ARM®

PrimeCell® Infrastructure AMBA™ 3 TrustZone™ Protection Controller (BP147)
Revision: r0p0
Technical Overview

This technical overview describes the functionality of the ARM AMBA 3 APB *TrustZone Protection Controller* (TZPC) in the following sections:

1 Preliminary material

1.1 Release information

Changes to this document are listed in Table 1.

Table 1 Change history

Date	Issue	Change
29 November 2004	A	First issue for r0p0

1.2 Proprietary notice

1.3 Confidentiality status

1.4 Product status

The information in this document is for a final product, that is a developed product.

1.5 Web address

`http://www.arm.com`

2 About the TrustZone Protection Controller

The *TrustZone Protection Controller* (TZPC), `TZProtCtrl`, is an AMBA-compliant, SoC peripheral that is developed, tested, and licensed by ARM Limited.

The TZPC provides a software interface to the protection bits in a secure system in a TrustZone design. It provides system flexibility to enable you to configure different areas of memory as secure or non-secure.

The TZPC has the following features:

- it has protection bits to enable you to program up to 24 areas of memory as secure or non-secure
- it has secure region bits to enable you to split an area of internal RAM into both secure and non-secure regions
- it has an AMBA APB system interface
- it does not generate any APB wait states or a slave error response and is therefore compatible with the AMBA 2 APB protocol.

Figure 1 shows a simplified block diagram of the TZPC.

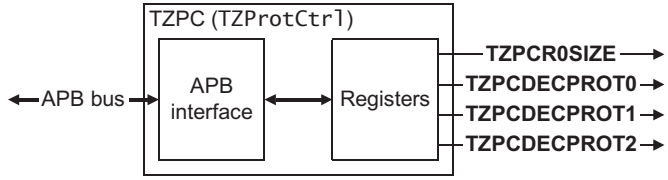

Figure 1 TrustZone Protection Controller

3 Functional description

The TZPC provides a software interface to set up memory areas as secure or non-secure. It does this in two ways:

- Programmable protection bits that can be allocated to areas of memory as determined by an external decoder.
- Programmable region size value for use by an AXI *TrustZone Memory Adapter* (TZMA). You can use this to split the RAM into two regions:
  - one secure
  - one non-secure.

This programmable flexibility enables you to reuse a single SoC design for different applications at different times. This enables the best use of memory and other system resources. It is assumed that the specific secure and non-secure requirements for an application are determined during:

- the SoC boot-up
- OS or secure kernel port development work.

This means that the secure and non-secure memory partitioning is not expected to change dynamically during normal software operation because it is fixed at compile time and is only configured once during system boot-up. Ensure that this boot-up is always made in secure-state to guarantee full security protection.

Caution

The APB protocol does not support protection signals. The TZPC relies on external protection to provide security for its registers. Implement these in a secure AXI-APB bridge or an AXI decoder.

You must use a secure software protocol before relying on any security settings that have been changed. This might include, but is not limited to:

- verifying that instructions to change the security settings have propagated across the interconnect to their final destination
- clearing any storage locations that have changed security status
- flushing caches and page tables
- stopping other masters.

Figure 2 on page 5 shows a TZPC configured in a typical TrustZone-enabled design.

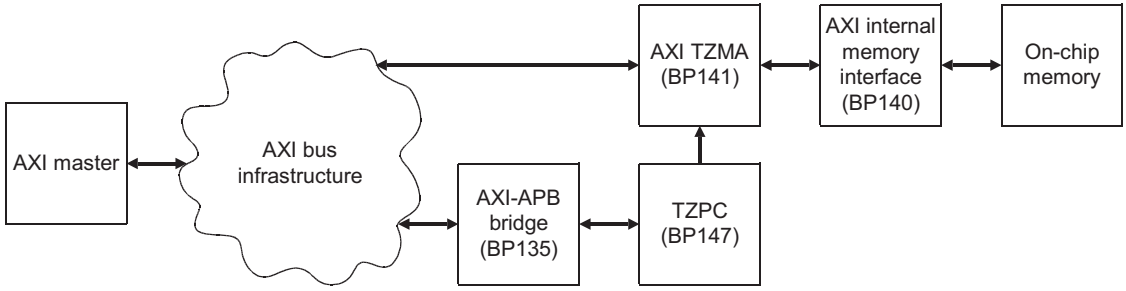

Figure 2 Typical configuration

The other components that Figure 2 shows are:

AXI master This initiates read and write transactions.

AXI bus infrastructure

This is typically a bus matrix or interconnect. You can use the PrimeCell Configurable AXI Interconnect (PL300) to implement this. See the *PrimeCell AXI Configurable Interconnect (Pl300) Technical Reference Manual* for more information.

AXI-APB bridge

This connects between the AXI and APB domains. See the *PrimeCell Infrastructure AMBA 3 AXI-APB Bridge (BP135) Technical Overview* and *Design Manual* for more information.

TZMA This determines the legality of a transaction and blocks it if the TZPC deems it as illegal. See the *PrimeCell Infrastructure AMBA 3 AXI TrustZone Memory Adaptor (BP141) Technical Overview* and *Design Manual* for more information.

AXI Memory Interface

This provides a single-port memory interface that you can configure for synchronous SRAM or ROM. See the *PrimeCell Infrastructure AMBA 3 AXI memory Interface (BP140) Technical Overview* and *Design Manual* for more information.

4 Programmer's model

This section describes the TZPC registers and provides programming information for them in:

- *About the programmer's model*
- *Summary of registers* on page 7
- *Register descriptions* on page 8.

4.1 About the programmer's model

The following applies to the registers used in the TZPC.

- Place the TZPC in a secure area of memory to ensure TrustZone security.
- The base address of the component is not fixed and can be different for any particular system implementation. However, the offset of any particular register from the base address is fixed.
- You must not access reserved or unused address locations because this can result in unpredictable behavior of the device.
- You must write reserved or unused register bits as zero and ignore them on read unless otherwise stated in the relevant text.
- All register bits are reset to a logic 0 by a system or power-on reset unless otherwise stated in the relevant text.
- All registers support read and write accesses unless otherwise stated in the relevant text. A write updates the contents of a register and a read returns the contents of the register.
- You can access all registers with zero wait states.

4.2 Summary of registers

Table 2 lists the TZPC registers in base offset order.

Table 2 Register summary

Name	Base offset	Type	Reset value	Description
TZPCR0SIZE	0x000	R/W	0x00000200	See *Secure RAM Region Size Register* on page 8
TZPCDECPROT0Stat	0x800	RO	0x00000000	See *Decode Protection 0-2 Status Registers* on page 9
TZPCDECPROT0Set	0x804	WO	-	See *Decode Protection 0-2 Set Registers* on page 9
TZPCDECPROT0Clr	0x808	WO	-	See *Decode Protection 0-2 Clear Registers* on page 10
TZPCDECPROT1Stat	0x80C	RO	0x00000000	See *Decode Protection 0-2 Status Registers* on page 9
TZPCDECPROT1Set	0x810	WO	-	See *Decode Protection 0-2 Set Registers* on page 9
TZPCDECPROT1Clr	0x814	WO	-	See *Decode Protection 0-2 Clear Registers* on page 10
TZPCDECPROT2Stat	0x818	RO	0x00000000	See *Decode Protection 0-2 Status Registers* on page 9
TZPCDECPROT2Set	0x81C	WO	-	See *Decode Protection 0-2 Set Registers* on page 9
TZPCDECPROT2Clr	0x820	WO	-	See *Decode Protection 0-2 Clear Registers* on page 10
TZPCPERIPHID0	0xFE0	RO	0x00000070	See *Peripheral Identification Register 0* on page 12
TZPCPERIPHID1	0xFE4	RO	0x00000018	See *Peripheral Identification Register 1* on page 12
TZPCPERIPHID2	0xFE8	RO	0x00000004	See *Peripheral Identification Register 2* on page 12
TZPCPERIPHID3	0xFEC	RO	0x00000000	See *Peripheral Identification Register 3* on page 13
TZPCPCELLID0	0xFF0	RO	0x0000000D	See *TZPC Identification Register 0* on page 14
TZPCPCELLID1	0xFF4	RO	0x000000F0	See *TZPC Identification Register 1* on page 14
TZPCPCELLID2	0xFF8	RO	0x00000005	See *TZPC Identification Register 2* on page 14
TZPCPCELLID3	0xFFC	RO	0x000000B1	See *TZPC Identification Register 3* on page 15

4.3 Register descriptions

This section provides descriptions of the registers listed in Table 2 on page 7.

Note

Three TZPC Decode Protection Status Registers, Decode Protection Set Registers, and Decode Protection Clear Registers are implemented to derive the associated signals, **TZPCDECPROT0**, **TZPCDECPROT1**, and **TZPCDECPROT2**. The descriptions in this section use the letter x to denote an individual register number of 0-2.

Secure RAM Region Size Register

The read and write TZPCR0SIZE Register has a reset value of `0x00000200`. It sets the size of the secure region in the internal RAM. Figure 3 shows the register bit assignments.

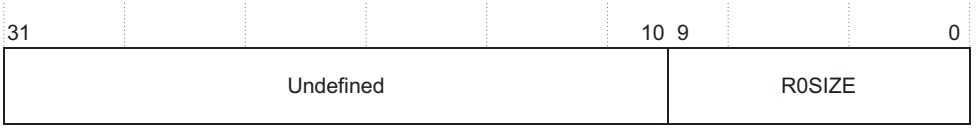

Figure 3 TZPCR0SIZE Register bit assignments

Table 3 lists the register bit assignments.

Table 3 TZPCR0SIZE Register bit assignments

Bits	Name	Function
[31:10]	-	Read undefined. Write as zero.
[9:0]	R0SIZE	Secure RAM region size in 4KB steps: `0x00000000` = no secure region `0x00000001` = 4KB secure region `0x00000002` = 8KB secure region … `0x000001FF` = 2044KB secure region. `0x00000200` or above sets the entire RAM to secure regardless of size

Decode Protection 0-2 Status Registers

The read-only TZPCDECPROTxStat Registers have a reset value of `0x00000000`. They provide the status of the appropriate decode protection 0-3 output signals. Figure 4 shows the register bit assignments.

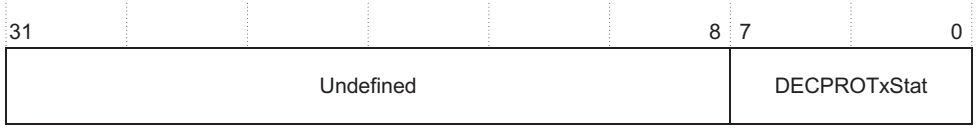

Figure 4 TZPCDECPROTxStat Register bit assignments

Table 4 lists the register bit assignments.

Table 4 TZPCDECPROTxStat Register bit assignments

Bits	Name	Function
[31:8]	-	Read undefined.
[7:0]	DECPROTxStat	Shows the status of the decode protection output: 0 = decode region corresponding to the bit is secure 1 = decode region corresponding to the bit is non-secure. There is one bit of the register for each protection output, eight outputs are implemented as standard.

Decode Protection 0-2 Set Registers

The write-only TZPCDECPROTxSet Registers set the appropriate bits in the **TZPCDECPROTx[7:0]** output signals. Figure 5 shows the register bit assignments.

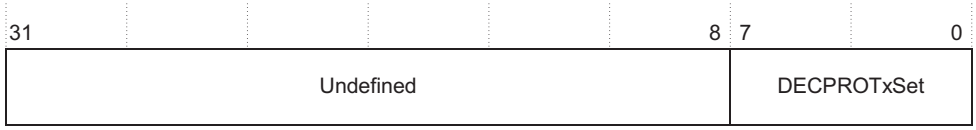

Figure 5 TZPCDECPROTxSet Register bit assignments

Table 5 lists the register bit assignments.

Table 5 TZPCDECPROTxSet Register bit assignments

Bits	Name	Function
[31:8]	-	Write as zero.
[7:0]	DECPROTxSet	Sets the corresponding decode protection output: 0 = no effect 1 = set decode region to non-secure. There is one bit of the register for each protection output, eight outputs are implemented as standard.

Decode Protection 0-2 Clear Registers

The write-only TZPCDECPROTxClr Registers clear the appropriate bits in the **TZPCDECPROTx[7:0]** output signals. Figure 6 shows the register bit assignments.

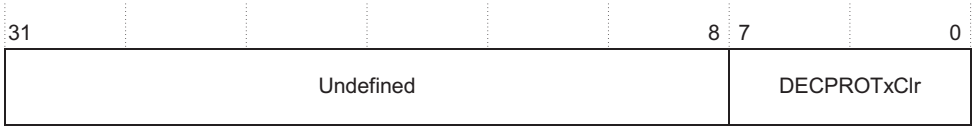

Figure 6 TZPCDECPROT0Clr Register bit assignments

Table 6 lists the register bit assignments.

Table 6 TZPCDECPROTxClr Register bit assignments

Bits	Name	Function
[31:8]	-	Write as zero.
[7:0]	DECPROTxClr	Clears the corresponding decode protection output: 0 = no effect 1 = set decode region to secure. There is one bit of the register for each protection output, eight outputs are implemented as standard.

TZPC Peripheral Identification Registers 0-3

The read-only TZPCPERIPHID0-3 Registers are four 8-bit registers, that span address locations 0xFE0-0xFEC. Figure 7 shows how you can treat the registers conceptually as a single 32-bit register. The registers provide the following options for the peripheral:

Part number [11:0]

This identifies the peripheral. The three digit product code `0x870` is used for the TZPC.

Designer [19:12]

This is the identification of the designer. ARM Limited is `0x41`, ASCII A.

Revision number [23:20]

This is the revision number of the peripheral. The revision number starts from 0 and the value is revision-dependent.

Configuration [31:24]

This is the configuration option of the peripheral. The configuration value is 0.

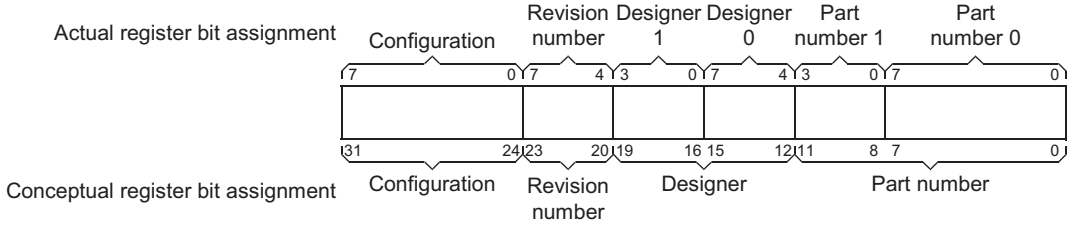

Figure 7 Peripheral identification Register bit assignments

The four 8-bit peripheral identification registers are described in:

- *Peripheral Identification Register 0* on page 12
- *Peripheral Identification Register 1* on page 12
- *Peripheral Identification Register 2* on page 12
- *Peripheral Identification Register 3* on page 13.

Peripheral Identification Register 0

The read-only TZPCPERIPHID0 Register is hard-coded and the fields in the register determine the reset value. Table 7 lists the register bit assignments.

Table 7 TZPCPERIPHID0 Register bit assignments

Bits	Name	Function
[31:8]	-	Read undefined
[7:0]	Partnumber0	These bits read back as `0x70`

Peripheral Identification Register 1

The read-only TZPCPERIPHID1 Register is hard-coded and the fields in the register determine the reset value. Table 8 lists the register bit assignments.

Table 8 TZPCPERIPHID1 Register bit assignments

Bits	Name	Function
[31:8]	-	Read undefined.
[7:4]	Designer0	These bits read back as `0x1`
[3:0]	Partnumber1	These bits read back as `0x8`

Peripheral Identification Register 2

The read-only TZPCPERIPHID2 Register is hard-coded and the fields in the register determine the reset value. Table 9 lists the register bit assignments.

Table 9 TZPCPERIPHID2 Register bit assignments

Bits	Name	Function
[31:8]	-	Read undefined
[7:4]	Revision	These bits read back as the revision number which can be 0-15
[3:0]	Designer1	These bits read back as `0x4`

Peripheral Identification Register 3

The read-only TZPCPERIPHID3 Register is hard-coded and the fields in the register determine the reset value. Table 10 lists the register bit assignments.

Table 10 TZPCPERIPHID3 Register bit assignments

Bits	Name	Function
[31:8]	-	Read undefined
[7:0]	Configuration	These bits read back as `0x00`

Identification Registers 0-3

The read-only TZPCPCELLID0-3 Registers are four 8-bit registers that span address locations 0xFF0-0xFFC. You can treat the register conceptually as a single 32-bit register. The register is used for a standard cross-peripheral identification system. Figure 8 shows the register bit assignments.

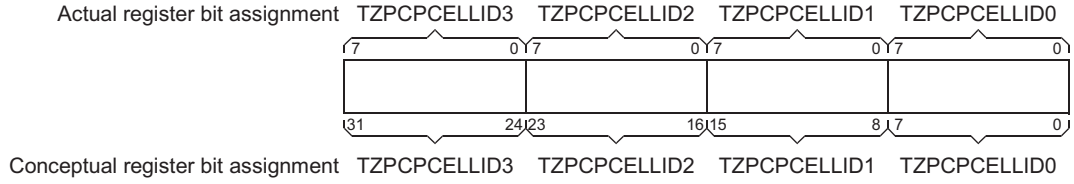

Figure 8 TZPC Identification Register bit assignments

The four 8-bit TZPC Identification Registers are described in:

- *TZPC Identification Register 0* on page 14
- *TZPC Identification Register 1* on page 14
- *TZPC Identification Register 2* on page 14
- *TZPC Identification Register 3* on page 15.

TZPC Identification Register 0

The read-only TZPCPCELLID0 Register is hard-coded and the fields in the register determine the reset value. Table 11 lists the register bit assignments

Table 11 TZPCPCELLID0 Register bit assignments

Bits	Name	Function
[31:8]	-	Read undefined
[7:0]	TZPCPCELLID0	These bits read back as `0x0D`

TZPC Identification Register 1

The read-only TZPCPCELLID1 Register is hard-coded and the fields in the register determine the reset value. Table 12 lists the register bit assignments.

Table 12 TZPCPCELLID1 Register bit assignments

Bits	Name	Function
[31:8]	-	Read undefined
[7:0]	TZPCPCELLID1	These bits read back as `0xF0`

TZPC Identification Register 2

The read-only TZPCPCELLID2 Register is hard-coded and the fields in the register determine the reset value. Table 13 lists the register bit assignments.

Table 13 TZPCPCELLID2 Register bit assignments

Bits	Name	Function
[31:8]	-	Read undefined
[7:0]	TZPCPCELLID2	These bits read back as `0x05`

TZPC Identification Register 3

The read-only TZPCPCELLID3 Register is hard-coded and the fields in the register determine the reset value. Table 14 lists the register bit assignments.

Table 14 TZPCPCELLID3 Register bit assignments

Bits	Name	Function
[31:8]	-	Read undefined
[7:0]	TZPCPCELLID3	These bits read back as `0x00`

5 Physical data

This section describes:

- *AC characteristics*
- *Gate count*.

5.1 AC characteristics

The TZPC adheres to the following timing guidelines. The figures refer to the percentage of clock cycle allowed for each function:

- APB inputs must be valid for 70% prior to the rising edge of the clock
- APB outputs must be valid for 20% after the rising edge of the clock.

Timing characteristics are confirmed by performing synthesis on the block using the slow-slow process point of the Artisan SAGE HS library for the TSMC CL013G process at a target speed of 200MHz.

5.2 Gate count

The estimated total gate counts with respect to the library described in AC characteristics is 777.

Note

The gate count estimate does not include scan logic.

6 Signal descriptions

Figure 9 shows the signal connections.

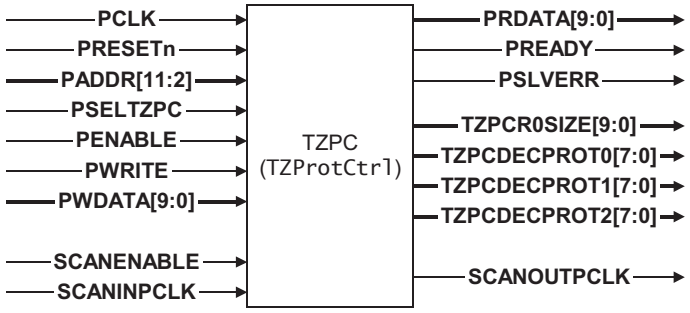

Figure 9 TZPC signal connections

The signals are described in:

- *AMBA APB signals*
- *Non-AMBA APB signals*.

6.1 AMBA APB signals

The *AMBA 3 APB Protocol Specification* describes the AMBA APB signals that the controller uses.

6.2 Non-AMBA APB signals

The following sections describe the non-AMBA APB signals:

- *TZ-PC signals* on page 18
- *Scan insertion signals* on page 18.

TZ-PC signals

Table 15 lists the TZ-PC signals.

Table 15 TZ-PC signals

Name	Type	Destination	Description
TZPCR0SIZE[9:0]	Output	AXI TrustZone memory adaptor	R0, secure RAM size
TZPCDECPROT0[7:0]	Output	AXI decoder or bridge	Protection bits: 0 = secure 1 = non-secure.
TZPCDECPROT1[7:0]	Output	AXI decoder or bridge	Protection bits: 0 = secure 1 = non-secure.
TZPCDECPROT2[7:0]	Output	AXI decoder or bridge	Protection bits: 0 = secure 1 = non-secure.

Scan insertion signals

Table 16 lists the TZ-PC internal scan test control signals.

Table 16 TZ-PC scan test control signals

Name	Type	Source/destination	Description
SCANENABLE	Input	Scan controller	Scan enable, for all clock domains
SCANINPCLK	Input	Scan controller	Scan data input for **PCLK** domain
SCANOUTPCLK	Output	Scan controller	Scan data output for **PCLK** domain