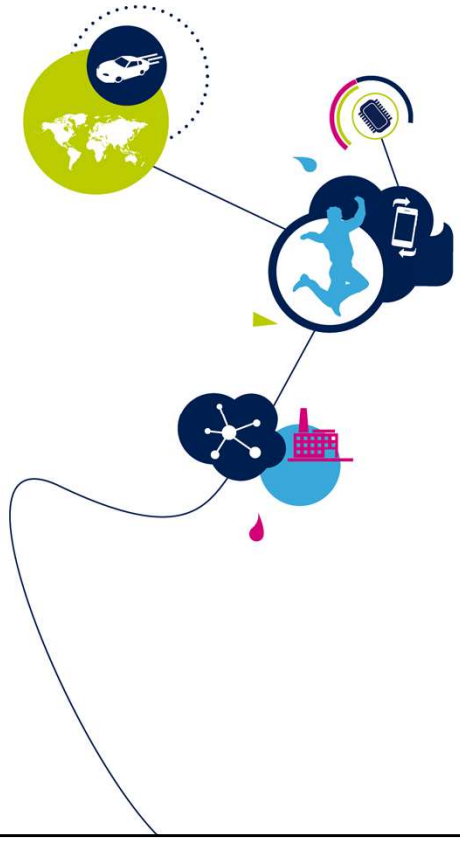
STM32MP1 – SECOVR

セキュリティアーキテクチャの概要
1.0 版



life.augmented

STM32MP1 セキュリティアーキテクチャの概要のプレゼンテーションにようこそ。

概要

- STM32MP1 セキュリティアーキテクチャは、Arm® TrustZone® 技術をベースとしている。
- TrustZone は、2 つの実行環境（セキュアワールドとノーマル非セキュアワールドという名前）にリソースを分ける。
- Cortex® A7 はセキュリティ拡張を備えた Armv7-A アーキテクチャをサポートしている。これは分けられた環境のルートにある。
- SoC 相互接続セキュリティゲート（別名スタブ）はさまざまなレベル（AHB と AHB2APB のブリッジレベル）の許可をチェックし、セキュリティの影響を受けやすいリソースへの無許可アクセスをブロックする。
- TrustZone メモリアダプタ（TZMA）は、セキュア／非セキュアにおけるオンチップ RAM/ROM の 4KB の倍数での分割をサポートしている。
- TrustZone アドレス空間コントローラ（TZC）は、セキュア／非セキュアアクセスを備えた領域への DDR アドレス範囲の分類をサポートしている。
- セキュリティの影響を受けやすいリソース（TrustZone 認識）はローカルアクセス制御を備えている。

life.augmented

STM32MP1 セキュリティアーキテクチャは、Arm TrustZone® 技術をベースとしています。

Arm TrustZone は、2 つの実行環境（セキュアワールドとノーマル非セキュアワールドという名前）にリソースを分けます。

Cortex A7 はセキュリティ拡張を備えた Armv7-A アーキテクチャをサポートしています。これは分けられた環境のルートにあります。

SoC 相互接続機能セキュリティゲート（別名スタブ）は SoC 相互接続のさまざまなレベル（AHB バスと AHB2APB のブリッジレベル）の許可をチェックし、セキュリティの影響を受けやすいリソースへの無許可アクセスをブロックします。

TrustZone メモリアダプタ（TZMA）は、セキュア／非セキュア領域でのオンチップ RAM/ROM メモリの 4KB 単位分割をサポートしています。

TrustZone アドレス空間コントローラ（TZC）は、セキュア／非セキュアアクセスを備えた領域への DDR アドレス範囲の分類をサポートしています。

セキュリティの影響を受けやすいリソース（TrustZone 認識）はローカルアクセス制御を備えています。

セキュリティコンポーネントと分類

3

- TrustZone 対応 IP:
  - セキュリティ拡張を備えた Cortex-A7 サブシステム(L1 および L2 キャッシュ、MMU、GIC を含む)
  - チャネルごとのセキュリティを実装した MDMA
  - DAP:認証インタフェースでデバッグを安全に保つデバッグアクセスポート
- セキュア IP:
  - 無条件セキュアまたは書込みセキュア
- セキュリティ保護可能 IP:
  - ETZPC でセキュア、書込みセキュア、非セキュアにプログラムできるペリフェラルおよびオンチップメモリ
- TrustZone 認識 IP
  - セキュアにするローカルの機能をいくつか備えたセキュリティの影響を受けやすいペリフェラル
- 非セキュア IP
- メモリアダプタ(TZMA)
  - SYSRAM メモリおよび ROM メモリをセキュア領域と非セキュア領域にセグメント化
- TZC(DDR)
  - DDR メモリを複数の領域にセグメント化、セキュア/非セキュア権限あり、非セキュア領域は NSAID によってマスタごとにフィルタされる場合があることに注意

life.augmented

コンポーネントのセキュリティプロパティは次のように列挙できます。

TrustZone 対応 IP:

- セキュリティ拡張を備えた Cortex-A7 サブシステム(L1 および L2 キャッシュ、MMU、GIC を含む)
- チャネルごとのセキュリティを実装した MDMA
- DAP:認証インタフェースでデバッグを安全に保つデバッグアクセスポート

セキュア IP:

- 無条件セキュアまたは書込みセキュア

セキュリティ保護可能 IP:

- ETZPC でセキュア、書込みセキュア、非セキュアにプログラムできるペリフェラルおよびオンチップメモリ

TrustZone 認識 IP

- セキュアにするローカルの機能をいくつか備えたセキュリティの影響を受けやすいペリフェラル

非セキュア IP

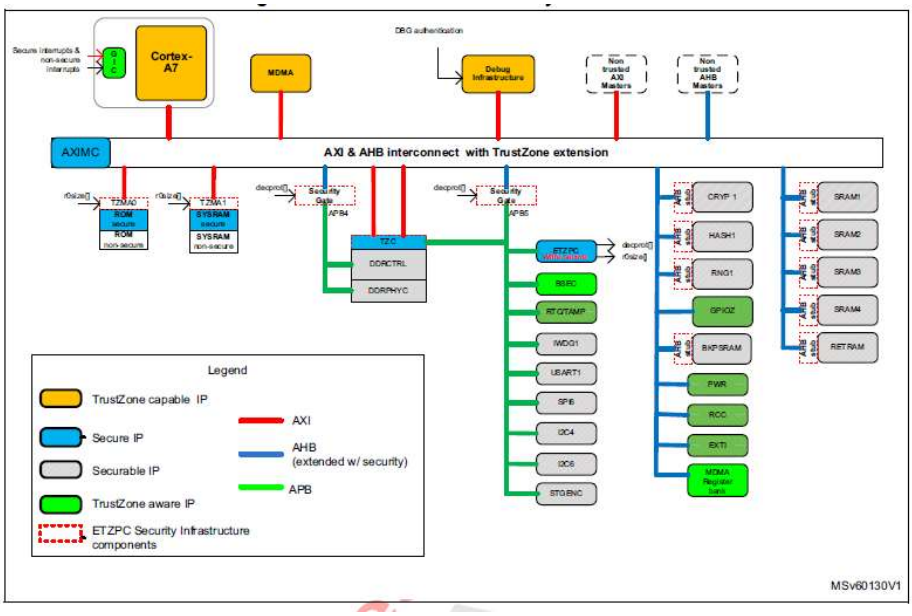
メモリアダプタ(TZMA)

- SYSRAM メモリおよび ROM メモリをセキュア領域と非セキュア領域にセグメント化

TZC(DDR)

- DDR メモリを複数の領域(セキュア/非セキュア権限あり)にセグメント化。非セキュア領域は NSAID によってマスタごとにフィルタされる場合があることに注意

STM32MP1 セキュリティアーキテクチャ



これは、STM32MP1 セキュリティアーキテクチャのブロック図です。
主なコンポーネントは次の通りです。

- ETZPC、ETZC、AXIMC といった無条件セキュアのセキュア IP
- ROM および SYSRAM でセキュア領域の定義に使用される TZMA0 および TZMA1
- セキュリティ保護可能 IP：これらの IP のセキュリティは ETZPC で定義
- TrustZone 認識 IP：BSEC、RTC/TAMP、MDAM、PWR、RCC、EXTI、GPIOZ

セキュリティルール

5

- セキュアワールドによる非セキュアリソースへのアクセスは常に可能。
- 非セキュアワールドがセキュアリソースへのアクセスを試みた場合、アクセスは不正となる。
- 不正アクセスのエラー動作：
  - 不正アクセスは常に拒否、書込みアクセスは無視、読出しアクセスでは 0 が返る。
  - エラーをフラグするオプションは、サイレントフェイル、バスエラー、割込みのいずれか。
- デフォルト設定
  - 独自のルールは無いが、IP はデフォルトではほぼ非セキュア。
  - TZ 認識 IP については、IP の説明を参照。
  - セキュリティ保護可能 IP および TZMA は、デフォルトでは不正アクセス時にバスエラーを応答するセキュアな状態。

life.augmented

セキュアワールドによる非セキュアリソースへのアクセスは常に可能です。

非セキュアワールドがセキュアリソースへのアクセスを試みた場合、アクセスは不正となります。

不正アクセスのエラー動作は次の通りです。

- 不正アクセスは常に拒否されます。書込みアクセスは無視され、読出しアクセスでは 0 が返されます。
- エラーをフラグするオプションは、サイレントフェイル、バスエラー、割込みのいずれかになります。

デフォルト設定は次の通りです。

- 独自のルールはありませんが、IP はデフォルトではほぼ非セキュアです。
- TZ 認識 IP については、IP の説明を参照してください。
- セキュリティ保護可能 IP および TZMA は、デフォルトでは不正アクセス時にバスエラーを応答するセキュアな状態です。

セキュリティ保護可能ペリフェラル

- セキュリティ保護可能ペリフェラルは、ETZPC DECPROT ビットで制御される。
- DECPROT[1:0] ビットは次のようにエンコードされる。
  - 0b00：セキュア
  - 0b01：書込みセキュア
  - 0b11：非セキュア
- 注：0b10 は予約済みか、MCU の制御に使用される。

（ETZPC OLT トレーニングを参照）

life.augmented

セキュリティ保護可能ペリフェラルは、ETZPC DECPROT ビットで制御されます。

DECPROT[1:0] ビットは次のようにエンコードされます。

- 0b00：セキュア
- 0b01：書込みセキュア
- 0b11：非セキュア

注：0b10 は予約済みか、MCU の制御に使用されます。

セキュリティ保護可能 IP と ETZPC DECPROT

#	decprot bits	IP	BUS	default	bus mast…	type	attributes
0	DECPROT0[1:0]	STGENC	APB5	0b00		1	securable
1	DECPROT0[3:2]	BKPSRAM	AHB5	0b00		1	securable
2	DECPROT0[5:4]	IWDG1	APB5	0b00		1	securable
3	DECPROT0[7:6]	USART1	APB5	0b00		1	securable
4	DECPROT0[9:8]	SPI6	APB5	0b00		1	securable
5	DECPROT0[11:10]	I2C4	APB5	0b00		1	securable
7	DECPROT0[15:14]	RNG1	AHB5	0b00		1	securable
8	DECPROT0[17:16]	HASH1	AHB5	0b00		1	securable
9	DECPROT0[19:18]	CRYP1	AHB5	0b00		1	securable
10	DECPROT0[21:20]	DDRCTRL	APB4	0b00		1	securable
11	DECPROT0[23:22]	DDRPHYC	APB4	0b00		1	securable
12	DECPROT0[25:24]	I2C6	APB5	0b00		1	securable

#	decprot bits	IP	BUS	default	bus mast…	type	attributes
80	DECPROT5[1:0]	SRAM1	MLAHB	0b11		3	securable and MCU isolation support
81	DECPROT5[3:2]	SRAM2	MLAHB	0b11		3	securable and MCU isolation support
82	DECPROT5[5:4]	SRAM3	MLAHB	0b11		3	securable and MCU isolation support
83	DECPROT5[7:6]	SRAM4	MLAHB	0b11		3	securable and MCU isolation support
84	DECPROT5[9:8]	RETRAM	MLAHB	0b11		3	securable and MCU isolation support

life.augmented

セキュリティ保護可能ペリフェラルおよび MCU RAMS に関連付けられた DECPROT ビットをこの表に列挙しています。
セキュリティ保護可能 IP:

- セキュアアプリケーションのサービスペリフェラル:USART1、SPI6、I2C4、I2C6
- 暗号アクセラレータ:CRYP1、HASH1、RNG1
- システムペリフェラル:STENC、IWDG1
- タンパ時の消去でセキュリティ保護できる BKPSRAM
- DDRCTRL および DDRPPHYC:TrustZone アドレス空間コントローラ(TZC)が関係する場合はセキュリティ保護可能

TrustZone 認識 : BSEC

- BSEC はデバイスのライフサイクルとデバッグ認証の制御、OTP での機密情報の格納に使用。
- BSEC は TrustZone 認識（BSEC トレーニングを参照）。
- BSEC は 3 つの領域で構成。
  - 制御インタフェースレジスタ
  - 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 モードに応じてセットされる（以下を参照）。

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

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

life.augmented

BSEC はデバイスのライフサイクルとデバッグ認証の制御、OTP での機密情報の格納に使用します。

BSEC は TrustZone 認識です（BSEC トレーニングを参照）。

BSEC は 3 つの領域で構成されます。:

- 制御インタフェースレジスタ
- 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 モードに応じてセットされます。

TrustZone 認識 IP：RCC

- クロックゲーティングおよびセキュア IP のリセット制御はセキュアアクセスでのみ変更できる。
- RCC には、クロックセキュリティに関する専用のセキュア割込みがある。
- RCC セキュリティは 2bit で制御される。TZEN と MCKPROT は書込みセキュア。

** 詳細については、製品のリファレンスマニュアルの RCC のセクションを参照。

life.augmented

クロックゲーティングおよびセキュア IP のリセット制御はセキュアアクセスでのみ変更できます。

RCC には、クロックセキュリティに関する専用のセキュア割込みがあります。

RCC セキュリティは 2bit で制御されます。 TZEN と MCKPROT は書込みセキュアです。

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

TrustZone 認識 IP：PWR

10

- セキュア IP の電力モード制御は、セキュアアクセスでのみ変更する必要がある。
- PWR セキュリティは RCC から TZEN ビットで制御される。
- PWR セキュリティには次の目的の非セキュア書込みを防ぐことも含まれる。
  - VBAT および TEMP の監視、PVD、AVD の設定変更
  - 低電力ディープスリープおよび RAM 低電力の設定変更
  - バックアップドメイン書込み保護の変更
  - バックアップレギュレータ、保持レギュレータ、1V8 レギュレータ、1V1 レギュレータ、USB 3.3V 電圧レベル検出器の設定変更
  - バックアップバッテリ充電の設定変更
  - MPU 電源制御レジスタの設定変更
  - STANDBY ウェイクアップの設定およびフラグの変更

** 詳細については、製品のリファレンスマニュアルの PWR のセクションを参照。

life.augmented

セキュア IP の電力モード制御は、セキュアアクセスでのみ変更する必要があります。

PWR セキュリティは RCC から TZEN ビットで制御されます。

PWR セキュリティには次の目的の非セキュア書込みを防ぐことも含まれます。

- VBAT および TEMP の監視、PVD、AVD の設定変更
- 低電力ディープスリープおよび RAM 低電力の設定変更
- バックアップドメイン書込み保護の変更
- バックアップレギュレータ、保持レギュレータ、1V8 レギュレータ、1V1 レギュレータ、USB 3.3V 電圧レベル検出器の設定変更
- バックアップバッテリ充電の設定変更
- MPU 電源制御レジスタの設定変更
- STANDBY ウェイクアップの設定およびフラグの変更

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

TrustZone 認識 IP：EXTI

- EXTI は、機密イベントに関連する制御ビットや設定ビットへのアクセスを制限することで、これらのイベントを保護できる。
- EXTI_TZENR ビットで入力ごとにセキュリティを有効にできる。
- セキュリティによって、非セキュア書込みアクセスによる設定変更や、セキュアな入力のステータスのマスクとクリアを防ぐ。

** 詳細については、製品のリファレンスマニュアルの EXTI のセクションを参照。

life.augmented

EXTI は、機密イベントに関連する制御ビットや設定ビットへのアクセスを制限することで、これらのイベントを保護できます。

EXTI_TZENR ビットで入力ごとにセキュリティを有効にできます。

セキュリティによって、非セキュア書込みアクセスによる設定変更や、セキュアな入力のステータスのマスクとクリアを防ぎます。

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

TrustZone 認識 IP：GPIOZ

- セキュリティは GPIOZ にのみ適用可能。
- リセット後、すべての GPIOZ I/O ピンがセキュアになる。
- GPIOZ I/O ピンは、GPIOZ_SECCFGR レジスタで個別にセキュアにセットできる。
- I/O ピンがセキュアな場合、すべての I/O 設定ビットが書込みセキュアになる。
- セキュアなピンへの入力は、どのような設定であっても非セキュアな I/O にリダイレクト不可。
- セキュアなピンからの出力データは、別のペリフェラルからの出力によって置き換え不可。
- セキュアな I/O データは、非セキュアな I/O にリダイレクト不可。
- 非セキュアな I/O データは、セキュアな I/O にリダイレクト不可。

life.augmented

セキュリティは GPIOZ にのみ適用できます。

リセット後、すべての GPIOZ I/O ピンがセキュアになります。

GPIOZ I/O ピンは、GPIOZ_SECCFGR レジスタで個別にセキュアにセットできます。

I/O ピンがセキュアな場合、すべての I/O 設定ビットが書込みセキュアになります。

セキュアなピンへの入力は、どのような設定であっても非セキュアな I/O にリダイレクトできません。

セキュアなピンからの出力データは、別のペリフェラルからの出力によって置き換えられません。

セキュアな I/O データは、非セキュアな I/O にリダイレクトできません。

非セキュアな I/O データは、セキュアな I/O にリダイレクトできません。

TrustZone 認識 IP：RTC

- 4 種類の RTC 機能：アラーム A、アラーム B、ウェイクアップタイマおよびタイムスタンプは個別にセキュアに設定可。
- RTC はセキュアに設定可（全体）。
- RTC の初期化および較正制御はセキュアに設定可。
- 書込みセキュアな RTC_SCMR は、RTC セキュリティ設定を制御するために使用。
- サイレントフェイルは、RTC_SCMR ビットへの非セキュアアクセスにより発生。
- RCC クロックおよびリセット制御の継承はリソースに関連。
- RTC はデフォルトでは非セキュア。
- セキュリティ設定は低電力で持続します。この設定はバックアップドメイン POR によってのみリセットされ、システムリセットの影響は受けない。
- 割込み制御（マスクとクリア）は、割込みに関連する機能のセキュリティプロパティを継承する。

life.augmented

4 種類の RTC 機能：アラーム A、アラーム B、ウェイクアップタイマおよびタイムスタンプは個別にセキュアに設定できます。

RTC は全体的にセキュアに設定できます。

RTC の初期化および較正制御はセキュアに設定できます。

書込みセキュアな RTC_SCMR は、RTC セキュリティ設定を制御するために使用します。

サイレントフェイルは、RTC_SCMR ビットへの非セキュアアクセスにより発生します。

RCC クロックおよびリセット制御の継承はリソースに関連しています。

RTC はデフォルトでは非セキュアです。

セキュリティ設定は低電力で持続します。この設定はバックアップドメイン POR によってのみリセットされ、システムリセットの影響は受けません。

割込み制御（マスクとクリア）は、割込みに関連する機能のセキュリティプロパティを継承します。

TrustZone 認識 IP：TAMP

- タンパ制御はセキュアに設定可。
- 128 個のバックアップレジスタは次の 3 つのゾーンに整理される。
  - Zone1：セキュア、セキュアな状態でのみ読出しおよび書込み
  - Zone2：書込みセキュア、セキュアな状態でのみ書込み
  - Zone3：非セキュア
- TAMP はセキュアに設定可（全体）。
- 書込みセキュアな TAMP_SCMR レジスタ は、TAMP セキュリティ設定を制御するために使用。
- バックアップレジスタのゾーンサイズはプログラム可能。
- TAMP クロックおよびリセット制御の継承はリソースに関連。
- TAMP はデフォルトでは非セキュア。
- セキュリティ設定は低電力で持続します。この設定はバックアップドメイン POR によってのみリセットされ、システムリセットの影響は受けない。
- 割込み制御（マスクとクリア）は、割込みに関連する機能のセキュリティプロパティを継承。

タンパ制御はセキュアに設定できます。

128 個のバックアップレジスタは次の 3 つのゾーンに整理されます。

- Zone1：セキュア、セキュアな状態でのみ読出しおよび書込み
- Zone2：書込みセキュア、セキュアな状態でのみ書込み
- Zone3：非セキュア

TAMP はセキュアに設定できます。

書込みセキュアな TAMP_SCMR レジスタ は、TAMP セキュリティ設定を制御するために使用します。

バックアップレジスタのゾーンサイズはプログラム可能です。

TAMP クロックおよびリセット制御の継承はリソースに関連しています。

TAMP はデフォルトでは非セキュアです。

セキュリティ設定は低電力で持続します。この設定はバックアップドメイン POR によってのみリセットされ、システムリセットの影響は受けません。

割込み制御（マスクとクリア）は、割込みに関連する機能のセキュリティプロパティを継承します。

TrustZone 認識および対応 IP：MDMA

- MDMA は 32チャネルをサポート。
- チャネルは、MDMA_CxCR レジスタ（x はチャネル番号（0～31））から SM ビットをセットしてセキュアに設定可。
- SM ビットは、セキュアアクセスによってのみ変更可（書込みセキュアビット）。
- MDMA はチャネルのセキュリティ属性に応じて割込みをセキュアラインと通常ラインにルーティングしている。
- チャネルがセキュアな場合、すべての関連するレジスタが書込みセキュアになる。
- MDMA AXI マスタポートは、対応するチャネルのセキュリティ属性を伝播する。

life.augmented

MDMA は 32チャネルをサポートしています。

チャネルは、MDMA_CxCR レジスタ（x はチャネル番号（0～31））から SM ビットをセットしてセキュアに設定できます。

SM ビットは、セキュアによってのみ変更できます（書込みセキュアビット）。

MDMA はチャネルのセキュリティ属性に応じて割込みをセキュアラインと通常ラインにルーティングしています。

チャネルがセキュアな場合、すべての関連するレジスタが書込みセキュアになります。

MDMA AXI マスタポートは、対応するチャネルのセキュリティ属性を伝播します。

TrustZone とデバッグ

- デバッグアクセスポート（DAP）は、非セキュアなバスマスタ。
- デバッグリソースへのアクセスは、BSEC から発行されるデバッグ認証インタフェースで制御される。

** 詳細については、製品のリファレンスマニュアルのデバッグのセクションを参照。

life.augmented

デバッグアクセスポート（DAP）は、非セキュアなバスマスタです。
デバッグリソースへのアクセスは、BSEC から発行されるデバッグ認証インタフェースで制御されます。
詳細については、製品のリファレンスマニュアルのデバッグのセクションを参照してください。