒットするたびに、その内容が現在の命令バッファに転送され、プリフェッチ･バッファに次の命令を配置するために新しい Flash アクセスが実行されます。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･バッファが無効な場合、ART 命令キャッシュは通常のキャッシュのように動作します。プリフェッチ･バッファを使用できないので、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。
プリフェッチ･バッファを有効にした場合と無効にした場合のどちらが良いかを判断するには、アプリケーションごとに電力と性能のトレードオフを評価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性能がわずかに向上しますが、消費電力が増加します。ほとんどの場合、キャッシュを有効、プリフェッチを無効にすると最大限のエネルギー効率が得られます。これによって普通は Flash メモリへのアクセス回数が減少するからです。

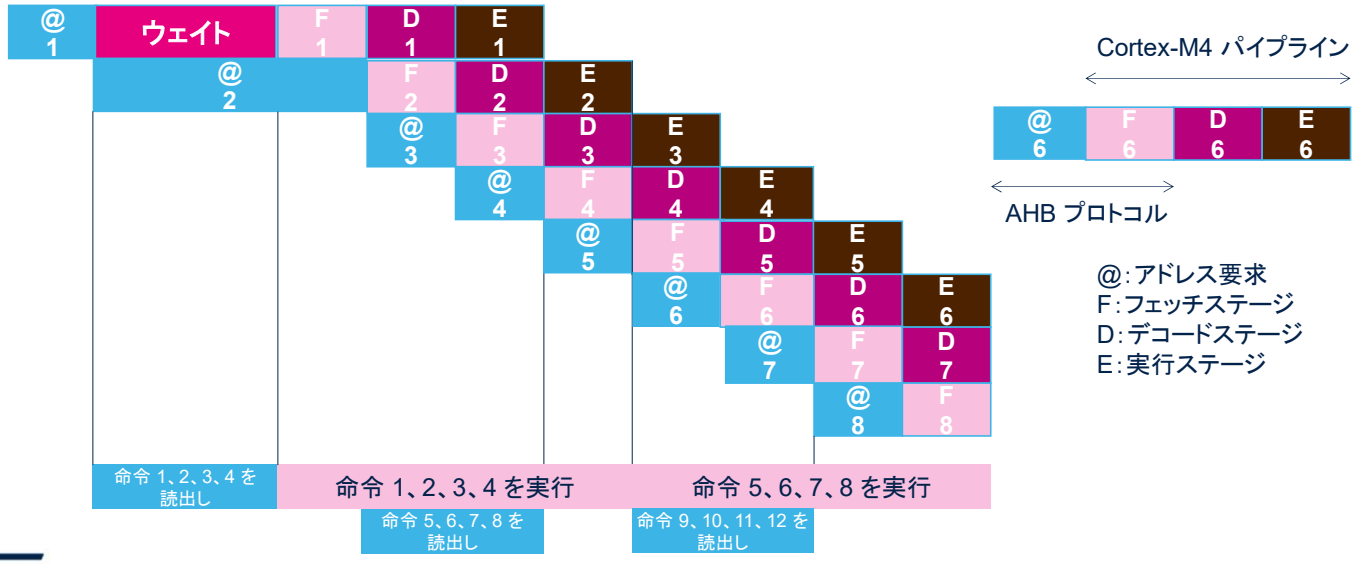
シーケンシャル 16 ビット命令の実行（2 WS）、プリフェッチなし



life.augmented

このスライドは、Flash メモリにアクセスするために 2 回のウェイトステートが必要な場合、プリフェッチなしでシーケンシャル 16 ビット命令を実行するために必要なサイクル数を示しています。1 回の Flash アクセスで 64 ビット（4 つの命令）を取得します。したがって、Flash にアクセスするたびに、4 つの命令ごとに 2 回のウェイトステートが挿入されます。

シーケンシャル 16 ビット命令の実行（2 WS）、プリフェッチあり



life.augmented

15

このスライドは、Flash メモリにアクセスするために 2 回のウェイトステートが必要な場合、プリフェッチを有効にしてシーケンシャル 16 ビット命令を実行するために必要なサイクル数を示しています。Flash にアクセスするたびに、プリフェッチ・バッファを別の命令を配置するために新しい Flash アクセスが実行されます。したがって、カレント・バッファからすべ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・バッファから読み出されます。命令フローが順次処理される限り、ウェイトステートは挿入されません。

専用のトレーニングを参照

Flashメモリの保護

アプリケーションのニーズに応じた柔軟な Flash メモリ保護

- 読出し保護（RDP）
  - Flash、SRAM2、バックアップ・レジスタへのアクセスを、デバッグ・インタフェース（JTAG/SWD）を介している場合、SRAM1からブートするとき、ブートローダを選択しているときに禁止
- 商用コード保護（PCROP）
  - 1KBの粒度で定義した2つの領域を保護、特定のコード領域を読出しアクセスまたは書込みアクセスから保護、コードは実行のみが可能
- 書込み保護（WRP）
  - 2KBの粒度で定義した2つの領域を保護、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
- Cortex-M0+ セキュリティ（SFD）
  - Flashの上位部分への排他アクセス（粒度2KB）をCortex-M0+に付与

life.augmented

16

オプション・バイトを使用して、さまざまな Flash メモリ保護オプションを設定できます。
読出し保護は、RDP オプション・バイトを使用して設定します。読出し保護は、Flash メモリ、SRAM2、バックアップレジスタへのアクセスを、デバッグインタフェースを介している場合、SRAM1 からブートするとき、またはブートローダを選択しているときに禁止します。
商用コード保護は、PCROP オプション・バイトを使用して設定します。これらのオプションは、特定のコード領域を読出しまたは書込みアクセスから保護します。コードは実行のみ可能です。保護領域は 1 KB の粒度で 2 つの領域を定義できます。
書込み保護は、WRP オプション・バイトを使用して設定します。これらのオプションは、不要な書込みアクセスと消去から特定のコード領域を保護します。書込み保護領域は 2 KB の粒度で定義できます。
Cortex-M0+ セキュリティは、SFD オプション・バイトを使用して設定します。このオプションは、特定の Flash メモリ領域を Cortex-M0+ による排他アクセス用として保護します。Cortex-M0+ セキュリティ領域は 2 KB の粒度で定義できます。
これらの保護オプションの詳細については、システム保護と Cortex-M0+ セキュリティに関するトレーニングを参照してください。

Cortex-m0+セキュリティ

- Flashメモリの上位部分はCortex-M0+による排他アクセス用としてセキュリティで保護可能
  - セキュア·ユーザ·オプションのSFDとSFSAで定義
- グローバル·セキュリティが有効
  - セキュア·ユーザ·オプションのSBRDとSBRSAにより、SRAM2aの上位部分のセキュリティを追加できる
  - セキュア·ユーザ·オプションのSNBRDとSNBRSAにより、SRAM2bの上位部分のセキュリティを追加できる
  - 一部のペリフェラルを保護できる

life.augmented

17

Flash Security Disable オプションをオフにすると、Cortex-M0+ セキュリティが有効になります。セキュア Flash は、Secure Flash Start Address オプションで指定したアドレスから始まります。Flash メモリのほかに、SRAM2a と SRAM2b のセキュリティも、Secure Backup RAM Disable、Secure Backup RAM Start Address、Secure Non Backup RAM Disable、Secure Non-Backup RAM Start Address の各オプションで有効化できます。セキュリティ保護可能な Sub-GHz シリアルペリフェラルインタフェースペリフェラルも、Sub-GHz シリアルペリフェラルインタフェースの Security Disable オプションをオフにすることによってセキュリティを有効化できます。高度暗号化標準アクセラレータ、秘密鍵アクセラレータ、真の乱数発生器などのセキュリティ保護可能なペリフェラルは、TrustZone セキュリティコントローラ IP のレジスタビットによって実行時にセキュリティで保護できます。

ユーザ･オプション･バイト

ユーザオプション･バイトがロードされるタイミング：
- 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ビットをセットしたとき

オプション	説明
BOR_LEV[2:0]	ブラウンアウト･リセット閾値レベル
nRST_STOP、nRST_STDBY、nRST_SHDW	STOP/STANDBY/SHUDOWN モード終了時のリセット生成の有無
WWDG_SW、IDWG_SW IWDG_STOP、IWDG_STDBY	ハードウェア/ソフトウェアによるウィンドウ型ウォッチドッグ/独立型ウォッチドッグ STOP/STANDBY モード時の独立型ウォッチドッグカウンタ停止の有無
nBOOT0、nBOOT1、BOOT0SW BOOT_LOCK、C2BOOT_LOCK	ブート設定 BOOT0 選択 CPU1 と CPU2 のブートロック設定
SRAM_RST SRAM_PE	システムリセット時の SRAM2a/2b 消去 SRAM2a/2b パリティチェック･イネーブル
IPCCDBA	IPCC データバッファのベースアドレス

life.augmented

18

Flash メモリには、デバイスの特定の機能を設定するためのさまざまなユーザオプションバイトが用意されています。
ユーザオプションバイトがロードされるタイミングは 2 つあり、1 つは電源リセットまたはブラウンアウトリセットの後で STANDBY モードまたは SHUTDOWN モードを終了したとき、もう 1 つは Flash 制御レジスタの OBL_LAUNCH ビットをセットしたときです。
ブラウンアウトリセット閾値を設定するには、3 つのオプション･ビットを使用します。
STOP、STANDBY、および SHUTDOWN の低消費電力モードを禁止または許可する 3 つのオプションがあります。
ウォッチドッグをハードウェアとソフトウェア設定のどちらで有効にするか、および STOP モードと STANDBY モードで独立型ウォッチドッグを停止するかどうかを設定する 4 つのオプションがあります。
ブートに使用するメモリおよびブートエントリポイントを設定するには、5 つのオプションを BOOT0 ピンと組み合わせて使用します。
システムリセットで SRAM2 を消去するかどうかを設定するオプションと、SRAM2 のパリティチェックを有効にするオプションの 2 つがあります。
プロセッサ間通信のデータバッファとして使用する SRAM2 の共通メモリ領域を定義するオプションが 1 つあります。

ユーザ･オプション･バイト

オプション	説明
RDP[7:0]、ESE	読出し保護レベルとセキュリティ環境
PCROP1A_STRT PCROP1A_END PCROP1B_STRT PCROP1B_END	PCROP 領域 A 開始オフセットアドレス PCROP 領域 A 終了オフセットアドレス PCROP 領域 B 開始オフセットアドレス PCROP 領域 B 終了オフセットアドレス
PCROP_RDP	RDP レベルが低下したときに PCROP 領域を保持
WRP1A_STR WRP1A_END WRP1B_STRT WRP1B_END	書込み保護領域 A 開始オフセットアドレス 書込み保護領域 A 終了オフセットアドレス 書込み保護領域 B 開始オフセットアドレス 書込み保護領域 B 終了オフセットアドレス
SFSA、SBRSA、SNBRSA HDPSA、SBRV、C2BOPT	Cortex-M0+ の Flash と SRAM2 のセキュリティ開始アドレス Cortex-M0+ の Flash 秘匿保護開始アドレス Cortex-M0+ ブートリセットベクタおよびブートオプション Flash/SRAM2
DDS、SUBGHZSPISD	Cortex-M0+ デバッグの無効化 Sub-GHz SPI セキュリティの無効化

* Cortex-M0+ 書込みセキュアのオプション

19

メモリ保護とペリフェラルへのアクセスのオプションとして、さまざまなオプション･バイトを使用します。
RDP は読出し保護、PCROP は 2 つの領域の開始アドレスと終了アドレス、WRP は 2 つの領域の開始アドレスと終了アドレスを、それぞれ設定します。
PCROP_RDP ビットは、読出し保護がレベル 1 からレベル 0 に下がったときに PCROP 領域を維持するか、消去するかを設定します。
Cortex-M0+ のセキュアなメモリ領域は、Flash メモリでは SFSA、SRAM2a では SBRSA、SRAM2b では SNBRSA で、それぞれ定義します。Cortex-M0+ のリセットベクタは、SBRV と C2BOPT で定義します。有効にしたセキュリティ環境は ESE ビットで示され、RDP と ESE の同時回帰によって削除できます。
Cortex-M0+ のデバッグは DDS によって無効になります。
Sub-GHz シリアルペリフェラルインタフェースのセキュリティは SUBGHZSPISD で定義します。
Cortex-M0+ のセキュアなメモリ領域、ブートオプション、ペリフェラルへのアクセスとデバッグの無効化は、Cortex-M0+ の排他書込みアクセスです。これらを Cortex-M4 で読み出して、セキュリティに関する情報が得られます。

割込み

割込みイベント	説明
割込み	
操作終了	1 つ以上のFlashメモリ操作（プログラム/消去）が正常に完了したときに、ハードウェアによってセットされる
操作エラー	Flashメモリ操作（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される
読出しエラー	Dバスを通じて読み出すアドレスがFlashメモリの読出し保護領域に属する場合に、ハードウェアによってセットされる（PCROP保護）
ECC 訂正	1 つのECCエラーが検出され訂正されたときに、ハードウェアによってセットされる
Flashインタフェースへの不正アクセス	Flashインタフェースへの不正アクセスが検出されたときに、ハードウェアによって設定される
Flash への不正アクセス	Flashメモリへの不正アクセスが検出されたときに、ハードウェアによって設定される
ノンマスカブル割込み（NMI）	
ECC 検出	2 つのECCエラーが検出されたときに、ハードウェアによってセットされる

life.augmented

20

Flash メモリでは、次の 4 つの割込みが生成されます。
操作終了割込み：Flash メモリに対する 1 つ以上の プログラム操作または消去操作が正常に完了するとトリガされます。
操作エラー割込み：Flash メモリに対するプログラム操作または消去操作が失敗するとトリガされます。
読出しエラー割込み：コア・データ・バスを通じて読み出すデータのアドレスが、PCROP オプションで保護されている Flash 領域に属しているとトリガされます。
ECC 割込み：1 つの ECC エラーが検出されて訂正されるとトリガされます。2 つの ECC エラーが検出されたときは、ノンマスカブル割込みが生成されます。
Flash インタフェースまたは Flash メモリへの不正アクセスがあると、TrustZone 割込みコントローラに対する不正イベントが生成されます。

低消費電力モード

SRAM からコードを実行している場合の消費電力の最適化

- RUN/低消費電力RUNでの実行またはSLEEP / 低消費電力SLEEPの各モードではFlashクロックの供給を停止できる
  - Flashクロックはリセットおよびクロック･コントローラ（RCC）で設定する
  - Flashクロックはデフォルトで有効
- FlashメモリはSLEEP / 低消費電力SLEEPモードでパワーダウン･モードになるように設定できる
- FlashメモリはRUN / 低消費電力RUNモードでパワーダウン･モードになるように設定できる

life.augmented

21

コードを Flash メモリから実行しないようにすれば、Flash メモリの消費電力を低減できます。
RUN/低消費電力 RUN モードでは Flash クロックの供給を停止できます。また、SLEEP/低消費電力 SLEEP モードでも供給を停止するように設定できます。Flash クロックは、リセットおよびクロックコントローラで設定します。このクロックはデフォルトで有効です。
Flash メモリは、SLEEP/低消費電力 SLEEP モードでパワーダウン･モードになるように設定できます。
また、SRAM からコードを実行しているときに、RUN/低消費電力 RUN モードでパワーダウン･モードになるように設定することもできます。
クロックの供給を停止して Flash メモリをパワーダウン･モードにすることで、消費電力を大幅に低減できます。

低消費電力モード

モード	説明
RUN	アクティブ。 SRAMからコードを実行すればFlashクロックを無効にすることができ、Flashメモリはパワーダウン·モードになる。
SLEEP	アクティブ。ペリフェラル割込みによって、デバイスはSLEEPモードを終了する。 SLEEPモード中はFlashクロックを無効化できる。Flashメモリをパワーダウン·モードにすることができる。
低消費電力RUN	アクティブ。 SRAMからコードを実行すればFlashクロックを無効にすることができ、Flashメモリはパワーダウン·モードになる。
低消費電力SLEEP	アクティブ。ペリフェラル割込みによって、デバイスは低消費電力SLEEPモードを終了する。 低消費電力SLEEPモードではFlashクロックを無効化できる。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 / STOP 2	Flashクロックはオフ。ペリフェラルの各レジスタの内容は保持される。
STANDBY	パワーダウン状態。Flashメモリのインタフェースは、STANDBYモード終了後に再初期化する必要がある。
SHUTDOWN	パワーダウン状態。Flashメモリのインタフェースは、SHUTDOWNモード終了後に再初期化する必要がある。

life.augmented

22

RUN/低消費電力 RUN モードでは、Flash メモリはアクティブです。SRAM からコードを実行すれば Flash クロックを無効にすることができ、Flash メモリはパワーダウン·モードになります。
SLEEP/低消費電力 SLEEP モードでは、Flash クロックを無効にすることで Flash メモリをパワーダウン·モードに設定できます。
STOP 0、STOP 1、STOP 2 の各モードでは、Flash クロックはオフです。Flash インタフェースの各レジスタの内容は保持されます。
STANDBY/SHUTDOWN モードでは、Flash インタフェースのレジスタの内容は失われるので、このモードの終了後に再初期化する必要があります。

Flashメモリの性能

CoreMark/MHz

- ART Accelerator により、Flash メモリの性能はクロック周波数にほぼ正比例：3.40 CoreMark/MHz（キャッシュ有効、プリフェッチ無効）

		ART Accelerator 有効 （キャッシュ有効、プリフェッチ無効）
レンジ 1@ 48MHz （ウェイトステート2回）	消費電流（µA/MHz）（SMPS有効）	116
	性能（CoreMark/MHz）	3.40
	エネルギー効率（CoreMark/mA）	29
レンジ 2@ 8MHz （ウェイトステート1回）	消費電流（µA/MHz）（SMPS有効）	155
	性能（CoreMark/MHz）	3.43
	エネルギー効率（CoreMark/mA）	22

life.augmented

Flash メモリの性能は、ART アクセラレータを使用することで、クロック周波数にほぼ正比例します。命令キャッシュとデータキャッシュが有効、プリフェッチが無効な場合、CoreMark スコアは 48 MHz で 116 であり、これは 3.40 CoreMark/MHz に相当します。

Flashメモリの共有

- Flash メモリは Cortex-M4 と Cortex-M0+ の間で共有される
  - アクセス調停は ART によってラウンドロビン方式で処理される
    - 読出しとフェッチのアクセスは上書きと消去より優先される
    - 読出しアクセスは他のコアによるフェッチより優先される
- 共有時の性能
  - Cortex-M4 と Cortex-M0+ の両方に命令キャッシュとデータキャッシュがあるので影響はわずか

Cortex-M4	Cortex-M0+	ART Accelerator有効 （キャッシュ有効、プリフェッチ無効）	
@ 48MHz	@ 48MHz	Cortex-M4の性能（CoreMark/MHz）	3.40
		Cortex-M0+の性能（CoreMark/MHz）	2.40

life.augmented

Flash メモリは、Cortex-M4 と Cortex-M0+ の間で共有されます。両方の CPU が、Flash メモリを使用して命令を実行します。ART Accelerator により、Flash メモリの性能への影響は最小限に抑えられます。コードを同時実行する場合、Cortex-M0+ のクロック周波数が 48 MHz、命令キャッシュとデータキャッシュが有効、プリフェッチ・バッファが無効の条件で、Cortex-M4 の CoreMark/MHz は 48 MHz で 3.40 です。

Flashメモリの操作

- プログラムと消去の操作は電力レンジ1でのみ実行できる
- シングルバンクのみを使用できるので、Flashメモリのプログラムと消去の操作により、両方のCPUに対して Flashメモリからの実行はブロックされる
- Program Erase Suspend （PESD）により新しいFlashメモリ操作の開始をサスペンドできる
  - 実行中の操作は完了するまで続行される
  - PESDビットがクリアされるまで新しい操作はサスペンドされる
  - CPUごとに固有のPESDビットがある

life.augmented

Flash メモリのプログラムと消去の操作は電力レンジ 1 でのみ実行できます。レンジ 2 モードと低消費電力モードでは、Flash メモリのプログラムと消去の操作は禁止されています。
Flash メモリはシングルバンク･アーキテクチャなので、プログラムと消去の操作により、両方の CPU に対して実行がブロックされます。Flash メモリの操作がリアルタイムの CPU 性能に影響しないように、Flash メモリの操作をサスペンドできます。サスペンドがアクティブである限り、新しい操作が開始されることはないので、実行を確実に継続できます。サスペンドの前に有効になっていた実行中の Flash 操作は、完了するまで続行されます。各 CPU は、固有のサスペンド･レジスタのビットを使用して、Flash 操作のサスペンドを要求できます。

関連ペリフェラル

- 次のペリフェラルにリンクされている、ペリフェラルのトレーニングを参照
  - 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 および AIEC）
  - システム保護
  - Cortex-M0+セキュリティ

life.augmented

これは、Flash メモリに関連するペリフェラルのリストです。詳細については、必要に応じてこれらのペリフェラルのトレーニングを参照してください。

参考文書

- 詳細については、次の文書を参照してください
  - AN2606：STM32 マイクロコントローラ·システム·メモリ·ブート·モード - アプリケーションノート

life.augmented

詳細については、STM32 マイクロコントローラ·システムのメモリ·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。