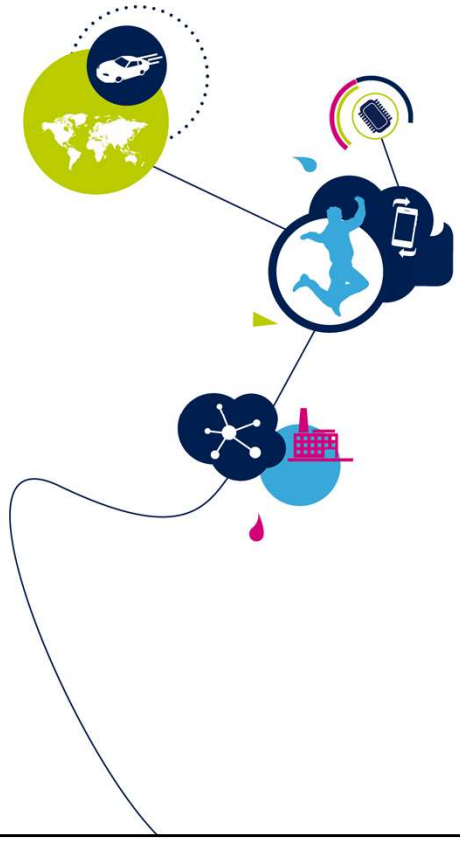
STM32MP1 – BSEC

ブートおよびセキュリティ・コントローラ
1.0 版



life.augmented

STM32MP1 ブートおよびセキュリティ・コントローラのプレゼンテーションにようこそ。

概要

- BSEC は、オンチップの 1 度だけプログラム可能な（OTP）ビットの読出し、プログラム、アクセス制御を目的としています。
- 3Kbit の有効な OTP エリアは、異なるプロパティを持つ 2 つの領域に整理されています。
  - 下位 OTP エリア：1Kbit、2:1 の冗長性、インクリメンタル・ビット・プログラミング
  - 上位 OTP エリア：2Kbit、ECC 保護、ワード・プログラミングのみ
- OTP エリアは、不揮発性情報を格納するために使用します。
  - 製造データ（メモリ・リペア、アナロ・グトリミング、チップ ID など）
  - デバッグ・アクセスとデバイス・プロビジョニングを制御するデバイスのライフサイクル情報
  - ブート設定
  - キーおよびセキュリティ機密情報（ST 秘密鍵および OEM 機密情報）

life.augmented

ブートおよびセキュリティ・コントローラは、オンチップの 1 度だけプログラム可能な（OTP）ビットの読出し、プログラム、アクセス制御を目的としています。

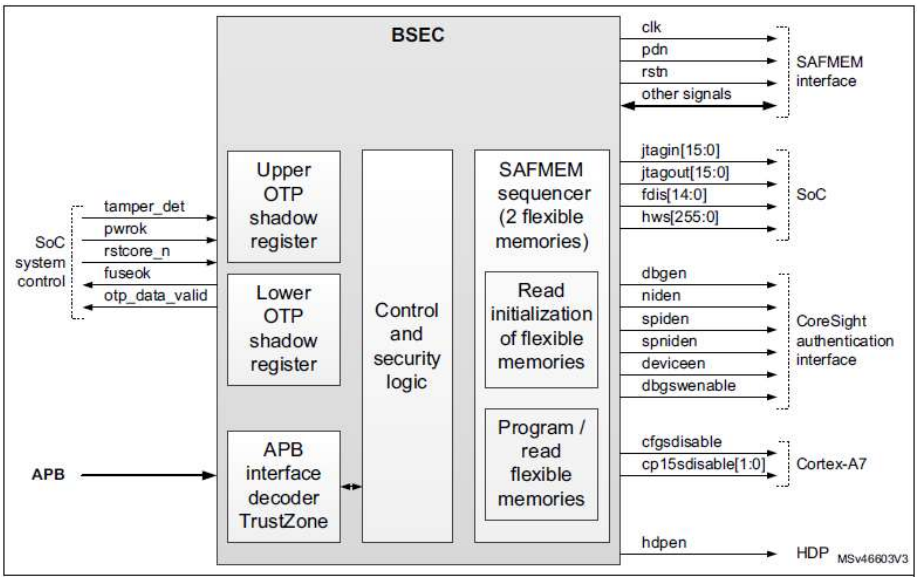
3Kbit の有効な OTP エリアは、異なるプロパティを持つ 2 つの領域に整理されています。

- 下位 OTP エリア：1Kbit、2:1 の冗長性、インクリメンタル・ビット・プログラミング
- 上位 OTP エリア：2Kbit、ECC 保護、ワード・プログラミングのみ

OTP エリアは、不揮発性情報を格納するために使用します。

- 製造データ（メモリ・リペア、アナログ・トリミング、チップ ID など）
- デバッグ・アクセスとデバイス・プロビジョニングを制御するデバイスのライフサイクル情報
- ブート設定
- キーおよびセキュリティ機密情報（ST 秘密鍵および OEM 機密情報）

BSEC ブロック図



これは、ブートおよびセキュリティ・コントローラの簡略化されたブロック図です。
SAFMEM は、下位 OTP エリアと上位 OTP エリアの 2 つの領域に分けられたヒューズ・ボックスで、それぞれ 1Kbit（ビット・プログラム可能）と 2Kbit（ワード・プログラム可能）となっています。
制御ロジックは、OTP ビットの読出しとプログラムをサポートしています。
OTP ビットはリセット時にシャドウ・レジスタに読み出されます。
複数の有効化信号が SoC にエクスポートされます。
シャドウ・レジスタのアクセスと有効化信号の値は、最初のワードによって決まるデバイスのライフサイクル状態に条件付けされます。

主な機能(1/2)

- 32bit APB4 インタフェース
- 4096 個の OTP ビット(3072 個の有効ビット)
- スティッキー・ビットによるグローバル・プログラム・ロック
- ワードごとの永久的な OTP プログラム・ロック
- ブート・フェーズ中のスティッキー・ビットによる OTP ワード・プログラム・ロック
- ブート・フェーズ中のスティッキー・ビットによるシャドウ OTP レジスタの個別書込みロックが可能
- 再ロードを防止するために、ブート・フェーズ中のスティッキー・ビットによるシャドウ OTP レジスタの個別読出しロックが可能

life.augmented

BSEC の主な機能は次の通りです。

- 32bit APB4 インタフェース
- 下位 OTP では 2:1 の冗長性であるため、4096 個の元 OTP ビット(= 3072 個の有効ビット)
- スティッキー・ビットによるグローバル・プログラム・ロック
- ワードごとの永久的な OTP プログラム・ロック
- ブート・フェーズ中のスティッキー・ビットによる OTP ワード・プログラム・ロック
- ブート・フェーズ中のスティッキー・ビットによるシャドウ OTP レジスタの個別書込みロックが可能
- 再ロードを防止するために、ブート・フェーズ中のスティッキー・ビットによるシャドウ OTP レジスタの個別読出しロックが可能

主な機能(2/2)

- ブート・パラメータを格納するために外部エージェントと通信するための BSEC スクラッチ・レジスタ
- JTAG TAP コントローラへの通信チャネルとしての BSEC_JTAGIN および BSEC_JTAGOUT レジスタを経由した JTAG SOC インタフェース
- OTP ワード値を認定するための妨害チェックにより、OTP 読出し中のクロックやパワー・グリッチによるハードウェア攻撃への耐性を改善

life.augmented

その他の主な機能は次の通りです。

- ブート・パラメータを格納するために外部エージェントと通信するための BSEC スクラッチ・レジスタ
- JTAG TAP コントローラへの通信チャネルとしての BSEC_JTAGIN および BSEC_JTAGOUT レジスタを経由した JTAG SOC インタフェース
- OTP ワード値を認定するための妨害チェックにより、OTP 読出し中のクロックやパワー・グリッチによるハードウェア攻撃への耐性を改善

OTP マッピング

6

- OTP ワードとビット・フィールドのリスト
- OTP プログラミング（ST またはユーザ）
- 出荷時にプログラムされる完全ロックワード
- BOOT ROM によって制御され、デバイスのライフ・サイクルに応じてセットされるスティッキー・ロック属性

** 詳細については、製品のリファレンス・マニュアルの OTP マッピングのセクションを参照してください。

life.augmented

OTP マップは、次のものを記述しています。

- OTP ワードとビット・フィールドのすべてのリスト
- OTP ワードをプログラムできる人物に関する情報（STマイクロエレクトロニクス またはユーザ）
- ワードが出荷時にプログラムされたもので完全にロックされている場合（アナログ・トリミングやメモリ・リペアなど）
- BOOT ROM によって制御され、デバイスのライフ・サイクルに応じてセットされるスティッキー・ロック・ビット（OTP ワードごとに 3 個のスティッキー・ビット）：シャドウ書込みロック、シャドウ再ロード・ロック、シャドウ・プログラム・ロック）

詳細については、製品のリファレンス・マニュアルの OTP マッピングのセクションを参照してください。

下位 OTP マッピング

- 32ワード、2:1 の冗長性付きビット・プログラム可能
- 使用目的:
  - デバイスのライフ・サイクルおよび SoC の機能(ST)
  - ブート・デバイス選択およびユーザ設定(ユーザ)
  - ハードウェア設定(ST)出荷時トリミング・ビット、メモリ・リペアなど
  - 製品固有の設定(ユーザ)BOR 閾値、IWDG の動作など
  - 公開鍵ハッシュ

life.augmented

下位 OTP エリアはビット・プログラムのみ可能な 32ワードで、2:1 の冗長性が備わっています。以下の目的で使用します。

- ワード 0～2:CFG0～CFG2 は、STMicroelectronics によって予約済みであり、ライフ・サイクルや製品で有効化される SoC の機能を制御します。CFG0 から 1bit だけ、シークレット・プロビジョニング後にデバイスを終了するためにユーザがアクセスできます。
- ワード 3～7 は、ブート・デバイス選択を定義するために使用できます。
- ワード 16～24 はハードウェア設定に使用されます。
- ワード 16 には、ユーザの製品固有の設定が含まれます。
- ワード 24～31 は公開鍵ハッシュに使用されます。

上位 OTP マッピング

- 64ワード、固有の ECC 保護でのワードプログラムのみ可能
- 使用目的:
  - SSP の ST ECDSA プライベートおよび ST パブリック ECDSA 証明書(ST)
  - MAC アドレス(ユーザ)
  - RMA パスワード(ユーザ)
  - ボード情報(ユーザ)
  - 残りのワードは、ユーザからの不揮発性のキーや機密情報の格納に使用できます。

life.augmented

上位 OTP エリアは ECC 保護でプログラムのみ可能な 64ワードで、次の目的で使用します。

- SSP の ST ECDSA プライベートおよび ST パブリック ECDSA 証明書(ST)
- MAC アドレス(ユーザ)
- RMA パスワード(ユーザ)
- ボード情報(ユーザ)
- 残りの 36ワードは、ユーザからの不揮発性のキーや機密情報の格納に使用できます。

OTP セキュリティ

- BSEC は、TrustZoneに対応しており、次の 3 つのレジスタ領域に応じた条件付きアクセスを行います。
  - BSEC 制御レジスタ
  - 下位 OTP シャドウ・レジスタ
  - 上位 OTP シャドウ・レジスタ
- 読出しおよび書込みの許可は OTP モードに応じて決まります。

書込みアクセス許可と領域

OTP mode	Control registers(1)		Lower OTP shadow registers		Upper OTP shadow registers	
	APB secure	APB non-secure	APB secure	APB non-secure	APB secure	APB non-secure
OTP-SECURED	Yes	No	Yes	No	Yes	No
OTP-INVALID	No	No	No	No	No	No

読出しアクセス許可と領域

OTP mode	Control registers(1)		Lower OTP shadow registers		Upper OTP shadow registers	
	APB secure	APB non-secure	APB secure	APB non-secure	APB secure	APB non-secure
OTP-SECURED	Yes	Yes	Yes	Yes	Yes	No
OTP-INVALID	Yes	No	No	No	No	No

BSEC は、TrustZoneに対応しており、次の 3 つのレジスタ領域に応じた条件付きアクセスを行います。

- BSEC 制御レジスタ
- 下位 OTP シャドウ・レジスタ
- 上位 OTP シャドウ・レジスタ

領域ごとに、読出しおよび書込みの許可が OTP モードに応じて決まります。

BSEC OTP モード

- デバイスのライフ・サイクルは、OTP ワード 0 で制御されます。
- デバイス製造後の関連する状態だけをここに示します。

	BSEC_OTP_DATA0 [6:0]	OTP mode	BSEC_OTP_STATUS SECURE	BSEC_OTP_STATUS FULLDBG	BSEC_OTP_STATUS INVALID
オープン・デバイス	0xxx1x1	OTP-SECURED open_device	1	0	0
	01x1xxx				
	0xx11xx				
	01xxxx1				
クローズ・デバイス	1xxx1x1	OTP-SECURED closed_device	1	0	0
	11x1xxx				
	1xx11xx				
	11xxxx1				
	All other values	OTP-INVALID	x	x	1

この表は、デバイスのライフ・サイクルの簡略化された図を示しています。
機密情報が製造中に OTP ワードにプロビジョニングされると、デバイス状態が OTP-SECURED にセットされます。
オープン・デバイスからクローズ・デバイスへの移行は、後で OTP ワード 0 のビット 6 を「1」にプログラムして制御されます。
OTP ヒューズまたはワード 0 が漏洩された場合、デバイスは OTP-INVALID 状態にセットされ、OTP の機密情報を保護する「寿命」状態となります。

BSEC とシステム・リセット

- システム・リセット時、BSEC は自動的にすべてのシャドウ・レジスタを更新します。
- OTP モードはこのフェーズで決まります。
- BSEC_OTP_STATUS、BSEC_OTP_DISTURBED、BSEC_OTP_ERROR のレジスタも更新されます。
- **fuseok** 信号は、このフェーズの最後にアサートされます。この信号は SoC にリセットをリリースするために使用されます。

life.augmented

システムリセット時、BSEC は自動的にすべてのシャドウ・レジスタを更新します。

OTP モードはこのフェーズで決まります。

BSEC_OTP_STATUS、BSEC_OTP_DISTURBED、BSEC_OTP_ERROR のレジスタも更新されます。

fuseok 信号は、このフェーズの最後にアサートされます。この信号は SoC にリセットをリリースするために使用されます。

OTP 読出し

- 読出し動作を起動するには、ソフトウェアを使って ADDR フィールドで指定されたワード数で BSEC_OTP_CONTROL レジスタをセットし、PROG ビットを 0 にセットする必要があります。
- ソフトウェアで BSEC_OTP_STATUS レジスタの BUSY ビットをチェックできます。この BUSY ビットがクリアされると、読出し動作が完了したことを示します。
- 読出し動作が終了したら、BSEC ステート・マシンが「中断」および「エラー」ステータスのレジスタを更新します。
- OTP の内容に依存する BSEC パラメータも、対応する OTP ワードが読み出されると更新されます。ワード 0 の読出し動作が実行されると、OTP モードが更新されます。

life.augmented

読出し動作を起動するには、ソフトウェアを使って ADDR フィールドで指定されたワード数で BSEC_OTP_CONTROL レジスタをセットし、PROG ビットを 0 にセットする必要があります。

ソフトウェアで BSEC_OTP_STATUS レジスタの BUSY ビットをチェックできます。この BUSY ビットがクリアされると、読出し動作が完了したことを示します。

読出し動作が終了したら、BSEC ステート・マシンが「中断」および「エラー」ステータスのレジスタを更新します。

OTP の内容に依存する BSEC パラメータも、対応する OTP ワードが読み出されると更新されます。ワード 0 の読出し動作が実行されると、OTP モードが更新されます。

OTP プログラミング

- OTP ワードは複数のステップで書き込むことができます。ワード値は、ビットに 1 を加えて更新できますが、すでに 1 にセットされているビットを 0 に書き戻すことはできません。
- プログラミング動作を起動するには、次の 2 つのステップが必要です。
  - ワード値を BSEC_OTP_WRDATA レジスタに書き込みます。
  - BSEC_OTP_CONTROL レジスタに次のものを書き込みます。
    - ADDR フィールドのワード数
    - PROG ビットを 1 にセット
    - LOCK ビットを 0 にセット
- ソフトウェアで BSEC_OTP_STATUS レジスタの BUSY ビットをチェックします。この BUSY ビットがクリアされると、書込み動作が完了したことを示します。
- 同じレジスタで、書込み動作が失敗した場合、PRGFAIL ビットがセットされます。

life.augmented

OTP ワードは複数のステップで書き込むことができます。ワード値は、追加ビットを「1」のみにセットすることで更新できます。すでに 1 にセットされたビットは、0 にリセットできません。
プログラミング動作を起動するには、次の 2 つのステップが必要です。
ワード値を BSEC_OTP_WRDATA レジスタに書き込みます。
BSEC_OTP_CONTROL レジスタに次のものを書き込みます。
ADDR フィールドのワード数
PROG ビットを 1 にセット
LOCK ビットを 0 にセット
ソフトウェアで BSEC_OTP_STATUS レジスタの BUSY ビットをチェックします。この BUSY ビットがクリアされると、書込み動作が完了したことを示します。
同じレジスタで、書込み動作が失敗した場合、PRGFAIL ビットがセットされます。

デバッグおよび DFT 制御

- BSEC は、デバイスのライフ・サイクル状態に応じてデバッグ・アクセスを実行しています。
- BSEC_DENABLE レジスタは、CoreSight 認証インタフェースと特定の制御信号を含む、SoC へのハードウェア信号を駆動しています。

Signal	OTP-SECURED open_device	OTP-SECURED closed_device	OTP-INVALID	Comment
dbgen	1	0	0	CoreSight authentication
niden	1	0	0	CoreSight authentication
spiden	0	0	0	CoreSight authentication
spniden	0	0	0	CoreSight authentication
deviceen	1	0	0	CoreSight authentication
dbgswenable	0	0	0	CoreSight authentication
hdpen	0	0	0	Hardware debug port tracing
cfgsdisable	0	0	0	Disable some of Cortex®-A7 GIC secure access
cp15sdisable[1:0]	0b00	0b00	0b00	Disable some of Cortex®-A7 CP15 secure access

life.augmented

** 詳細については、製品のリファレンスマニュアルの BSEC デバッグ制御のセクションを参照してください。

ブートおよびセキュリティ・コントローラは、デバイスのライフ・サイクル状態に応じてデバッグ・アクセスを制御しています。

BSEC_DENABLE レジスタは、CoreSight 認証インタフェースと特定の制御信号を含む、SoC への複数のハードウェア信号を駆動しています。

詳細については、製品のリファレンス・マニュアルの BSEC デバッグ制御のセクションを参照してください。