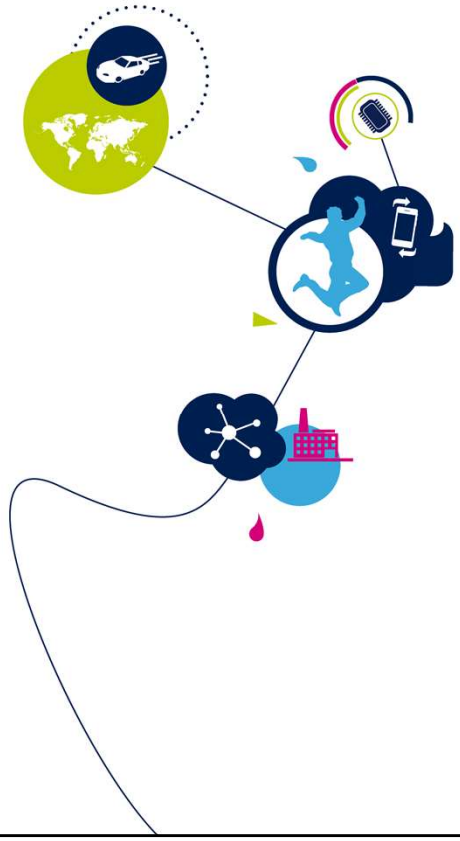
STM32MP1 - ETZPC

TrustZone アドレス空間コントローラ
1.0 版



こんにちは、STM32MP1 TrustZone アドレス空間コントローラの
プレゼンテーションへようこそ。

概要

強化された TrustZone 保護コントローラ(ETZPC)の使用目的は以下のとおり

1. セキュリティ保護可能な IP の **TrustZone** セキュリティを設定
   - ペリフェラルセキュリティモードの種類:
     - セキュア:読出しおよび書込みアクセスは、セキュアワールドに対してのみ許される
     - 書込みセキュア:書込みアクセスはセキュアワールドに対してのみ許され、読出しはどこからでも可能
     - 非セキュア:読出しおよび書込みアクセスは、どこからでも可能
2. SYSRAM および ROM のセキュア領域サイズを設定
   - セキュア領域は、4KB の倍数で最下位アドレスに定義される
3. MCU ドメインに割り当てられる分離可能な IP のセットで MCU 分離ドメインを設定

life.augmented

強化された TrustZone 保護コントローラ(ETZPC)の使用目的は以下のとおりです。

1)セキュリティ保護可能な IP の TrustZone セキュリティを設定する。ペリフェラルセキュリティモードの種類は以下のとおり。

- セキュア:読出しおよび書込みアクセスは、セキュアワールドに対してのみ許される
- 書込みセキュア:書込みアクセスはセキュアワールドに対してのみ許され、読出しはどこからでも可能
- 非セキュア:読出しおよび書込みアクセスは、どこからでも可能

2)SYSRAM および ROM のセキュア領域サイズを設定する。セキュア領域は、4KB の倍数で最下位アドレスに定義されます。

3)MCU ドメインに割り当てられる分離可能な IP のセットで MCU 分離ドメインを設定する

ETZPC の主な機能

3

- 32bit APB4 インタフェース
- ETZPC は書込みセキュアのみ
- 以下の SoC セキュリティおよび分離設定を制御するレジスタセット
  - SYSRAM および ROM のセキュア領域サイズ（TZMA0/TZMA1）
  - セキュリティ保護可能な AHB および APB ペリフェラルに対するアクセス権限
  - AHB および APB ペリフェラルの Cortex®-M4 ドメインへのリソース分離
- メモリ領域ごと、およびペリフェラルごとのセキュリティ設定のロック

life.augmented

TrustZone アドレス空間コントローラの主要機能は次の通りです。

- 32bit APB4 インタフェース
- ETZPC は書込みセキュアのみ
- 以下の SoC セキュリティおよび分離設定を制御するレジスタセット
  - SYSRAM および ROM のセキュア領域サイズ（TZMA0/TZMA1）
  - セキュリティ保護可能な AHB および APB ペリフェラルに対するアクセス権限
  - AHB および APB ペリフェラルの Cortex-M4 ドメインへのリソース分離
- メモリ領域ごと、およびペリフェラルごとのセキュリティ設定のロック

ペリフェラルのセキュリティ

4

- セキュアリソース:
  - ETZPC からの制御なし
  - ETZPC:書込みセキュアのみ
  - TZC:常にセキュア
  - AXIM/GPC:常にセキュア
- 非セキュアリソース:
  - 多くのペリフェラルはセキュリティに関係がなく、セキュリティの観点から ETPZ によって制御されることはない
  - MCU 分離は非セキュアリソースに適用され、ETZPC から制御される
- セキュリティ保護可能リソース:
  - ペリフェラルのセキュリティは、DECPROT ビットに従ってセキュア、書込みセキュア、非セキュアのどれかに設定可能
  - SYSRAM および BootROM メモリには、TZMA0/1 設定に従って、プログラム可能なセキュア領域サイズが設けられる

注:SRAM1/2/3/4 および RETRAM は、DECPROT ビットに従ってセキュアにしたり、書込みセキュアにしたりすることは出来ない

life.augmented

セキュアリソース:

- ETZPC からの制御なし
- ETZPC:書込みセキュアのみ
- TZC:常にセキュア
- AXIM/GPC:常にセキュア

非セキュアリソース:

- 多くのペリフェラルはセキュリティに関係がなく、セキュリティの観点から ETPZ によって制御されることはありません。
- MCU 分離は非セキュアリソースに適用され、ETZPC から制御されます。

セキュリティ保護可能リソース:

ペリフェラルのセキュリティは、DECPROT ビットに従ってセキュア、書込みセキュア、非セキュアのどれかにできます。

SYSRAM および BootROM メモリには、TZMA0/1 設定に従って、プログラム可能なセキュア領域サイズが設けられます。

注:SRAM1/2/3/4 および RETRAM は、DECPROT ビットに従ってセキュアにしたり、書込みセキュアにしたりすることはできません。

MCU 分離可能な IP

- MPU および MCU ドメインの定義:
  - MCU ドメインには、Cortex-M4 と、Cortex-M4 コアに割り当てられた DMA バスマスタが含まれる
  - MPU ドメインは、TZ セキュリティが適用されるペリフェラルを除き、Cortex-A7 および Cortex-M4 のペリフェラルにわたる共有制御によって MCU ドメインを補完
  - DMA バスマスタは、この IP スレーブバスに割り当てられた MCU 分離特性を継承する

life.augmented

MPU および MCU ドメインの定義:

- MCU ドメインには、Cortex-M4 と、Cortex-M4 コアに割り当てられた DMA バスマスタが含まれます。
- MPU ドメインは、TZ セキュリティが適用されるペリフェラルを除き、Cortex-A7 および Cortex-M4 の共有制御によって MCU ドメインを補完するものです。
- DMA バスマスタは、この IP スレーブバスに割り当てられた MCU 分離特性を継承します。

ペリフェラルのタイプとアクセス

- ペリフェラルは以下の 3 つのタイプのいずれかになる
  - タイプ 1:セキュリティ保護可能
  - タイプ 2:非セキュアで、MCU 分離可能
  - タイプ 3:セキュリティ保護可能で、MCU 分離可能
- ETZPC は DECPROT[1:0] ビットに従って MPU/MCU ドメインへのアクセスを制御

DECPROT[1:0]	MPU アクセス				MCU アクセス		許容される DECPROT ビット対 ペリフェラルタイプ			ペリフェラルモード
	セキュア		非セキュア		非セキュア					
	読出し	書込み	読出し	書込み	読出し	書込み	タイプ 1	タイプ 2	タイプ 3	
0b00	y	y	n	n	n	n	可能／デフォルト	予約済み	可能	セキュアペリフェラル
0b01	y	y	y	n	y	n	可能	予約済み	可能	書込みセキュアペリフェラル
0b10	n	n	n	n	y	y	予約済み	可能	可能	非セキュアペリフェラル、MCU 分離
0b11	y	y	y	y	y	y	可能	可能／デフォルト	可能／デフォルト	非セキュア共有

life.augmented

ペリフェラルは以下の 3 つのタイプのどれかになります。
タイプ 1:セキュリティ保護可能
タイプ 2:非セキュアで、MCU 分離可能
タイプ 3:セキュリティ保護可能で、MCU 分離可能
この表に示すように、ETZPC は DECPROT[1:0] ビットに従って MPU/MCU ドメインへのアクセスを制御します。
タイプ 1 は、セキュア、書込みセキュア、または非セキュア共有にできるが、MCU 分離にはできません。
タイプ 2 は、共有、または MCU 分離にできるが、セキュアまたは書込みセキュアにはできません。
Type 3 は、セキュア、書込みセキュア、または非セキュアで MCU 分離、あるいは非セキュア共有にできます。

タイプ 1:セキュリティ保護可能 な IP

7

- AHB5/APB5 バスに配置
- リセット後にデフォルトでセキュリティ保護される
- セキュリティの特性は、ETZPC によって書込みセキュアまたは非セキュアに変更可能
- MCU 分離可能には出来ない
- ペリフェラル一覧:
  - STGENC、BKPSRAM、IWDG1、USART1、SPI6、I2C4、I2C6、CRYP1、HASH1、RNG1、DDRCTRL、DDRPHYC

life.augmented

タイプ 1 のセキュリティ保護可能な IP は AHB5/APB5 バスに配置されます。

これらはリセット後にデフォルトでセキュリティ保護されます。

セキュリティの特性は、ETZPC によって書込みセキュアまたは非セキュアに変更できます。

MCU 分離可能にはできません。

タイプ 2：非セキュアで MCU 分離可能な IP

- 多くのペリフェラルはタイプ 2 の非セキュア IP
- リセット後にデフォルトで MPU と MCU 間で共有される
- セキュリティの特性は、ETZPC によって MCU 分離可能に変更可能
- セキュアまたは書込みセキュアには出来ない
- バスマスタを備えたペリフェラルは MCU 分離に従ってバスマスタの属性を変更

life.augmented

多くのペリフェラルはタイプ 2 の非セキュア IP です。

リセット後にデフォルトで MPU と MCU 間で共有されます。

セキュリティの特性は、ETZPC によって MCU 分離可能に変更できます。

セキュアまたは書込みセキュアにはできません。

バスマスタを備えたペリフェラルは MCU 分離に従ってバスマスタの属性を変更します。

タイプ 3:セキュリティ保護可能で、MCU 分離可能な IP

9

- 内部 RAM のみ: SRAM1/2/3/4 および RETRAM メモリ
- これらはリセット後にデフォルトで非セキュアで、MPU と MCU 間で共有される
- セキュリティの特性は、ETZPC によって下記に変更できる
  - セキュア
  - 書込みセキュア
  - 非セキュアで、MCU 分離可能

life.augmented

タイプ 3 のセキュリティ保護可能 IP は次の内部 RAM のみです: SRAM1/2/3/4 および RETRAM メモリ

これらはリセット後にデフォルトで非セキュアで、MPU と MCU 間で共有されます。

セキュリティの特性は、ETZPC によって下記に変更できます。

- セキュア
- 書込みセキュア
- 非セキュアで、MCU 分離可能

DMA マスタ IP

- MCU ドメインに割り当てられることがある DMA マスタ IP は以下のとおり
  - DMA1/DMA2
  - ETH
  - SDMMC3
  - OTG
- DMA マスタは、そのスレーブインタフェースが DECPROT ビットによって MCU に割り当てられると、MCU に設定される
- MCU に割り当てられた DMA マスタは、MPU によるすべての R/W アクセス（セキュアまたは非セキュア）を無視

life.augmented

MCU ドメインに割り当てられることがある DMA マスタ IP は以下のとおりです。

- DMA1/DMA2
- ETH
- SDMMC3
- OTG

DMA マスタは、そのスレーブインタフェースが DECPROT ビットによって MCU に割り当てられると、MCU に設定されます。
MCU に割り当てられた DMA マスタは、MPU によるすべての R/W アクセス（セキュアまたは非セキュア）を無視します。