STM32U5 マイクロコントローラシリーズのすべての製品に内蔵されている内蔵 Flash メモリのプレゼンテーションへようこそ。

Flash の機能

機能	STM32U5
最大サイズ*	最大4 MB
バンク数	2
ページサイズ	8 KB
読出しのデータバス幅	128 ビット
耐久性(プログラム/消去)	10 キロサイクル バンクあたり 256 KB で 100 キロサイクル
ワンタイムプログラミング	512 バイト
プリフェッチ	✓
バンクスワッピング	✓
デバイスのライフサイクル	✓ ライフサイクル:パスワードを使用して RDP の回帰を有効にすることが可能性

* 製品による

life.augmented

2

この表に、STM32U5 に搭載されている Flash の機能を示します。
Flash サイズは製品によってFlashサイズは最大4MBです。また、Flash には 512 バイトのワンタイムプログラミング領域も内蔵されています。
Flash 読出しデータバス幅は 128 ビットです。STM32U5 は、常にデュアルバンクアーキテクチャに対応しています。ユーザオプションバイトの SWAP-BANK オプションは、バンク 1 とバンク 2 のアドレスをスワップするのに使用されます。
そのため、STM32U5 は常に書込み中読出し機能（RWW）に対応しています。
最小の消去粒度を保証するページサイズは 8 KB です。
STM32U5 では耐久時間が長くなり、バンクあたり 256 KB で最大 100 キロサイクルとなっています。
また、Coretex-M33は、C-AHB バスの効率を高める読出しプリフェッチ・ユニットもサポートしています。
最後に、STM32U5 では読出し保護（RDP）を備えた柔軟性の高いライフサイクル方式を実装しており、パスワードを使用してレベル 2 からでも製品のデコミッショニングができる機能もサポートしています。

Flash 耐久性

すべて Flash メモリで 10 キロサイクルの耐久性

バンクあたり 256 KB（32 ページ）で 100 キロサイクル

任意の Flash ページを選択して、最大 100,000 サイクルとすることができます

サイクル数 10,000 回以上の Flash 領域のサイズをバンクごとに 256 KB に制限することは、アプリケーションで行われます

life.augmented

3

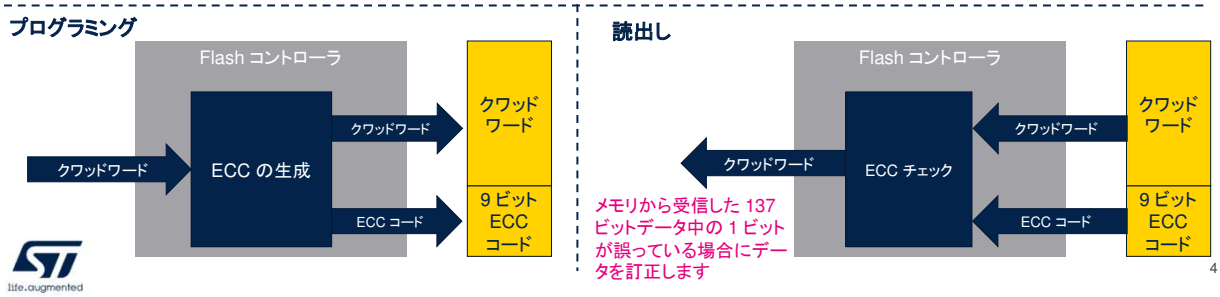
プログラム/消去操作により、Flash メモリセルが劣化することがあります。
プログラム/消去サイクルが累積して、メモリセルが機能しなくなり、メモリエラーの原因となることがあります。
耐久性とは、Flash メモリが信頼性に影響を与えることなくサポートできる消去/プログラミングシーケンスの最大数のことです。
バンクあたり 256 KB（32 ページ）では、耐久性が 100 KB に向上しており、通常、コード・ストレージよりも集中的なサイクル容量を必要とするデータ・ストレージに使用できます。
任意の Flash ページを選択して、10,000 サイクル以上、最大で 100,000 サイクルとすることができます。
サイクル数 10,000 回以上の Flash 領域のサイズをバンクごとに 256 KB に制限することは、アプリケーションで行われます。

Flash ECC

128 ビットデータラインに 9 ECC ビットを追加

ECC メカニズムのサポート内容:

- 1 つのエラー検出/訂正、とオプションの割込みあり
- 2 つのエラー検出、NMI 生成あり



Flash メモリのデータは 137 ビット幅です。128 ビットのクワッドワードごとに 9 ビットが追加されます。
ECC メカニズムは次のものをサポートしています。

- 1 つのエラー検出および訂正
- 2 つのエラー検出

1 つのエラーが検出されて訂正されると、Flash ECC レジスタで ECCC フラグ（ECC 訂正）がセットされます。割込みが生成できます。
2 つのエラーが検出されると、Flash ECC レジスタで ECCD フラグ（ECC 検出）がセットされます。この場合、NMI が生成されます。
エラーが検出されたアドレスとバンク番号はステータスレジスタにキャプチャされ、さらなる調査に使用できます。

Flash 読出しアクセスのレイテンシ

ウェイトステート（レイテンシ）	LPM = 0 の場合の HCLK 最大(MHz)			
	VCORE レンジ 1	VCORE レンジ 2	VCORE レンジ 3	VCORE レンジ 4
0 WS(1 CPU サイクル)	≤ 32	≤ 30	≤ 24	≤ 12
1 WS(2 CPU サイクル)	≤ 64	≤ 60	≤ 48	≤ 25
2 WS(3 CPU サイクル)	≤ 96	≤ 90	≤ 55	-
3 WS(4 CPU サイクル)	≤128	≤ 110	-	-
4 WS(5 CPU サイクル)	≤ 160	-	-	-
	LPM = 1 の場合の HCLK 最大(MHz)			
0 WS(1 CPU サイクル)	WS ≥ HCLK (MHz) / 10 -1			≤ 8
1 WS(2 CPU サイクル)				≤ 16
2 WS(3 CPU サイクル)				≤ 25
...				-
15WS(16CPU サイクル)				-

life.augmented

5

Flashメモリからデータを正しく読み取るには、CPU クロック（HCLK）の周波数とデバイス VCORE の内部電圧範囲に従って、ウェイトステートの数（レイテンシ）を正しくプログラムする必要があります。 ウェイトステートと CPU クロック周波数の対応を次の表に示します。
LPM：Flashアクセス制御レジスタ （FLASH_ACR）の LPM ビットを設定すると、Flashメモリは低電力読出しモードに対応します。

Flash プリフェッチ

- CM33 は、C バス 上で、また I-キャッシュを通じて命令とリテラルプール（定数/データ）をフェッチします。
  - C バス のアクセス効率を上げます。I-キャッシュが有効な場合、キャッシュのリフィル遅延が低減されます。
- プリフェッチは、シーケンシャルコードの場合に効率的です。
  - 現在の命令ラインが命令キャッシュに書き込まれて CPU によって実行されている間に、次の連続命令ラインを Flash メモリから読み出すことができます
- プリフェッチでは、Flash メモリアクセスの増加という犠牲を払って、コード実行性能を向上させる傾向があります
- 電力効率のために、プリフェッチを有効にすることを推奨します

life.augmented

Cortex-M33 では、C バス上で、また命令キャッシュが有効な場合はそれを通じて、命令とリテラルプール定数をフェッチします。
プリフェッチブロックは、キャッシュのリフィル遅延を低減することによって、命令キャッシュが有効なときの C バス アクセスの効率を向上させます。
プリフェッチは、シーケンシャルコードの場合に効率的です。 Flash メモリ内のプリフェッチにより、現在の命令ラインが命令キャッシュに書き込まれて CPU によって実行されている間に、次の連続命令ラインを Flash メモリから読み出すことができます。
プリフェッチを有効にするには、FLASH アクセス制御レジスタ（FLASH_ACR）のPRFTENビットをセットします。
PRFTEN は、Flash メモリのアクセスに 1 つ以上のウェイトステートが必要な場合のみセットする必要があります。
プリフェッチでは、Flash メモリアクセスの増加という犠牲を払ってコード実行性能を向上させる傾向があることに注意してください。
有効化すると電力消費に影響する可能性がありますが、性能が向上すると、電力効率が向上します。
性能指標の一部を次に示します。 メガヘルツあたりのコアマークで表されます。
I-キャッシュがオフでプリフェッチがオフの場合の性能は 2.2 です。
I-キャッシュがオフでプリフェッチがオンの場合の性能は 2.7 です。
これは、キャッシュミス時にプリフェッチにより性能が向上することを示しています。コアマークコードは完全に I-キャッシュにあるので（最初の繰り返し後はキャッシュミスすることはありません）、I-キャッシュが有効なとき、コアマークスコアへのプリフェッチの影響はありません。

STM32U575を使った場合：Flash 低消費電力モード

- バンクパワーダウン：バンクごとに 45µA を節約
  - パワーダウンモードでバンクにアクセスすると、バンクは自動的にウェイクアップします
  - バンクのウェイクアップには少なくとも 5 µs かかります
- SLEEP モード中の Flash パワーダウン：90 µA 節約できますが、ウェイクアップ時間は長くなります
- Flash 低消費電力モード：50 µA 節約できますが、読出し遅延は大きくなります

life.augmented

7

コードが Flash から実行されない場合、Flash メモリの消費電力を抑えることができます。
リセット後、両方のバンクは通常モードになります。消費電力を下げるため、各バンクを別々にパワーダウンモードにするには、PDREQ x ビットをセットします。
パワーダウンモードでバンクにアクセスすると、バンクは自動的にウェイクアップします。バンクのウェイクアップには少なくとも 5 µs かかります。
バンクのパワーダウンでは 45 マイクロアンペアの節約、SLEEP モードでのFlashのパワーダウンでは 90 マイクロアンペアの節約となります。
Flash アクセス制御レジスタ（FLASH_ACR）の LPM ビットをセットして低電力読出しモードを有効にすると、遅延は増加しますが、50 マイクロアンペア節約できます。

STM32U575を使った場合：メモリ 消去操作とプログラム操作

- セキュアでも非セキュアでも、すべての電圧範囲でプログラムおよび消去操作をサポートします
- ページ消去（8 KB）、バンク消去、または全体消去をサポートします
- 標準プログラミングモード：クワッドワードプログラミング（4 x 32 ビットデータ）
  - ECC が自動的に計算され、プログラム 137 ビットラインに追加されます
- バーストプログラミングモード：8 個のクワッドワードプログラミング
  - アドレスは 8 クワッドワードアドレス上に整列させる必要があります。
- プログラミングまたは消去操作中にシステムリセットした場合、動作ステータスレジスタを回復できます

life.augmented

8

読出し、プログラム、および消去操作は、すべての電圧範囲でサポートされます。
TrustZone が有効な場合、非セキュアソフトウェアは Flash の非セキュア部分へのアクセスのみが許可されます。
消去は、1 つのバンクまたは両方のバンクに対して、ページ単位の粒度で実行できます。後者の場合、全体消去と呼びます。
Flash コントローラは、次の 2 つのプログラミングモードを実装しています。
-シングルクワッドワード：ノーマルモードと呼ばれます。
- 8 つのクワッドワードで 128 バイトを表現：バーストモードと呼ばれます。
いずれの場合も、ECC コードが計算されてデータに追加されるので、実際には 137 ビットがプログラムされます。
160 MHz で 1 MB のプログラミングを行うには、通常モードで 7.7 秒、バーストモードで 3.1 秒かかります。
Flash メモリのプログラム／消去操作中にリセットされると、現在アクセス中の Flash メモリの内容は保証されません。
Flash メモリのプログラムまたは消去操作中にシステムリセットが発生した場合、Flash 動作ステータスレジスタから Flash メモリのステータスを回復できます。
Flash メモリのステータスを確認し、修正処置を行うことは、ソフトウェアで行われます。

タイミング：メモリ消去操作とプログラム操作

パラメータ	STM32U575/585
TTprog（137 ビット Flash ラインのプログラム時間）、バーストモード	48 µs
Tmass_erase （2バンク）	390 ms
Tpage_erase（耐久サイクル 10 キロサイクル）	1.5 ms

- HSI16 はプログラミングシーケンスで使用され、オフに設定されている場合は自動的に有効化されます
- Flashには、サイクル数によるプログラミング／消去パフォーマンスの損失を補う内部アルゴリズムがある
  → サイクル数に伴う時間の増加:
  - ページ消去時間の標準の増加：
    - 100 キロサイクル後に + 0.2 ms

life.augmented

このスライドでは、Flash のプログラムおよび消去操作に関するいくつかの指標を示します。
クワッドワード + ECC コードをプログラムする時間は、バーストモード使用時で 48 マイクロ秒です。
2 つのバンクを完全に消去するための時間は 390 ミリ秒です。
耐久サイクル 10 キロサイクルを想定して、1 ページを消去するための時間は 1.5 ミリ秒です。
内部アルゴリズムによって消去シーケンスが管理されます。
消去時間は、耐久サイクル数が増加すると増加します。100 キロサイクルでページを消去する場合、一般的に 0.2 ミリ秒の追加時間が必要です。
内部 16 メガヘルツオシレータ HSI16 は、事前に有効化されている場合を除き、消去またはプログラミングシーケンスが開始されると自動的に有効になり、このシーケンスが完了すると自動的に無効になります。

Flash の TrustZone サポート

- TrustZone はオプションバイトで有効化され、RDP 1→0 の回帰により無効化されます
- ウォーターマークベースのセキュア Flash メモリ保護領域
  - バンクごとに 1 つあり、ページ単位の粒度を持ち、オプションバイトで定義されます
- セキュア領域のセキュア非表示保護領域(HDP)の一部
  - バンクごとに 1 つあり、ページ単位の粒度を持ち、オプションバイトで定義されます
  - ACCDIS ビットがセットされた場合:すべてのアクセスが拒否され、システムリセットでのみクリアされる
  - ACCDIS ビットがセットされた場合: HDP ゾーンでこれ以上操作できなくなります（サイズ/R/W/消去）
  - システムリセットでのみクリアされます

life.augmented

10

TrustZone セキュリティが有効な場合、Flash メモリの一部を非セキュア読出しおよび書込みアクセスから保護することができます。
TrustZone の無効化は、読出し保護（RDP）がレベル 1 からレベル 0 に変更されるときにのみ可能です。
最大 2 つの異なる不揮発性セキュア領域はオプションバイトで定義でき、セキュアアクセスにより、ページ単位の粒度を使用してバンクあたり 1 つの領域でのみ読出し/書込みができます。
これらはそれぞれ、同じ開始ページオフセットで始まり、プログラム可能な終了ページオフセットで終了するセキュア非表示保護領域に対応しています。
セキュア非表示保護領域の内容は、対応する HDP_ACCDIS ビットが 1 にセットされた後、アクセス不可としてマークされます。
これは、Flash の一部へのその後のアクセスを防止するために使用され、セキュアブートコードとデータをセキュアおよび非セキュアアプリケーションコードから隔離するために使用されます。

FLASH スレッドの隔離

4 つの隔離された世界：S/P S/NP NS/P NS/NP

- ページ単位の粒度を備えたブロックベースのセキュアな特権 Flash メモリの保護
  - 8 KB の各ページは S/NS および P/NP（揮発性設定）とすることができます
- セキュアレジスタ（SPRIV）と非セキュアレジスタ（NSPRIV）の個別の特権設定
  - STM32U5 の新機能
- 4 つの隔離された世界の象限を設定可能：S/P S/NP NS/P NS/NP

セキュア + 特権	非セキュア + 特権
セキュア + 非特権	非セキュア + 非特権

life.augmented

11

Flash インタフェースの専用セキュアレジスタ FLASH_SEC1BBR1 ~ 8 および FLASH_SEC2BBR1 ~ 8 を使用して、任意の Flash ページをセキュア/非セキュアとして設定できます。
リセット時に、これらのレジスタはクリアされます（非セキュア）。
すでにセキュアウォーターマーク領域に属しているページは、ブロックベースのビット設定に関係なく、セキュアになります。
各セキュリティ ドメインで、各 Flash ページの特権レベルは、FLASH_PRIVBB1Rx（x=1 ～ 8）および FLASH_PRIVBB2Rx（x=1 ～ 8）レジスタを使用して、特権レベルを非特権または特権のいずれかにプログラムできます。
これにより、隔離された世界の 4 つの四分円が得られます。
- セキュア特権
- セキュア非特権
- 非セキュア特権
- 非セキュア非特権

Flash のその他の保護

デバイスのライフサイクル管理が向上

レベル 1 からレベル 0 への RDP 回帰を許可する OEM1KEY
レベル 2 からレベル 1への RDP の回帰を許可する OEM2KEY
プロビジョニングされたキーがない場合、従来の RDP 遷移
詳細については、セキュリティトレーニングを参照してください

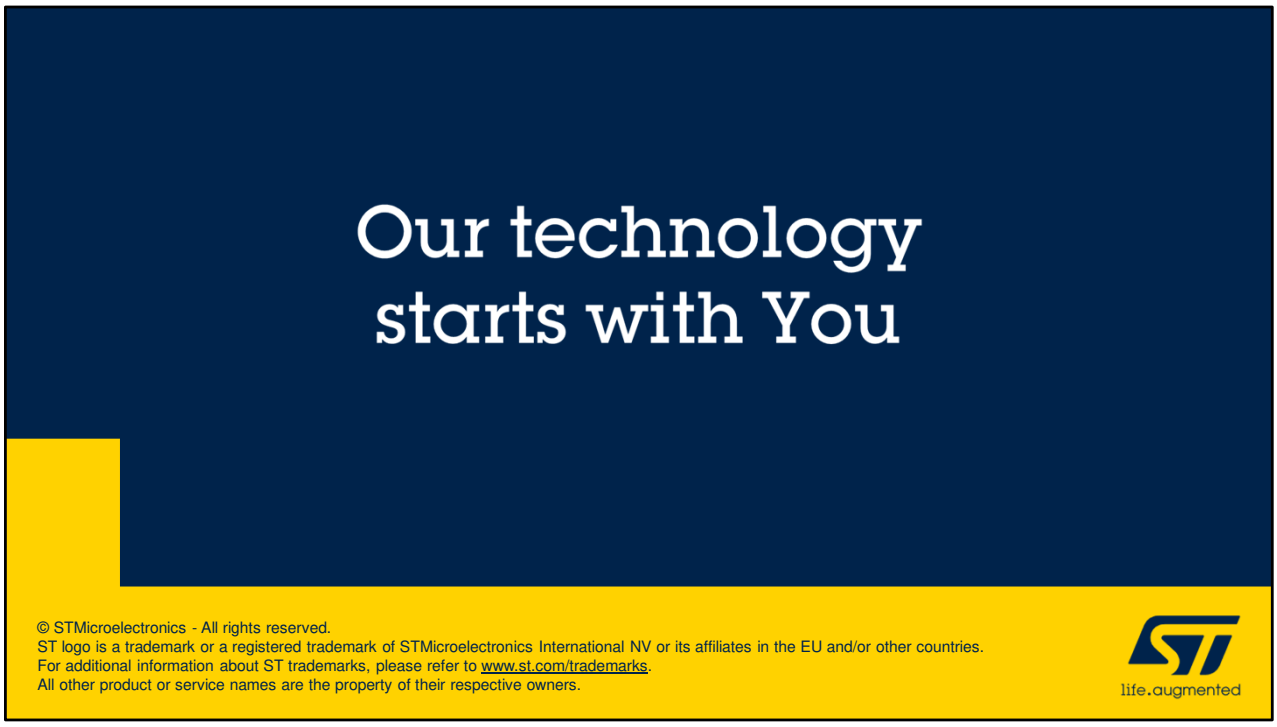
書込み保護領域

バンクごとに 2 つあり、ページ単位の粒度を持ち、オプションバイトで定義されます
書込み保護ロック
- いったんセットすると、アンロックするには L0 への RDP の回帰が必要となります

life.augmented

12

RDP ステートマシンに関しては、STM32U5 では、OEM1/OEM2 ロック有効化という新機能が実装されています。
2 つの 64 ビットキー OEM1KEY および OEM2KEY を定義することにより、レベル 1 からの RDP の回帰をロックしたり、レベル 2 からの回帰を許可することができます。
各 64 ビットキーは 2 つのレジスタでコード化されます。
OEM1KEY および OEM2KEY をこれらのレジスタから読み出すことはできません。
RDP レベル 1 から RDP レベル 0 に回帰するには、デバッガで正しい OEM1 キー値を提供する必要があります。
RDP レベル 1 から RDP レベル 0.5 に回帰するには、デバッガで正しい OEM2 キー値を提供する必要があります。
RDP レベル 2 から RDP レベル 1 に回帰するには、デバッガで正しい OEM2 キー値を提供する必要があります。
これらのキーがプロビジョニングされていない場合、STM32U5 では 、従来の遷移のみが実装されます。RDP がレベル 2 にセットされ、OEM2 キーがプロビジョニングされない場合、JTAG と SWD は完全に無効化されます。OEM2 キーがプロビジョニングされた場合、JTAG と SWD はリセット時に有効なままでデバイス識別の取得のみを行い、OEM2 キーを提供して RDP 回帰をリクエストします。
デバイスのライフサイクルの詳細については、セキュリティトレーニングを参照してください。
バンクごとに 2 つ、合計 4 つの書込み保護領域がサポートされます。
書込み保護領域へのプログラム/消去操作は禁止されています。結果として、領域が 1 つ書込み保護されているとソフトウェアの全体消去が実施できません。
各領域は、物理的なフFlashバンクベースアドレスに関連する開始ページオフセットと終了ページオフセットにより定義されます。書込み保護領域は、それぞれ独立してロックできます。この場合、領域設定を変更することはできず、RDP がレベル 0 に回帰した場合にのみアンロックできます。
書込み保護属性は、セキュアおよび HDP 設定とは無関係です。



ありがとうございました。