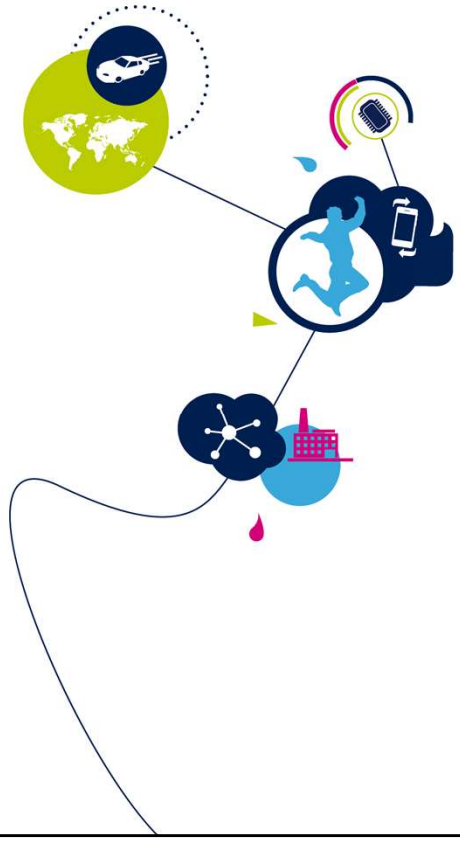
STM32MP1 - TZC

TrustZone アドレス空間コントローラ
1.0 版

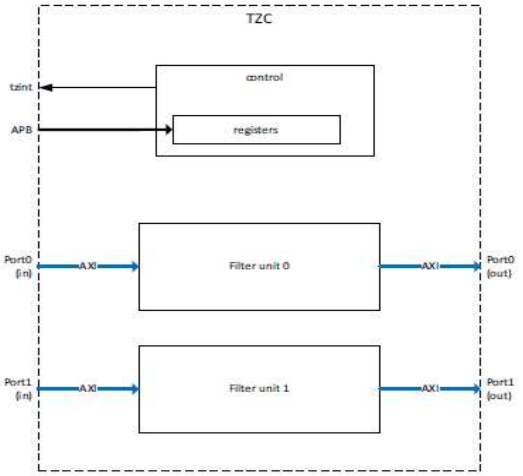


life.augmented

STM32MP1 TrustZone アドレス空間コントローラのプレゼンテーションにようこそ。

概要

- TZC は、プログラム可能な領域によって定義される TrustZone® セキュリティ制御および NSAID（非セキュアマスタアドレス ID）に応じて、DDR の読出しアクセスと書込みアクセスをフィルタすることを目的とした機能
- TZC には 2 つのフィルタ（AXI ポートに 1 つ）



life.augmented

TrustZone® アドレス空間コントローラ（TZC）は、セキュリティルールおよび非セキュアマスタアドレス ID に応じて、DDR アクセスをフィルタすることを目的としています。
これは、TZC の簡略化されたブロック図です。
TZC は 2 つのフィルタユニット（AXI ポートに 1 つ）で構成されます。フィルタは同時に機能しています。
2 つのフィルタは、APB インタフェースでセットされる共通の制御レジスタで制御されます。

主な機能（1/2）

- 2 つのフィルタユニットは同時に機能
- 9 つの領域
  - 領域 0 は常に有効になっており、DDR のアドレス範囲全体をカバー
  - 領域 1～8 には、4KB 単位のプログラム可能な開始／終了アドレスがあり、いずれかまたは両方のフィルタに割当て可能
- セキュアアクセスおよび非セキュアアクセスの許可は、領域ごとにプログラム
- 非セキュアアクセスは、非セキュアマスタアドレス ID（NSAID）に応じてフィルタ
- 同じフィルタで制御される領域はオーバーラップ不可

TZC は 2 つの AXI ポートで同時に機能している 2 つのフィルタユニットで構成されます。

アクセスのフィルタリングは最大 9 つの領域をサポートしています。

- 領域 0 は常に有効になっており、DDR のアドレス範囲全体をカバーしています。
- 領域 1～8 には、4KB 単位のプログラム可能な開始および終了アドレスがあります。1 つの領域を、いずれかまたは両方のフィルタに割り当てることができます。

セキュアアクセスおよび非セキュアアクセスの許可は、領域ごとに定義されます。

非セキュアアクセスは、非セキュアマスタアドレス ID に応じてフィルタされます。

同じフィルタで制御される領域はオーバーラップさせてはなりません。

主な機能(2/2)

- AXI バスエラーまたは割込みで許可のチェック失敗を発信
- 32bit APB4 インタフェース
- TZC 設定はセキュアマスタのみでサポート
- 読出しアクセスパスは、最大 256 個の未処理トランザクションをサポート
- ゲートキーパーロジックによって各フィルタを有効および無効化が可能
- 投機的アクセスをサポート

注:TZC には、2 サイクルの遅延があります。

許可のチェックに失敗すると、AXI バスエラーまたは割込み、あるいはその両方で信号送信できます。

TZC は 32bit APB4 インタフェースでプログラムされます。

TZC 設定はセキュアマスタのみでサポートされます。

読出しアクセスパスは、最大 256 個の DDR に対する未処理トランザクションをサポートしています。

ゲートキーパーロジックを使用して、各フィルタを有効および無効にします。

TZC は投機的アクセスをサポートしています。

注:TZC には、2 サイクルの遅延があります。主な機能を減らした高速パス(FPID)は、STM32MP1 シリーズではサポートしていません。

プログラミングガイドライン

5

- 領域 0 はベース領域で、アドレス範囲全体をカバーし、常に有効
- 領域 0 は領域 1～8 以外のアクセスの捕捉が可能
- 領域 1～8 を同じフィルタに割り当てる場合、互いにオーバーラップ不可
- 半静的プログラミングでは、フィルタ設定を再プログラムする前にすべてのアクセス（ゲート）のブロックが必要
- TZC は独立した読出しおよび書込みの設定をサポート
- セキュアと非セキュアの設定は独立していますが、セキュアチェックはあらゆるマスタに適用できる一方、非セキュアチェックはマスタごとにフィルタ（NSAID による選択）。

life.augmented

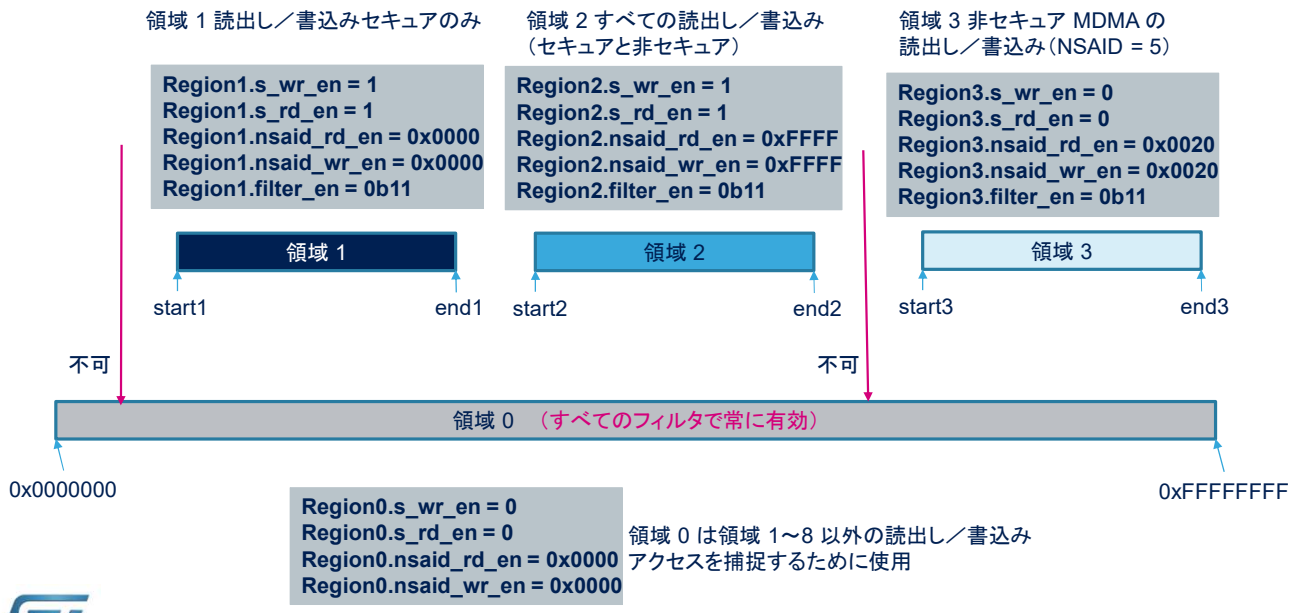
TZC プログラミングでは次のガイドラインを遵守する必要があります。

- 領域 0 はベース領域で、アドレス範囲全体をカバーし、常に有効になっています。
- 領域 0 は領域 1～8 以外のアクセスの捕捉が可能
- 領域 1～8 を同じフィルタに割り当てる場合、互いにオーバーラップさせてはなりません。
- 半静的プログラミングで再設定する場合、フィルタ設定を再プログラムする前にすべてのアクセス（ゲート）をブロックする必要があります。

TZC のアクセスフィルタリングは以下に基づきます。

- 読出しと書込みの設定（読出しのみ、書込みのみ、読出し／書込み、アクセスなし）は独立しています。
- セキュアと非セキュアの設定は独立していますが、セキュアチェックはあらゆるマスタに適用できる一方、非セキュアチェックはマスタごとにフィルタされます（NSAID による選択）。

プログラミングの例



このスライドでは、簡単なプログラミングの例を示しています。DDR 空間は、3 つの非オーバーラップ領域をサポートしています。

- 領域 1 は start1～end1 のアドレスで定義されます。領域 1 はセキュアアプリケーションによってのみ読み書きアクセスが可能です。
- 領域 2 は start2～end2 のアドレスで定義されます。領域 2 はセキュアアプリケーションと非セキュアアプリケーションによって共有領域の読み書きアクセスが可能です。
- 領域 3 は start3～end3 のアドレスで定義されます。領域 3 は非セキュア MDMA エンジン（NSAID = 5）によってのみ読み書きアクセスが可能です。

レジスタ設定とプログラミングシーケンスは、wr_en と rd_en のパラメータです。NSAID は次のスライドの表に列挙しています。

領域 0 は常に有効になっており、DDR のアドレス範囲全体をカバーしています。これらの領域以外のアクセスを捕捉するためにセットされます。
そのため、3 つの定義された領域以外からのアクセスは許可されません。

NSAID の表

MasterUSBH（EHCI）	NSAID[0:3]
CA7	0b0000
CM4	0b0001
LTDC	0b0011
GPU	0b0100
MDMA	0b0101
DMA1	0b0110
DMA2	0b0110
USBH（EHCI）	0b0111
USBH（OHCI）	0b0111
OTG	0b1000
SDMMC1	0b1001
SDMMC2	0b1001
SDMMC3	0b1001
ETH	0b1010
DAP	0b1111

life.augmented

非セキュアマスタアドレス ID（NSAID）は、この表に列挙されたマスタに応じて 4bit でエンコードされます。