ARM® CoreLink™ TZC-400 TrustZone® Address Space Controller

Revision: r0p1

Technical Reference Manual

ARM®

ARM DDI 0504C (ID063014)

ARM CoreLink TZC-400 TrustZone Address Space Controller
Technical Reference Manual

Release Information

The following changes have been made to this book.

Change history

Date	Issue	Confidentiality	Change
10 May 2013	A	Non-Confidential	First release for r0p0
15 July 2013	B	Non-Confidential	First release for r0p1
20 February 2014	C	Non-Confidential	Second release for r0p1

Proprietary Notice

Confidentiality Status

This document is Non-Confidential. The right to use, copy and disclose this document may be subject to license restrictions in accordance with the terms of the agreement entered into by ARM and the party that ARM delivered this document to.

Product Status

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

Web Address

`http://www.arm.com`

Contents
ARM CoreLink TZC-400 TrustZone Address Space Controller Technical Reference Manual

Preface

This preface introduces the *ARM® CoreLink™ TZC-400 TrustZone® Address Space Controller Technical Reference Manual*. It contains the following sections:

About this book

This book is for the ARM CoreLink *TrustZone Address Space Controller* (TZC-400). It gives a high-level overview of the TZC-400 and describes its registers. It also lists the signals that the TZC-400 provides.

Product revision status

The r*n*p*n* identifier indicates the revision status of the product described in this book, where:

r*n* Identifies the major revision of the product.

p*n* Identifies the minor revision or modification status of the product.

Intended audience

This book is written for system designers, system integrators, and verification engineers who are designing a *System-on-Chip* (SoC) device that uses the TZC-400. The manual describes the external functionality of the TZC-400.

Using this book

This book is organized into the following chapters:

Chapter 1 *Introduction*

Read this for an overview of the TZC-400 and a description of its features.

Chapter 2 *Functional Description*

Read this for a description of the major interfaces and the functional operation of the TZC-400.

Chapter 3 *Programmers Model*

Read this for a description of the memory map and registers, including test registers, of the TZC-400.

Appendix A *Signal Descriptions*

Read this for a description of the input and output signals of the TZC-400.

Appendix B *Revisions*

Read this for a description of the technical changes between released issues of this book.

Glossary

The *ARM® Glossary* is a list of terms used in ARM documentation, together with definitions for those terms. The *ARM® Glossary* does not contain terms that are industry standard unless the ARM meaning differs from the generally accepted meaning.

See *ARM® Glossary*, `http://infocenter.arm.com/help/topic/com.arm.doc.aeg0014-/index.html<no value>`.

Conventions

Conventions that this book can use are described in:

- *Typographical conventions* on page vii.
- *Timing diagrams* on page vii.
- *Signals* on page viii.

Typographical conventions

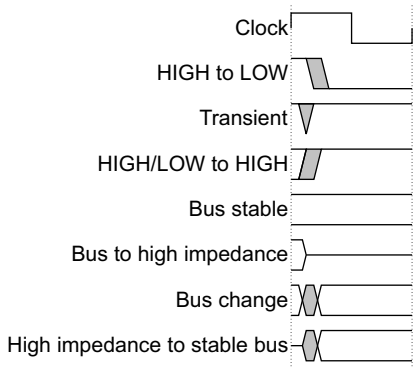
The following table describes the typographical conventions:

Style	Purpose
italic	Introduces special terminology, denotes cross-references, and citations.
bold	Highlights interface elements, such as menu names. Denotes signal names. Also used for terms in descriptive lists, where appropriate.
`monospace`	Denotes text that you can enter at the keyboard, such as commands, file and program names, and source code.
`mono`space	Denotes a permitted abbreviation for a command or option. You can enter the underlined text instead of the full command or option name.
`monospace` *`italic`*	Denotes arguments to monospace text where the argument is to be replaced by a specific value.
`monospace bold`	Denotes language keywords when used outside example code.
<and>	Encloses replaceable terms for assembler syntax where they appear in code or code fragments. For example: `MRC p15, 0 <Rd>, <CRn>, <CRm>, <Opcode_2>`
SMALL CAPITALS	Used in body text for a few terms that have specific technical meanings, that are defined in the *ARM® glossary*. For example, IMPLEMENTATION DEFINED, UNKNOWN, and UNPREDICTABLE.

Timing diagrams

The figure named *Key to timing diagram conventions* explains the components used in timing diagrams. Variations, when they occur, have clear labels. You must not assume any timing information that is not explicit in the diagrams.

Shaded bus and signal areas are undefined, so the bus or signal can assume any value within the shaded area at that time. The actual level is unimportant and does not affect normal operation.



Key to timing diagram conventions

Timing diagrams sometimes show single-bit signals as HIGH and LOW at the same time and they look similar to the bus change shown in *Key to timing diagram conventions*. If a timing diagram shows a single-bit signal in this way then its value does not affect the accompanying description.

Signals

The signal conventions are:

Signal level The level of an asserted signal depends on whether the signal is active-HIGH or active-LOW. Asserted means:
- HIGH for active-HIGH signals.
- LOW for active-LOW signals.

Lower-case n At the start or end of a signal name denotes an active-LOW signal.

Additional reading

This section lists publications by ARM and by third parties.

See Infocenter, http://infocenter.arm.com, for access to ARM documentation.

ARM publications

This book contains information that is specific to this product. See the following documents for other relevant information:

- *ARM® AMBA® AXI and ACE Protocol Specification* (ARM IHI 0022).
- *ARM® AMBA® APB Protocol Specification* (ARM IHI 0024).

The following confidential books are only available to licensees:

- *ARM® CoreLink™ TZC-400 TrustZone® Address Space Controller Integration Manual* (ARM DIT 0042).
- *ARM® CoreLink™ TZC-400 TrustZone® Address Space Controller Implementation Guide* (ARM DII 0287).
- *ARM® CoreLink™ TZC-400 TrustZone® Address Space Controller Supplement to AMBA® Designer ADR-400 User Guide* (ARM DSU 0024).
- *ARM® CoreLink™ QVN Protocol Specification* (ARM IHI 0063).

  Note

  The *ARM® CoreLink™ QVN Protocol Specification* is available from ARM. This is a confidential document and a separate license is required.

- *Trusted Base System Architecture CLIENT1* (ARM DEN 0007).

  Note

  This document describes designing a TrustZone secure system. It is available only to licensees of ARM TrustZone technology.

Other Publications

This section lists relevant documents published by third parties:

- *JEDEC Solid State Technology Association, Standard Manufacture's Identification Code*, JEP106.

Feedback

ARM welcomes feedback on this product and its documentation.

Feedback on this product

If you have any comments or suggestions about this product, contact your supplier and give:

- The product name.
- The product revision or version.
- An explanation with as much information as you can provide. Include symptoms and diagnostic procedures if appropriate.

Feedback on content

If you have comments on content, send an e-mail to `errata@arm.com`. Give:

- The title.
- The number, ARM DDI 0504C.
- The page numbers to that your comments apply to.
- A concise explanation of your comments.

ARM also welcomes general suggestions for additions and improvements.

Note

ARM tests the PDF only in Adobe Acrobat and Acrobat Reader, and cannot guarantee the quality of the represented document when used with any other PDF reader.

Chapter 1
Introduction

This chapter introduces the TZC-400. It contains the following sections:

1.1 About the TZC-400

The *CoreLink TZC-400 TrustZone Address Space Controller* (TZC-400) is an AMBA compliant *System-on-Chip* (SoC) peripheral. It performs security checks on transactions to memory or peripherals. You can use the TZC-400 to create up to eight separate regions in the address space, each with an individual security level setting. Any transactions must meet the security requirements to gain access to the memory or peripheral. You can program the base address, top address, enable, and security parameters for each region.

For more information about designing TrustZone systems, see *ARM publications* on page viii.

The TZC-400 is a high-performance, area-optimized address space controller. The TZC-400 supports several different AMBA interfaces. See *Compliance* on page 1-4.

1.1.1 TZC-400 overview

The TZC-400 operates between ACE-Lite masters and ACE-Lite slaves in a TrustZone system and filters bus accesses from masters to slaves. It performs filtering based on security requirements specified for address regions. You can program the eight TZC-400 address regions with varying security requirements for your intended application.

You can program the TZC-400 to report faults using the ACE-Lite response channel or interrupts.

Figure 1-1 shows a high-level view of the TZC-400 with a control unit and between one and four filter units.

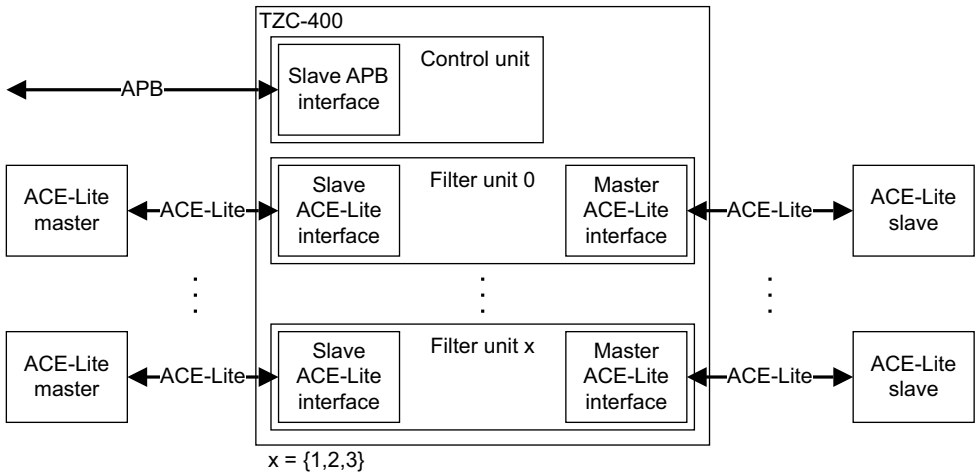


Figure 1-1 TZC-400 overview

Filter units perform security checks. Each filter unit has an ACE-Lite slave interface and an ACE-Lite master interface. All filter units operate from one set of shared region configuration registers. This ensures consistency across all filter units.

The *Fast Path IDentity* (FPID) inputs indicate to the filter units that they must handle an access with lower latency than for a normal path access. See *Fast Path IDentity inputs* on page 2-7. The *Non-Secure Access IDentity* (NSAID) input identifies the source interface of a transaction to a filter unit. See *Non-Secure Access IDentity inputs* on page 2-8.

Each filter unit operates in its own clock domain and has an AXI low-power interface for use in your clock gating strategy. Each domain can operate asynchronously from all other domains.

The APB interface of the control unit enables you to program the security setting and the addresses of each region. The control unit also has an AXI low-power interface for use in your clock gating strategy

1.1.2 TZC-400 example system

Figure 1-2 shows the TZC-400 in an example system with two filter units.

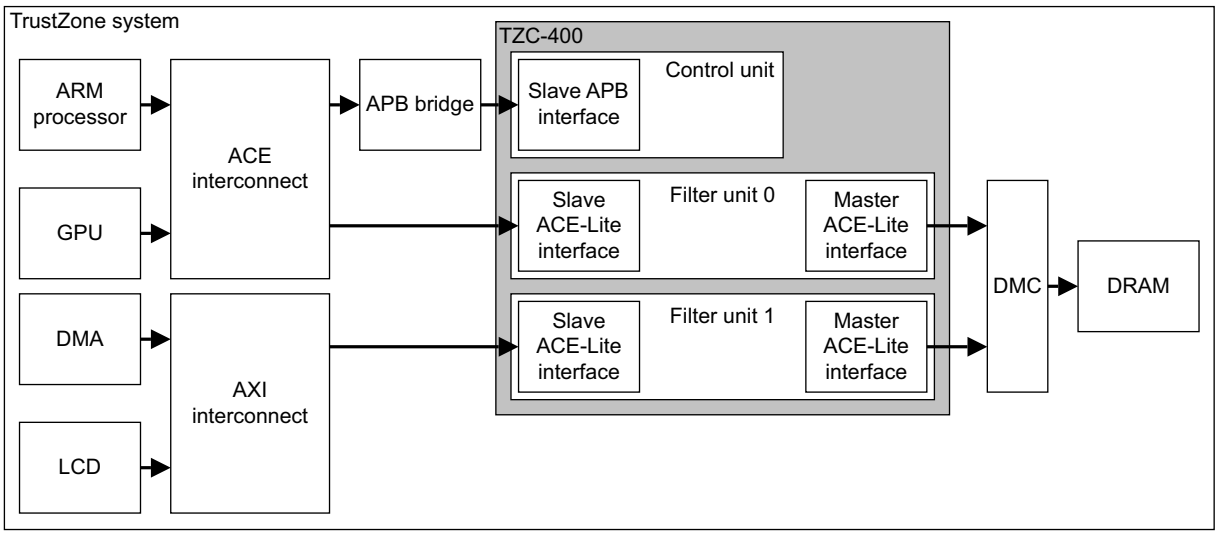


Figure 1-2 TZC-400 example system

This example has two filter units because there are two ACE-Lite paths into the *Dynamic Memory Controller* (DMC). The two paths are:

- One from the AXI interconnect that connects to the DMA and LCD AXI masters.
- The other from the ACE interconnect, that connects to the processor and the *Graphics Processor Unit* (GPU) ACE and ACE-Lite masters.

Both ACE-Lite master interfaces connect to a DMC. This provides complete control of accesses to DRAM.

1.2 Compliance

The TZC-400 complies with, or includes, components that comply with the following specifications:

- AMBA ACE-Lite.
- AMBA AXI4.
- AMBA AXI3.
- AMBA APB4.
- *QoS Virtual Networks* (QVN).

Note

- The *ARM® CoreLink™ QVN Protocol Specification* is available from ARM. This is a confidential document and a separate license is required.

This TRM complements the architecture reference manuals, architecture specifications, protocol specifications, and relevant external standards. It does not duplicate information from these sources.

1.3 Features

The TZC-400 provides the following key features:

- The ability to define up to eight address regions in the address map.
- A default base region to cover all remaining portions of the address map.
- Software programmable security access permissions for each address region through an APB4 interface. This includes the default base region, Region 0.
- Filter units only allow data transfer between an ACE-Lite master and an ACE-Lite slave if the security status of the ACE-Lite transaction and its identity match the security settings of the memory region it addresses.
- Common region configuration register settings shared between multiple filter units.
- The filter units can support asynchronous clocks that are independent of each other and of the control unit that is clocked by the APB interface clock.
- Dual read access path:
  - Fast path for low-latency accesses but with limited outstanding access support.
  - Normal path for accesses with a much higher outstanding access support.
- Identity-based filtering of Non-secure accesses.
- Reporting and interrupt signaling that is configurable from software to manage failed permission checks.
- Speculative accesses to support QVN and fast path. This feature can be disabled.
- AXI low-power interface for each clock domain.
- Gate keeper to allow or block accesses to each filter unit.
- Support for 256 outstanding transactions on the normal paths.

1.4 Interfaces

The TZC-400 provides the following external interfaces:

- *Clock and reset signals* on page 2-2.
- *AXI low-power interface signals* on page 2-3.
- *ACE-Lite interfaces* on page 2-4.
- *QoS Virtual Networks interface* on page 2-5:
  - *QVN enable signal and Fast Path Virtual Network Selection signals* on page 2-6.
- *APB slave interface* on page 2-6.
- *Identity input signals* on page 2-7:
  - *Fast Path IDentity inputs* on page 2-7.
  - *Non-Secure Access IDentity inputs* on page 2-8.
- *Interrupt signal* on page 2-8.

1.5 Configurable options

Table 1-1 shows the options that the TZC-400 implementer can configure. All options apply to the entire TZC-400 and cannot be changed for individual filter units.

Table 1-1 Configurable parameters

Option	Parameter	Values
Number of filter units	-[a]	1, 2, or 4
ACE-Lite address bus width	ADDR_WIDTH	32, 36, 40, 48, or 64 bits
ACE-Lite data bus width	DATA_WIDTH	32, 64, 128, or 256 bits
ACE-Lite transaction ID width	ID_WIDTH	2-24 bits
ACE-Lite USER bus width	USER_WIDTH	2-64 bits
Number of fast path outstanding read accesses	NUM_OUTSTAND	8, 16, or 32
ACE-Lite read address channel fast path register slice	FASTPATH_SLICE	Absent or Present
ACE-Lite read data channel register slice	RCHANNEL_SLICE	Absent or Present

a. This option can only be configured within AMBA Designer. See *ARM® CoreLink™ TZC-400 TrustZone® Address Space Controller Supplement to AMBA® Designer ADR-400 User Guide*.

1.6 Test features

The TZC-400 has no test features.

1.7 Product documentation, design flow, and architecture

The TZC-400 documentation is as follows:

Technical Reference Manual

The *Technical Reference Manual* (TRM) describes the functionality and the effects of functional options on the behavior of the TZC-400. This information is useful at all stages of the design flow. The choices that you make in the design flow can mean that some behavior that the TRM describes is not relevant. If you are programming the TZC-400 then contact:

- The implementer to determine the build configuration of the implementation.
- The integrator to determine the pin configuration of the device that you are using.

Integration Manual

The *Integration Manual* (IM) describes how to integrate the TZC-400 into a *System-on-Chip* (SoC). It includes a description of the signals that the integrator must tie off to integrate and configure the design. Some of the integration is affected by the configuration options you use when you generate the TZC-400 RTL.

The IM is a confidential book that is only available to licensees.

Implementation Guide

The *Implementation Guide* (IG) describes:

- Key implementation tasks.
- Product features to ease implementation.
- Information on the trial implementation flow.
- How to use the example scripts in the TZC-400.

The ARM product deliverables include reference scripts and information about how you use them to perform a trial implementation of your design.

The IG is a confidential book that is only available to licensees.

Supplement to AMBA Designer ADR-400 User Guide

The supplement describes how to use AMBA Designer to configure and generate the TZC-400 RTL.

The Supplement to AMBA Designer is a confidential book that is only available to licensees.

ARM recommends that you integrate the TZC-400 into your system prior to implementing the design. The implementation flow supplied with TZC-400 is for trial implementation only. However, there are mandatory implementation considerations that apply to the custom flow you use for your system. See the *ARM® CoreLink™ TZC-400 TrustZone® Address Space Controller Implementation Guide*.

1.8 Product revisions

This section describes the differences in functionality between product revisions:

r0p0 First release.

r0p0-r0p1 Updated the revision field for the Peripheral ID 2 register. See *Peripheral ID 2 register bit assignments* on page 3-22.

Chapter 2
Functional Description

This chapter describes the functionality of the TZC-400. It contains the following sections:

2.1 TZC-400 interfaces

Figure 2-1 shows the interfaces of the TZC-400.

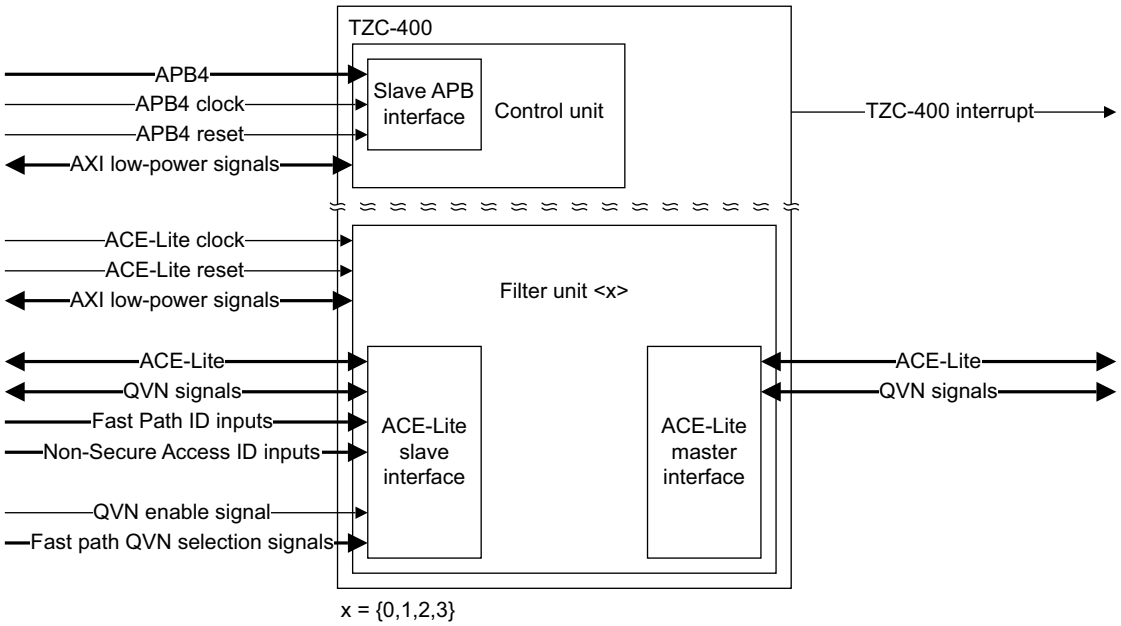


Figure 2-1 TZC-400 interfaces

The TZC-400 provides the following interfaces:

- *Clock and reset signals*.
- *AXI low-power interface signals* on page 2-3.
- *ACE-Lite interfaces* on page 2-4.
- *QoS Virtual Networks interface* on page 2-5:
  - *QVN enable signal and Fast Path Virtual Network Selection signals* on page 2-6.
- *APB slave interface* on page 2-6.
- *Identity input signals* on page 2-7:
  - *Fast Path IDentity inputs* on page 2-7.
  - *Non-Secure Access IDentity inputs* on page 2-8.
- *Interrupt signal* on page 2-8.
- *Revision AND configuration signal* on page 2-8.

2.1.1 Clock and reset signals

The TZC-400 contains the following clock domains:

- The **PCLK** domain for the control unit containing the APB interface.
- An ACE-Lite clock domain for each filter unit **ACLK<x>**, where <*x*> is the associated filter unit number. All clocks are asynchronous to each other and asynchronous to **PCLK**.

Reset signals

The TZC-400 provides an asynchronous reset input for each clock.These are:

- A reset input, **PRESETn**, for logic in the **PCLK** domain.

- A reset input, **ARESET<x>n**, for each **ACLK<x>**, where <*x*> is the associated filter unit number.

2.1.2 AXI low-power interface signals

- You can use the AXI low-power interface signals to indicate when it is safe to turn off the clocks of each clock domain. The signals indicate whether the domain is active or idle and control entry and exit from a low-power state. For more information on the AXI low-power interface, see the *ARM® AMBA® AXI and ACE Protocol Specification*.

The TZC-400 implements the following signals for the control unit and each filter unit. <*x*> is replaced by `APB` for the control unit, or by the filter unit number:

CSYSREQ<x> Set this input to LOW to request that the logic in the clock domain must take action to enter an idle state.The clock domain must be in an idle state before you can turn off the clock to that domain. During normal operation, **CSYSREQ<x>** is HIGH.

CSYSACK<x> This is an output from the TZC-400:

- TZC-400 drives **CSYSACK<x>** LOW in response to a request to enter the low-power state from a clock controller driving **CSYSREQ<x>** LOW. When TZC-400 drives **CSYSACK<x>** LOW, this indicates that the filter unit is ready to enter a low-power state and that the associated clock to this filter unit can be safely turned off.
- TZC-400 drives **CSYSACK<x>** HIGH in response to a request to exit the low-power state The system clock controller initiates this process by driving **CSYSREQ<x>** HIGH. When TZC-400 drives **CSYSACK<x>** HIGH, the associated clock to this filter unit is running and the TZC-400 operates as programmed.

CACTIVE<x> This is an output from the TZC-400. When HIGH, it indicates that you must supply the clock to the logic within the associated clock domain and complete the low-power exit sequence. When LOW, it indicates that the logic within the clock domain is idle. Your system clock controller can use this as a hint to initiate a low-power request using the **CSYSREQ<x>** signal.

Note

- You must use the entry and exit sequences of the AXI low-power interface and not use **CACTIVE<x>** to directly gate the TZC-400 clock.
- TZC-400 does not support the denial of low-power requests. Therefore, you do not have to evaluate **CACTIVE<x>** in your system clock controller when considering the **CSYSREQ<x>** and **CSYSACK<x>** handshake.

Figure 2-2 on page 2-4 shows the AXI low-power interface signals, and how they connect to the control and filter units in the TZC-400.

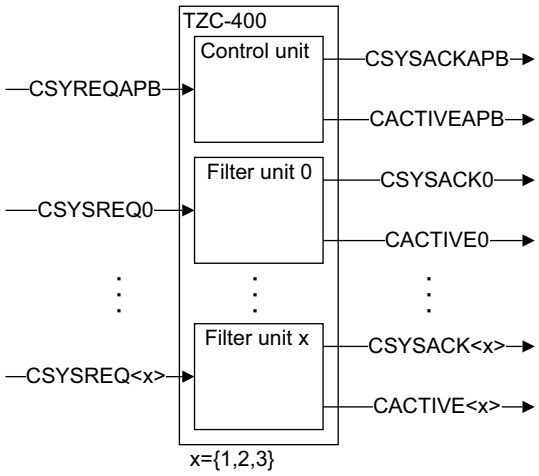


Figure 2-2 AXI low-power interface signals in the TZC-400

2.1.3 ACE-Lite interfaces

The TZC-400 provides the following ACE-Lite interfaces:

- ACE-Lite slave interface.
- ACE-Lite master interface.
- These interfaces exist as pairs of a single slave and a single master interface. Each pair is associated with a single filter unit. Each ACE-Lite interface implements all ACE-Lite channels. See the *ARM® AMBA® and ACE Protocol Specification*.

Each filter unit includes an ACE-Lite slave interface and an ACE-Lite master interface. The signals on each interface include a suffix of S<x> and M<x>, where:

- S identifies a slave interface.
- M identifies a master interface.
- <x> is the filter unit number.

The ACE-Lite slave and master interfaces also support QVN. When **QVNENABLE<x>** is set, the QVN tokens and the associated address or write data can be temporarily stalled in certain circumstances. For more information, see *QoS Virtual Networks interface* on page 2-5.

Table 2-1 shows the ACE-Lite slave and master interface attributes. To permit performance optimization, you must specify them for every component with an ACE-Lite interface:

Table 2-1 ACE-Lite interface attributes

Attribute	Definition	Value
Read acceptance capability.	The maximum number of active read transactions that the interface can accept. You must specify this if the combined acceptance capability is not specified.	256 on the normal path, plus the configured outstanding access value of the fast path. This can be 8,16, or 32. **Note** Each path only supports its respective outstanding access limit.
Write acceptance capability.	The maximum number of active write transactions that the interface can accept. You must specify this if the combined acceptance capability is not specified.	256.
Combined acceptance capability.	The maximum number of active transactions that the interface can accept. It is specified for slave interfaces that use combined storage for active write and read transactions. If not specified then you can assume it is equal to the sum of the write and read acceptance capabilities.	Equal to the read acceptance capability plus the write acceptance capability.

The ACE-Lite slave interface can connect to AXI4 and AXI3 master interfaces. You must tie unused AXI and ACE-Lite signals appropriately. See the *ARM® CoreLink™ TZC-400 TrustZone® Address Space Controller Integration Manual*.

- TZC-400 does not support write data interleaving, and write data is issued in the same order as write addresses. AXI4 and ACE-Lite protocols do not support lock transactions. See *ARM® AMBA® AXI and ACE Protocol Specification*.

2.1.4 QoS Virtual Networks interface

QVN support is available in TZC-400 and prevents congestion between traffic flows in a system. The implementer of the TZC-400 configuration must enable *Virtual Network* (VN) functionality for TZC-400 to support QVN. If you use the fast path functionality and require VN traffic to travel over the fast path, then you must select a single VN to use the fast path, otherwise blocking can occur.

TZC-400 passes all VN signals through unmodified, except in the following cases:

- When it blocks a write data token grant to prevent write data arriving before a write address.
- When it blocks a read address token grant to avoid exceeding the configured number of outstanding transactions that can use the fast path.

For more information on QVN, see *Additional reading* on page viii.

QVN enable signal and Fast Path Virtual Network Selection signals

A system implementer can enable or disable QVN functionality on a per filter unit basis. Ensure QVN is enabled if you want to use QVN functionality. You can use the **QVNENABLE<x>** configuration signal, where <*x*> represents the filter unit number, to enable or disable QVN as follows:

- When set HIGH, QVN support is enabled. This makes all token request channels operational. All access using the fast path must then use the VN selected by **FPVNSEL<x>**. QVN support relies on speculative access. Therefore, speculative access must be supported by the destination for the QVN traffic. See *Speculative accesses* on page 2-13.
- When set LOW, QVN support is disabled. All token request channels pass through the filter unit without modification.

The fast path Virtual Network selection 2-bit configuration signal, **FPVNSEL<x>** selects the VN number to use for fast path accesses that operate with QVN tokens. This enables the filter unit to control the number of read channel tokens issued and therefore to prevent the reception of more outstanding read transactions on the fast path than the filter unit can support.

Use the fast path Read token pre-allocate configuration signal, **FPQVNPREALLOC<x>**, to define whether the read token for the Virtual Network selected by **FPVNSEL<x>** is already pre-allocated upstream at reset:

- When set LOW, TZC-400 assumes that no read token is pre-allocated at reset for the Virtual Network that **FPVNSEL<x>** selects.
- When set HIGH, TZC-400 assumes that only one read token is pre-allocated at reset for the Virtual Network that **FPVNSEL<x>** selects.

When using QVN the filter unit performs speculative accesses. This way the master and slave interfaces connected to the filter unit can handle token requests and grants directly with each other. However, the TZC-400 blocks these token requests and grants on the following occasions:

- **VWVALID** and **VWREADY** of any of the four Virtual Networks can be set LOW by the filter unit to prevent a write data packet from arriving at the TZC-400 if it has not had its associated write address issued by the TZC-400.
- **VARVALID** and **VARREADY** of the VN selected by **FPVNSEL<x>** can be gated by a filter unit when a fast path only supports up to N outstanding transactions on the VN that is selected to use the fast path and the limit of N outstanding transactions is reached on that path. N is the configured number of outstanding transactions for the fast path. For this to work correctly, all accesses that use a fast path must be issued using the selected VN.

  Note

  If fast path accesses are sent on another VN, the filter unit is unable to prevent the number of outstanding accesses exceeding the configured limit of the filter unit. This can result in temporary head-of-line blocking of QVN accesses on the remaining VN paths.

When QVN support is disabled, the filter unit does not block signals on the token request channels.

2.1.5 APB slave interface

- Program the TZC-400 registers and obtain status through the APB slave interface. See *Register summary* on page 3-3. The TZC-400 supports the AMBA APB4 protocol. See the *ARM® AMBA® APB Protocol Specification*.

All control registers are Secure access only. The TZC-400 returns error responses for all Non-secure accesses. It ignores Secure accesses that target reserved areas of the register map and writes to read-only registers. The TZC-400 does not send an error response in these cases.

The TZC-400 also uses APB clock and reset signals. See *Clock and reset signals* on page 2-2.

2.1.6 Identity input signals

The TZC-400 provides the following identity inputs for each filter unit:

- *Fast Path IDentity inputs*.
- *Non-Secure Access IDentity inputs* on page 2-8.

Figure 2-3 shows how the TZC-400 uses FPIDs and NSAIDs. <*x*> is replaced by the number of the filter unit.

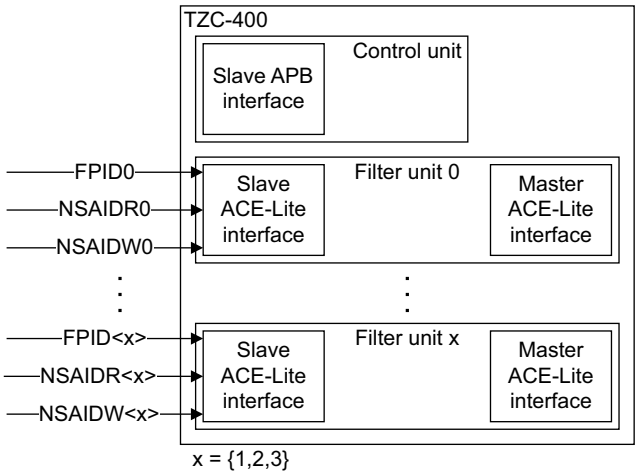


Figure 2-3 TZC-400 using FPIDs and NSAIDs

Fast Path IDentity inputs

The *Fast Path IDentity* (FPID) inputs determine whether read transactions take the lower latency path or the normal path through a filter unit. See *Fast path selection* on page 2-14.

Each filter unit has a single-bit FPID input, **FPID<x>**, where <*x*> is the filter unit number. The fast path relies on speculative access. You must enable speculative access for the master interface and the slave to use the fast path. If **FPID<x>** is HIGH during a read transaction on the ACE-Lite slave interface of the filter unit, the filter unit routes the access through the fast path. If speculative access is disabled, the filter unit routes the access through the normal path.

When **QVNENABLE<x>** is HIGH, all accesses using a fast path on a particular filter unit must only use the Virtual Network selected by the associated fast path Virtual Network selection signal, **FPVNSEL<x>**. This enables the read token handshake signals to control the number of outstanding accesses that use the fast path. Otherwise, the TZC-400 temporarily blocks all AR access through the filter unit, if the number of fast path accesses exceeds the number of outstanding transactions that the fast path can support. This can have a large impact on the throughput and latency of unrelated accesses of other virtual networks on the same interface.

Non-Secure Access IDentity inputs

When in Non-secure state the *Non-Secure Access IDentity* (NSAID) inputs identify the master that is the source of the access. See *Access permissions to regions* on page 2-11. Each filter unit has two NSAID bus inputs of 4 bits, one associated with read addresses, **NSAIDR<x>[3:0]**, and the other associated with write addresses, **NSAIDW<x>[3:0]**, where <*x*> is the filter unit number.

2.1.7 Interrupt signal

You can program the TZC-400 to assert **TZCINT** when an access fails its security check. See *Denied ACE-Lite transactions* on page 2-16.

2.1.8 Revision AND configuration signal

The TZC-400 provides a 4-bit input signal, **USERPID3REVAND**. This defines the value of the `RevAnd` field in the Peripheral ID 3 register. See *Peripheral ID 3 register* on page 3-23. Normally these values are all LOW. However, you can tie off to other values to reflect the implementation changes to the TZC-400.

2.2 TZC-400 operation

This section describes the operation of the TZC-400. It contains the following sections:

2.2.1 Access filtering with regions

The TZC-400 enables you to program the access permissions for each region. A region is a contiguous area in the address space with a defined start and end. Each region has a security level setting. A bus access must meet this security level to be given access to the required resource. The TZC-400 supports nine regions:

- One base region, Region 0, that is partially programmable from software.
- Eight other regions, Regions 1-8, that are fully programmable from software.

The security state of transactions is indicated by the **ARPROTS<x>[1]** or **AWPROTS<x>[1]** signals, where a value of 0 indicates a Secure access. The TZC-400 uses the NSAID values to identify the source of the transaction.

Through the control unit, you can program the security setting and addresses of each region. The filter units perform security checking when a master tries to access the memory region of a slave. The filter units share the same control unit but operate independently from each other. They can also operate in asynchronous clock domains.

The filters use the NSAID inputs to filter Non-secure accesses based on the source of the access. See *Non-Secure Access IDentity inputs* on page 2-8.

Region 0 is the default region. It covers any memory space that is not part of another region.

You can define a region and then disable checking of that region in software. You can do this independently for each filter unit.

Region access rules

The TZC-400 implements the following region rules:

- A region must be enabled for a filter unit to provide a valid match.
- Region 0 is always enabled.
- TZC-400 checks the access against Region 0 security settings only if the access cannot be found in any of the other enabled regions for that filter unit.
- Where an address maps to region 1 or higher, TZC-400 checks the access against the security settings of that region.
- For region 1 and higher, any enabled region in a filter unit must not overlap memory areas from another enabled region in the same filter unit.

Note

- Other regions can overlap the address area of Region 0. You can use an overlap between Region 0 and a higher region to manage all access rights for a Secure OS, by defining the security of the default region, Region 0, and then defining security for higher regions overlapping the default base region. For example, you can make Region 0 inaccessible to any Non-secure masters. The Secure OS can then selectively release regions for global access later.
- Regions 1 and higher can have address regions that overlap with each other, but only if they are set for different filters.
- The behavior of the TZC-400 is UNDEFINED for configurations where Regions 1 and higher overlap when enabled on the same filter unit. When an access to an overlapping region occurs, the TZC-400 sets a status bit to indicate an overlapping access. The TZC-400 can generate an interrupt when this occurs. Interrupt generation is a programmable feature of the TZC-400. See *Action register* on page 3-6.

Example region setup

Figure 2-4 shows an example security configuration with Regions 0-3.

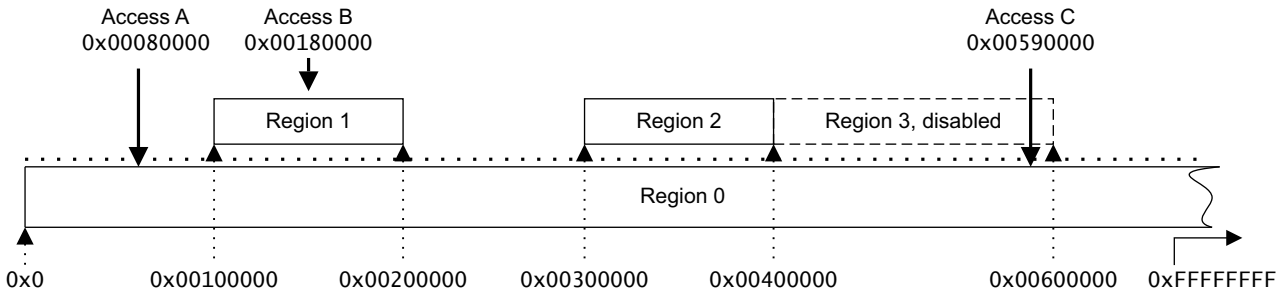


Figure 2-4 Region mapping example on a 32-bit address map for a filter unit

In this example Region 3 is disabled, and Region 1 and Region 2 are enabled.

Access A is mapped to Region 0 because its address is not in the regions that Regions 1-3 define.

Access B is mapped to Region 1.

Access C is mapped to Region 0 because Region 3 is not enabled.

Region setup

Table 2-2 describes the programmable parameters for Region 0 and Regions 1-8, respectively.

Table 2-2 Programmable parameters of regions

Parameter	Description	Value for Region 0	Value for Region 1 - Region 8
Region enables.	Enables and disables access checking for each filter unit and each region.	Always enabled for all filter units.	Programmable.
Secure access permissions.	Defines the Secure read and write permissions for the region.	Programmable.	Programmable.
Base address.	Defines the start address of the region, and is aligned to a 4KB boundary.	0[a].	Programmable.
Top address.	Defines the top address of the region, and is aligned to the top byte address of a 4KB region.	All bits are set to 1[a].	Programmable.
Non-secure ID filtering.	Defines the region to permit Non-secure read or write accesses to. This is based on the values of the **NSAIDR<x>** and **NSADIW<x>** inputs of each filter unit. See: • *Region ID access register* on page 3-18. • *Access permissions to regions*.	Programmable.	Programmable.

a. This means that Region 0 occupies the entire memory space.

Access permissions to regions

You must program access permissions separately for Secure access and Non-secure access.

Each region contains the following configuration registers:

- *Region attributes register* on page 3-17.
- *Region ID access register* on page 3-18.

Table 2-3 shows the region settings that you can define for Secure read and Secure write enables and relates this to the outcome that a Secure access can achieve. <*n*> is the filter unit number.

Table 2-3 Permissions for Secure accesses

Region parameters		Resulting permissions that grant access	
REGION_ATTRIBUTES_<n>.s_wr_en	REGION_ATTRIBUTES_<n>.s_rd_en	Secure write	Secure read
0	0	No	No
0	1	No	Yes
1	0	Yes	No
1	1	Yes	Yes

You must explicitly program a region to be granted Secure access if it is required, regardless of the settings for Non-secure reads and Non-secure writes. For example, when permissions are set so that a Non-secure read or Non-secure write access is permitted, it does not mean that the corresponding Secure read or Secure write access is also automatically granted.

Figure 2-5 shows how Non-secure enables and NSAIDs affect access permissions for Non-secure accesses.

If the access is a Non-secure write access at the filter unit <x>, use the flow diagram for write access on the left.

If the access is a Non-secure read access at the filter unit <x>, use the flow diagram for read access on the right.

Use the following replaceable terms when reading Figure 2-5:

- <*M*> is the region that the access resides in.
- <*x*> is the filter unit number.

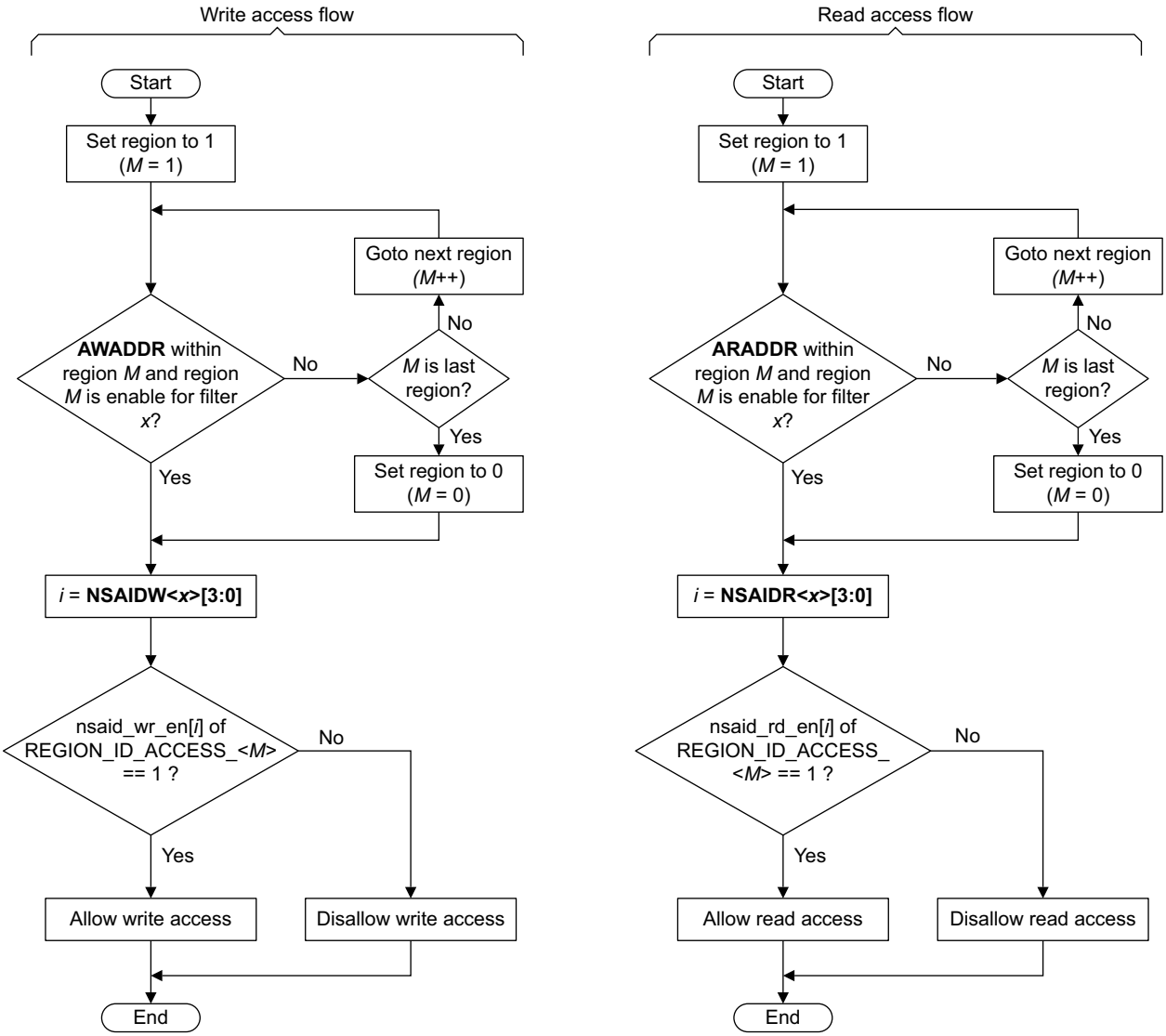


Figure 2-5 Non-secure accesses

For each type of access, the filter unit checks whether the Non-secure access address resides in any region between 1 and 8 that is enabled for that filter. If the filter finds a match, then it uses that region. Otherwise, the filter selects the default region 0. The filter uses the NSAID value associated with the access to select the nsaid_en bit in the REGION_ID_ACCESS register for the selected region. If that bit is 1, then the filter grants Non-secure access. Otherwise, if that bit is 0, then the filter denies the Non-secure access.

The **NSAIDR<x>** and **NSAIDW<x>** inputs uniquely identify a master or a group of masters.

A value of zero on the **NSAIDR<x>** and **NSAIDW<x>** inputs is the default ID.

Assign the default ID of zero to any master interface in the system that is either:

- Not required to be identified separately from others in the system.
- Not assigned a master ID.

When the filter unit detects that an access falls into an overlapping address area that two enabled regions define, it sets the overlap status bit in the Interrupt Status Register. The only exception to this is if the overlap only occurs with Region 0. In this case the filter unit does not change the overlap status bit in the Interrupt Status Register. See *Interrupt status register* on page 3-8.

Note

If there are components in your system that store ACE-Lite signals, but do not store the NS bit or the NSAID value for a transaction, then this might cause an unexpected response to one or more transactions. The unexpected response can either be the result of blocking a valid transaction or permitting a transaction that violates the security of the design. This is because any caching or buffering in the system might disassociate the intended security information from that associated transaction. This temporal separation of security settings from the associated transaction means that the TZC-400 receives security information that relates to a different transaction. You must resolve any such issues at a system level as TZC-400 cannot take responsibility for this issue.

2.2.2 Speculative accesses

The default behavior of the TZC-400 is to perform speculative accesses. You can disable speculative accesses if they have detrimental side effects, or might affect system security. See the *Speculation control register* on page 3-7.

An example of where speculative reads are a security risk is when TZC-400 is protecting a peripheral that has a simple register interface to push or pop a FIFO. A read or write access with insufficient security (failed access) must not progress to the peripheral. If a transaction did progress because of speculation, this would allow an unintended entry push or pop to occur and potentially break the Secure access control required for that peripheral.

When speculative access is enabled, the TZC-400 continues to allow accesses that fail security checks to progress through to the external slave interface. If this happens, the TZC-400 ensures that any read data, write data, and write enables are set to zero, so that no data is visible and no write transaction occurs.

Note

When a filter unit supports QVN, **QVNENABLE<x>** must be set HIGH. When **QVNENABLE<x>** is HIGH, the filter unit ignores the settings in the Speculation Control Register and always performs speculative accesses.

You must enable speculative access in the TZC-400 when support for QVN is enabled. This is because an access that is issued as a result of a granted QVN token from a downstream slave must arrive at the slave interface that granted the token. If, however, speculative access is not required or is undesirable when not supporting QVN, you can program the Speculation Control Register to disable speculative access for read or write separately. See *Speculation control register* on page 3-7.

2.2.3 Fast path selection

In each filter, the TZC-400 has two different read paths to support different latency and outstanding access requirements:

Fast Path This path provides the lowest possible access latency through a filter unit and supports a limited number of outstanding accesses. You can configure the fast path to support up to 32 outstanding accesses.

The fast path relies on speculative access and can only be used if speculative accesses are enabled in the filter.

Normal Path All other accesses that do not use the fast path use this path. This path supports a greater number of outstanding accesses. Accesses going through this path incur additional clock cycles of latency in comparison with the fast path.

For read accesses, the FPID signals determine whether an access uses the fast path or the normal path. Each filter unit has a single FPID signal. When set HIGH during a read address, the read address is routed using the fast path.

Note

In addition to the latency shown for the fast or normal path, the sending of an address and the return of data can each incur an additional cycle of latency. Whether or not either of these additional cycles occurs depends on the implementation of your TZC-400 configuration.

ARM recommends that you use the fast path for accesses from masters that are adverse to increased latency. These types of masters are often called latency-intolerant masters. An example of a latency-intolerant master that can benefit is an application processor. Typically, an application processor stalls when the next instruction does not hit in its cache. In this situation, any additional latency of the memory subsystem directly affects the performance of the application processor.

When a filter unit supports QVN, with **QVNENABLE<x>** set HIGH, all accesses on the fast path must also use the Virtual Network selected by **FPVNSEL<x>**. This means that the token request and grant channels for that Virtual Network can be monitored, and blocked to prevent the fast path from receiving more outstanding transactions than the number supported by the filter unit. Failing to do this for Virtual Network fast path accesses can result in temporary blocking of accesses on another Virtual Network when the number of outstanding accesses on the fast path exceeds the supported number of outstanding accesses.

See *Access latencies* on page 2-16.

2.2.4 Gate keeper

The TZC-400 implements gate keeper functionality on the ACE-Lite slave interface of each filter unit to permit or block accesses progressing through the filter unit. The two states are also called open and closed, respectively. You can use the gate keeper to suspend processing transactions immediately before changing region settings. See *Changing the programmers view on an active system* on page 2-18.

Each gate keeper provides an independent control bit in the GATE_KEEPER register, called open_request[<*x*>], where x is the filter unit number. This bit enables software to request the gate to open or close. An independent status bit, open_status[<*x*>], is also provided for each filter unit. This bit indicates whether the gate is open or closed. See *Gate keeper register* on page 3-6.

All open_request control bits default to zero at reset. To request access through a filter unit software must set the corresponding bit of open_request to 1. When set, the corresponding open_status bit transitions to 1 and then the gate keeper starts to permit accesses to pass through.

To request gate closure of a filter unit, software must set the corresponding bit of open_request to 0. When this occurs, the filter unit no longer permits any new access arriving on the AW and AR channels to progress to the filter unit. It also waits for all outstanding accesses that have already entered the filter unit to complete. This includes both those currently progressing through the filter unit and those already issued by the filter unit. When this has occurred, the corresponding open_status bit goes to 0.

Note

The gate keeper status register shows the gate of any filter unit as closed if that filter unit is currently in a low-power state. This only applies if you are using the AXI low-power interfaces and is irrespective of the programmed state of the gate keeper register. The programmed state stored in the control unit is restored when the filter unit exits from a low-power state.

2.2.5 Barriers

Transactions that arrive after a barrier is received do not proceed until all transactions preceding the barrier are sent, and then the barrier is sent.Then the transactions that arrived after the barrier are sent. This process applies irrespective of:

- The IDs of all transactions.
- The path each transaction takes through the TZC-400.

Barriers are handled in a different manner to other transactions in the TZC-400, with the following differences:

- Security checks are not performed on barrier transactions. This is because they do not contain an address and they do not transfer any data.
- Barriers are never sent along the fast path even if **FPID<x>** is set HIGH.

Note

TZC-400 treats each read and write channel independently. The downstream ACE-Lite slave is responsible for synchronizing reads with writes.

2.2.6 Lock transaction sequences

- The ACE-Lite and AXI4 protocols do not support locked transactions. Therefore, when using the AXI3 protocol on the ACE interface, you must not use lock transactions. See the *ARM® AMBA® AXI and ACE Protocol Specification*.

2.2.7 Exclusive accesses

If a master performs exclusive accesses to an address region, you must program the TZC-400 to permit read and write accesses to that address region for the expected security access settings. Otherwise, the read or write transaction might fail.

When a read exclusive access fails its security check, if the filter unit currently supports speculative reads, then the read exclusive access is sent as a read access with the **ARLOCKM<x>[0]** bit set to 0. However, a failed write exclusive access, when speculation is active, does not have its **AWLOCKM<x>[0]** bit cleared when the transaction is issued from the TZC-400.

All exclusive read accesses use the normal path regardless of the associated **FPID<x>** value.

2.2.8 Access latencies

Table 2-4 describes the minimum latencies of read and write access through the TZC-400.

Table 2-4 Minimum access latencies

Access type	Channel	Cycles of latency
Read access latencies	AR channel fast path	0 or 1[a]
	AR channel normal path	2
	R channel	0 or 1[b]
Write access latencies	AW channel	2
	W channel	0
	B channel	0

a. If FASTPATH_SLICE is configured as present then the latency for the read address channel is 1, otherwise it is 0.

b. If RCHANNEL_SLICE is configured as present then the latency for the read data channel is 1, otherwise it is 0.

2.2.9 Denied ACE-Lite transactions

If an ACE-Lite transaction has insufficient security privileges, then for:

Reads The TZC-400 responds to the master by setting all bits of the read data bus, **RDATAS<x>**, to zero. If you program the TZC-400 to perform speculative accesses, the TZC-400 still issues the read access, but its corresponding read data, **RDATAM<x>**, is discarded.

Note

For failed exclusive read accesses TZC-400 performs additional actions. See *Exclusive accesses* on page 2-15.

Writes The TZC-400 prevents the transfer of data from the master to the slave by discarding the data that **WDATAM<x>** contains. If you program the TZC-400 to perform speculative accesses, it modifies the transfer to the slave by setting all bits of the:

- Write data bus, **WDATAM<x>**, to zero.
- Write data strobe, **WSTRBM<x>**, to zero.

The action configuration register controls how the TZC-400 signals the region permission failure of an access. This does not include region overlap conditions. See *Action register* on page 3-6. The available response strategies of TZC-400 are:

OK and raise no interrupts

This enables the access to fail without permitting the read data to be returned or the write data to be committed. From the perspective of the master that issued the access, the access was permitted.

OK and raise an interrupt

This generates a bus response, in the same way as the OK, and raises no interrupts. However, TZC-400 generates an interrupt that must be routed to a Secure OS to notify it that a security violation has occurred.

Decode error and raise no interrupts

This enables the issuing master to behave as though the memory location is absent. The TZC-400 presents a DECERR response to indicate that the transaction has failed.

Decode error and raise an interrupt

This enables the issuing master to behave as though the memory location is absent. The TZC-400 presents a DECERR response and generates an interrupt that must be routed to a Secure OS to notify it that a security violation has occurred.

Even though the TZC-400 only has one interrupt signal, separate interrupt status, overflow, and clear bits are available for every filter unit. For information on controlling interrupt actions, see *Action register* on page 3-6.

For region overlap failure conditions, the bus response of the filter unit is unpredictable, but the overlap and status bits of the filter unit are set, and an interrupt is raised depending on the settings in the Action Register. See *Action register* on page 3-6. The FAIL status registers of the associated filter unit are set using values from the failed access.

2.2.10 Reset

The TZC-400 maintains a master copy of all region configurations in the configuration registers in the control unit. These are automatically copied across to any filter unit as soon as the filter exits reset. The filter unit blocks all accesses to the ACE-Lite slave interface while copying these settings over. When copying is complete, the TZC-400 starts permitting access through to the filter unit for permission checks.

2.3 Constraints of use

This section describes:

- *Changing the programmers view on an active system*.
- *Clock gating*.

2.3.1 Changing the programmers view on an active system

Consider the following if you want to change the programmers view on an active system:

- When you change the settings of a TZC-400 region:
  - If the current accepted ACE-Lite transaction falls into that region, it acts according to the previous settings for that region.
  - All other outstanding ACE-Lite transactions that fall into that region operate according to the new settings for that region.
  - This can generate unpredictable behavior relating to exactly when the hardware settings take affect and the phase that a transaction is in when the change occurs.
- ARM recommends, therefore, that no outstanding ACE-Lite transactions use the region when a change of setting is in progress. You can achieve this as follows:
  - Ensure that no access is sent to the region during the period when the region settings are being changed. However, the TZC-400 has no control over this and therefore the other masters in the system are responsible for this.
  - Software can use the gate keeper to request that all gates are closed. When all gate keeper status bits go to 0, there are no outstanding accesses and therefore changes to the regions can be made before opening the gates again.

    However, when the gates are closed, all accesses on all incoming ACE-Lite ports are blocked. This can potentially result in a system deadlock. This occurs if an access to the APB port of TZC-400 is blocked indirectly.

    For example, if a TZC-400 ACE-Lite slave port is the only method of reaching the TZC-400 APB port, then this means that when the gate keeper is closed traffic cannot pass through the ACE-Lite port and so you cannot reach the APB port to instruct the gate keeper to open. This results in the ACE-Lite slave interface being permanently closed to all other transactions, including your programming transactions.

    Note

    This only occurs in certain system architectures. Therefore, you must not architect your system in this way.

When there are no outstanding ACE-Lite transactions, the settings can be changed by writing to the TZC-400 APB interface. To ensure that all updates have been committed before starting transactions again, you must perform a read operation from the APB register in the TZC-400.

2.3.2 Clock gating

In this section, <*x*> denotes the number of the filter unit that each signal belongs to. The TZC-400 has a number of clock inputs that the system can gate independently. To achieve this, you must consider the following:

- If the **CACTIVE<x>** signal of a clock domain is HIGH, and the associated **CSYSREQ<x>** and **CSYSACK<x>** signals are LOW, the **CSYSREQ<x>** signal is expected to go HIGH after a reasonable time. This is a request to exit the low-power state.

If the **CSYSREQ<x>** signal is LOW and the TZC-400 drives the **CSYSACK<x>** signal LOW as a result. Then the TZC-400 must regard the clock to be unstable or off and therefore not begin normal operation. In this situation the following can occur:

— If the clock domain is the **PCLK** domain, transactions arriving on the APB interface are blocked. This can indirectly lead to a bus deadlock condition.

— If **PCLK** is running, but the clock of the filter unit that is the destination for the write transaction is not running, then a timeout can occur. The timeout is triggered if the filter unit clock and low-power exit sequence do not complete within 256 **PCLK** cycles. This might occur if the **CSYSREQ<x>** of the destination clock domain is being held LOW.

  When a timeout occurs no additional updates are issued to that filter unit until the filter unit requests a refresh from the control unit. The filter unit requests a refresh when the clock of the filter unit returns without **ARESET<x>n** being asserted.

  Note

  When a change of settings occurs, and a filter unit is in a low-power state, that filter unit does not instantaneously operate using the new settings. When exiting the low-power state, the filter unit settings are updated from the control unit settings over multiple clock cycles. If an access that would be denied by the new settings occurs before the completion of this process, then the access might be permitted to proceed. Therefore, the gate keeper must be used to close the gate, and you must check the status of the gate before any region settings are updated.

— If the clock domain is the **ACLK<x>** domain, transactions arriving on the ACE-Lite and VN token interface are blocked. This can indirectly lead to a bus deadlock condition.

Chapter 3
Programmers Model

This chapter describes the registers of the TZC-400 and provides information on how to program them. It contains the following sections:

3.1 About this programmers model

The following information applies to all registers:

- Do not attempt to access reserved or unused address locations. Attempting to access these locations can result in unpredictable behavior.
- Unless otherwise stated in the accompanying text:
  - Do not modify undefined register bits.
  - Ignore undefined register bits on reads.
  - All register bits are set to 0 by a system reset or a powerup reset.
- The following abbreviations describe the different access types:

  RW Read and write.

  RO Read-only.

  WO Write-only.
- The base address of the TZC-400 is not fixed, and can be different for any particular system implementation. The offset of each register from the base address is fixed.
- The TZC-400 always provides an error response to any Non-secure read or Non-secure write access. For Non-secure writes the write is never issued. For Non-secure reads the read data is always returned as zero.
- The TZC-400 always responds with an OKAY response to Secure accesses.
- Secure read accesses to reserved or unused address locations return zeros. The TZC-400 ignores Secure writes to reserved or unused address locations. ARM recommends that you avoid accessing these locations where possible to ensure that software written for the TZC-400 can remain compatible with future releases.
- Secure read accesses to reserved fields and unused bits in a partially used register always return zeros. The TZC-400 ignores Secure writes to these same areas.
- For register programming, the TZC-400 supports data in word-invariant endianness.
- System designers must ensure that only processors in Secure state can access the TZC-400 registers. Otherwise, it can compromise the security of the system.

Note

For more information about considerations relating to changing the programmers view of an active system, see *Constraints of use* on page 2-18.

3.2 Register summary

If a region or filter unit does not exist, the area containing configuration or status registers for that region or filter unit becomes a reserved area.

The register map of the TZC-400 spans 4KB.

Table 3-1 shows the registers offset from the base memory address.

Table 3-1 Register summary

Offset	Name	Type	Reset	Width	Description
The configuration, control, and interrupt registers define the global configuration and operation of the TZC-400.					
0x000	BUILD_CONFIG	RO	_[a]	32	*Build configuration register* on page 3-5
0x004	ACTION	RW	0x00000000	32	*Action register* on page 3-6
0x008	GATE_KEEPER	RW	0x00000000	32	*Gate keeper register* on page 3-6
0x00C	SPECULATION_CTRL	RW	0x00000000	32	*Speculation control register* on page 3-7
0x010	INT_STATUS	RO	0x00000000	32	*Interrupt status register* on page 3-8
0x014	INT_CLEAR	WO	0x00000000	32	*Interrupt clear register* on page 3-9
0x018 to 0x01C	-	-	-	-	Reserved
The fail status registers provide information about an access that fails because of insufficient permissions or an overlap condition. A separate set of fail status registers is provided for each filter unit.					
0x020+(0x10*<x>)[bc]	FAIL_ADDRESS_LOW_<x>	RO	0x00000000	32	*Fail address low register* on page 3-10
0x024+(0x10*<x>)[bc]	FAIL_ADDRESS_HIGH_<x>	RO	0x00000000	32	*Fail address high register* on page 3-11
0x028+(0x10*<x>)[bc]	FAIL_CONTROL_<x>	RO	0x00000000	32	*Fail control register* on page 3-12
0x02C+(0x10*<x>)[bc]	FAIL_ID_<x>	RO	0x00000000	_[d]	*Fail ID register* on page 3-13
0x060 to 0x0FC	-	-	-	-	Reserved
The region control registers control the address space that each region controls and the security attributes to use for that region.					
0x100	REGION_BASE_LOW_0	RO	0x00000000	32	*Region base address low register* on page 3-14
0x104	REGION_BASE_HIGH_0	RO	0x00000000	32	*Region base address high register* on page 3-15
0x108	REGION_TOP_LOW_0	RO	0xFFFFFFFF	32	*Region top address low register* on page 3-16
0x10C	REGION_TOP_HIGH_0	RO	_[e]	32	*Region top address high register* on page 3-16
0x110	REGION_ATTRIBUTES_0	RW	0x00000000	32	*Region attributes register* on page 3-17
0x114	REGION_ID_ACCESS_0	RW	0x00000000	32	*Region ID access register* on page 3-18
0x118+(0x20*n)[f] to 0x11C+(0x20*n)[f]	-	-	-	-	Reserved
0x100+(0x20*n)[f]	REGION_BASE_LOW_<n>	RW	0x00000000	32	*Region base address low register* on page 3-14

Table 3-1 Register summary (continued)

Offset	Name	Type	Reset	Width	Description
0x104+(0x20*n)[f]	REGION_BASE_HIGH_<n>	RW	0x00000000	32	*Region base address high register* on page 3-15
0x108+(0x20*n)[f]	REGION_TOP_LOW_<n>	RW	0x00000FFF	32	*Region top address low register* on page 3-16
0x10C+(0x20*n)[f]	REGION_TOP_HIGH_<n>	RW	0x00000000	32	*Region top address high register* on page 3-16
0x100+(0x20*n)[f]	REGION_ATTRIBUTES_<n>	RW	0x00000000	32	*Region attributes register* on page 3-17
0x114+(0x20*n)[f]	REGION_ID_ACCESS_<n>	RW	0x00000000	32	*Region ID access register* on page 3-18
0x218 to 0xEFC	-	-	-	-	Reserved
Component identification registers enable the identification of system components by software.					
0xFD0	PID4	RO	0x04	8	*Peripheral ID 4 register* on page 3-19
0xFD4	PID5	RO	0x00	8	*Peripheral ID 5 register* on page 3-20
0xFD8	PID6	RO	0x00	8	*Peripheral ID 6 register* on page 3-20
0xFDC	PID7	RO	0x00	8	*Peripheral ID 7 register* on page 3-20
0xFE0	PID0	RO	0x60	8	*Peripheral ID 0 register* on page 3-20
0xFE4	PID1	RO	0xB4	8	*Peripheral ID 1 register* on page 3-21
0xFE8	PID2	RO	0x2B	8	*Peripheral ID 2 register* on page 3-22
0xFEC	PID3	RO	0x00	8	*Peripheral ID 3 register* on page 3-23
0xFF0	CID0	RO	0x0D	8	*Component ID 0 register* on page 3-23
0xFF4	CID1	RO	0xF0	8	*Component ID 1 register* on page 3-24
0xFF8	CID2	RO	0x05	8	*Component ID 2 register* on page 3-24
0xFFC	CID3	RO	0xB1	8	*Component ID 3 register* on page 3-25

a. The reset value of this read-only register depends on the configuration of the TZC-400.
b. Where <*x*> is a valid filter unit number for your configuration.
c. The configuration of TZC-400 controls the number of filter units. Therefore, if a filter, for example Filter 3, is not implemented, all FAIL_<...>_3 registers are unused and are reserved.
d. This depends on the width configuration of the ACE-Lite ID in the TZC-400.
e. The least significant N bits of this register are always 1 and the most significant bits are 0, where N = AXI_ADDRESS_WIDTH - 32.
f. Where <*n*> is the region number in the range 1-8.

3.3 Register descriptions

This section describes the registers that the TZC-400 provides.

3.3.1 Build configuration register

The BUILD_CONFIG register characteristics are:

Purpose Provides information about the configuration of the TZC-400.

Usage constraints There are no usage constraints.

Configurations Available in all configurations of the TZC-400.

Attributes See Table 3-1 on page 3-3.

Figure 3-1 shows the bit assignments.

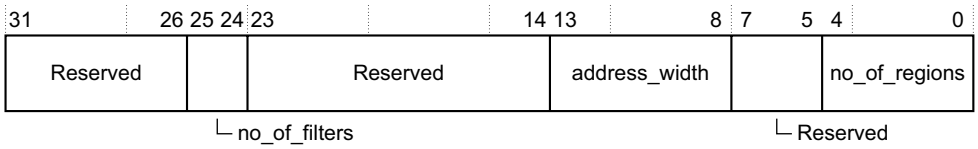


Figure 3-1 Build configuration register bit assignment

Table 3-2 shows the bit assignments.

Table 3-2 Build configuration register bit assignments

Bits	Name	Function
[31:26]	-	Reserved.
[25:24]	no_of_filters	Defines the number of filter units in the design implementation: `0b00` One filter unit. `0b01` Two filter units. `0b10` Reserved. `0b11` Four filter units.
[23:14]	-	Reserved.
[13:8]	address_width	Defines the width of the ACE-Lite address bus: `0b011111` 32 bits. `0b100011` 36 bits. `0b100111` 40 bits. `0b101111` 48 bits. `0b111111` 64 bits. **All other values** Reserved.
[7:5]	-	Reserved.
[4:0]	no_of_regions	Defines the number of regions that the TZC-400 provides: `0b01000` Nine regions. **All other values** Reserved.

3.3.2 Action register

The ACTION register characteristics are:

Purpose Controls the interrupt and bus response signaling behavior of the TZC-400 when region permission failures occur.

Usage constraints There are no usage constraints.

Configurations Available in all configurations of the TZC-400.

Attributes See Table 3-1 on page 3-3.

Figure 3-2 shows the bit assignments.

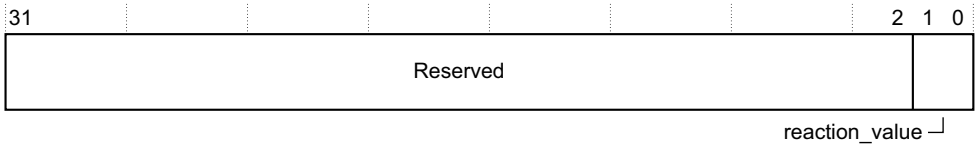


Figure 3-2 Action register bit assignments

Table 3-3 shows the bit assignments.

Table 3-3 Action register bit assignments

Bits	Name	Function
[31:2]	-	Reserved.
[1:0]	reaction_value	Controls how the TZC-400 uses the **BRESPS[1:0]**, **RRESPS[1:0]**, and **TZCINT** signals when a region permission failure occurs, excluding region overlap errors. The settings for these bits are: `0b00` Sets **TZCINT** LOW and issues an OKAY response. `0b01` Sets **TZCINT** LOW and issues a DECERR response. `0b10` Sets **TZCINT** HIGH and issues an OKAY response. `0b11` Sets **TZCINT** HIGH and issues a DECERR response. When a region overlap for region 1 and higher occurs, this field also determines how **TZCINT** is set. The settings are: `0b00`, `0b01` **TZCINT** LOW. `0b10`, `0b11` **TZCINT** HIGH.

3.3.3 Gate keeper register

The GATE_KEEPER register characteristics are:

Purpose Provides control and status for the gate keeper in each filter unit implemented.

Usage constraints Closing the gate can cause accesses on the command channels to stall and can inadvertently cause a bus deadlock. Use this with caution.

Configurations Available in all configurations of the TZC-400. The number of bits in each field varies with the number of filter units in the design implementation. For example, if there are two filter units, then each field is 2 bits, and all other bits are reserved and *Should Be Zero* (SBZ).

Attributes This is a RW register, but the bits in the most significant half, that is, the top 16 bits, of the register are RO. See Table 3-1 on page 3-3.

Figure 3-3 shows the bit assignments.

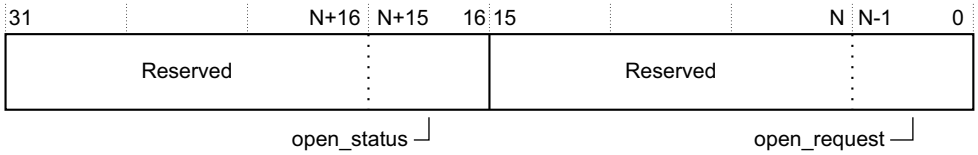


Figure 3-3 Gate keeper register bit assignments

Table 3-4 shows the bit assignments.

Table 3-4 Gate keeper register bit assignments

Bits	Name	Function
[31:N[a]+16]	-	Reserved.
[N[a]+15:16]	open_status	The current state of the gate keeper in each filter unit. The bit associations are as follows: **bit 16** Filter 0 gate keeper status. **bit 17** Filter 1 gate keeper status. **bit 18** Filter 2 gate keeper status. **bit 19** Filter 3 gate keeper status. When a bit is set to 1, the gate keeper permits access to its associated filter, that is, it is open. When a bit is set to 0, the gate keeper no longer permits access to its associated filter, that is, it is closed. This bit is set to 0 when both of the following conditions are fulfilled: • The gate keeper no longer permits access to its associated filter. • All outstanding accesses through the filter unit are complete. This means that the gate keeper always waits for outstanding accesses to complete. If any of the associated filter units are not implemented, the corresponding gate keeper bits are unused, reserved, and SBZ.
[15:N[a]]	-	Reserved.
[N[a]-1:0]	open_request	Each bit in this field requests the gate of the associated filter unit to be open or closed. Each bit is associated as follows: **bit 0** Filter 0. **bit 1** Filter 1. **bit 2** Filter 2. **bit 3** Filter 3. Set the open_request bit to 1, to request the gate to be open. Set the open_request bit to 0, to request the gate to be closed. If any of the associated filter units are not implemented, the corresponding open_request bits are unused, reserved, and SBZ.

a. N is the number of filter units in the TZC-400 design implementation and its value is in the range 1-4.

3.3.4 Speculation control register

The SPECULATION_CTRL register characteristics are:

Purpose Controls the read access speculation and write access speculation.

Usage constraints There are no usage constraints.

Configurations Available in all configurations of the TZC-400.

Attributes See Table 3-1 on page 3-3.

Figure 3-4 shows the bit assignments.

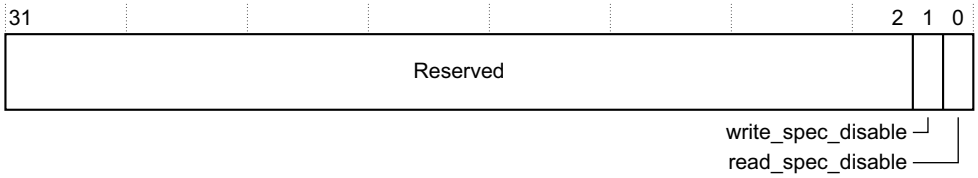


Figure 3-4 Speculation control register bit assignments

Table 3-5 shows the bit assignments.

Table 3-5 Speculation control register bit assignments

Bits	Name	Function
[31:2]	-	Reserved.
[1]	write_spec_disable	Controls write access speculation. **Note** This bit is ignored and assumed to be zero at a filter unit if the corresponding **QVNENABLE<x>** signal is HIGH. Set this bit as follows: `0` Enables write access speculation. This is the default. `1` Disables write access speculation.
[0]	read_spec_disable	Controls read access speculation. **Note** This bit is ignored and assumed to be zero at a filter unit if the corresponding **QVNENABLE<x>** signal is HIGH. You can set this bit as follows: `0` Enables read access speculation. This is the default. `1` Disables read access speculation.

3.3.5 Interrupt status register

The INT_STATUS register characteristics are:

Purpose Contains the status of the interrupt signal, **TZCINT**, that reports access security violations or region overlap errors.

Usage constraints There are no usage constraints.

Configurations Available in all configurations of the TZC-400.

Attributes See Table 3-1 on page 3-3.

Figure 3-5 shows the bit assignments.

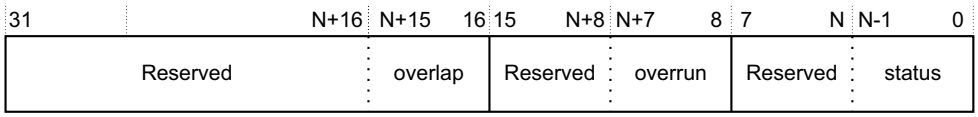


Figure 3-5 Interrupt status register bit assignments

Table 3-6 shows the bit assignments.

Table 3-6 Interrupt status register bit assignments

Bits	Name	Function
[31:N[a]+16]	-	Reserved
[N[a]+15:16]	overlap	The bit associations are as follows: **bit 16** Filter 0. **bit 17** Filter 1. **bit 18** Filter 2. **bit 19** Filter 3. When a bit is set to 1 it indicates a violation of the overlap region configuration rules for the associated filter unit. This occurs when an access matches with two enabled regions at the same time unless the overlap is only with Region 0, see *Access filtering with regions* on page 2-9. This bit is set even if the ACTION register is set to not drive the interrupt. See *Action register* on page 3-6. When this bit is 1, the interrupt status bit is also set to 1. Clear the interrupt status of the associated bit in the *Interrupt clear register* to also clear this field.
[15:N[a]+8]	-	Reserved.
[N[a]+7:8]	overrun	The bit associations are as follows: **bit 8** Filter 0. **bit 9** Filter 1. **bit 10** Filter 2. **bit 11** Filter 3. When a bit is set to 1, it indicates the occurrence of two or more region permission or region overlapping failures at the associated filter unit after the interrupt was cleared by the associated bit in the *Interrupt clear register*. This bit is set even if the ACTION register is set to not drive the interrupt. See *Action register* on page 3-6. Clear the interrupt status of the associated bit in the INT_CLEAR register to also clear this field.
[7:N[a]]	-	Reserved
[N[a]-1:0]	status	Each bit is associated as follows: **bit 0** Filter 0. **bit 1** Filter 1. **bit 2** Filter 2. **bit 3** Filter 3. Each bit in this field indicates the status of the interrupt from each filter unit as follows: `0` Interrupt is not asserted. `1` Interrupt is asserted and waiting to be cleared. This bit is set even if the ACTION register is set to not drive the interrupt output **TZCINT** HIGH. See *Action register* on page 3-6. Therefore, the status acts as an indicator that a region permission check failure or an overlap error has occurred at a particular filter unit.

a. N is the number of filter units, and its value is in the range 1-4.

3.3.6 Interrupt clear register

The INT_CLEAR register characteristics are:

Purpose Clears the interrupt.

Usage constraints There are no usage constraints.

Configurations Available in all configurations of the TZC-400.

Attributes This is a WO register. It is not possible to read this register. A read request returns all zeros. See Table 3-1 on page 3-3.

Figure 3-6 shows the bit assignments.

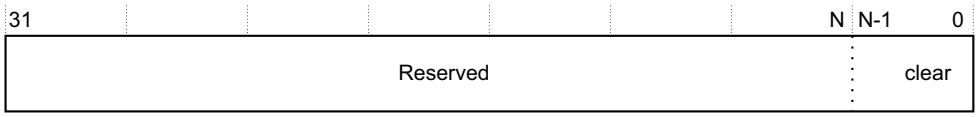


Figure 3-6 Interrupt clear register bit assignments

Table 3-7 shows the bit assignments.

Table 3-7 Interrupt clear register bit assignments

Bits	Name	Function
[31:N[a]]	-	Reserved.
[N[a]-1:0]	clear	Contains the control bits to clear interrupts. The bit associations are as follows: **bit 0** Filter 0. **bit 1** Filter 1. **bit 2** Filter 2. **bit 3** Filter 3. Write a 1 to any of these bits to clear the associated status, overrun, and overlap bits in the INT_STATUS register. See *Interrupt status register* on page 3-8.

a. N is the number of filter units, and its value is in the range 1-4.

3.3.7 Fail address low register

Each filter unit has a FAIL_ADDRESS_LOW_<*x*> register where <*x*> is the filter unit number. The fail address low register characteristics are:

Purpose Contains the lower 32 bits of the address of the first access that failed a region permission check in the associated filter unit. This occurs even if the ACTION register is set to not drive the interrupt signal. See *Action register* on page 3-6. The first failing access is defined as the first permission failure in the associated filter unit after one of the following occurs:

- Reset.
- The last clearance of an interrupt using the INT_CLEAR register. See *Interrupt clear register* on page 3-9.

Usage constraints There are no usage constraints.

Configurations Available in all configurations of the TZC-400.

Attributes See Table 3-1 on page 3-3.

Figure 3-7 on page 3-11 shows the bit assignments.

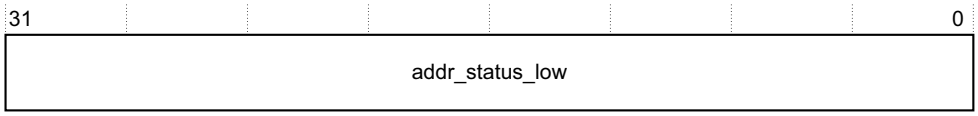


Figure 3-7 Fail address low register bit assignments.

Table 3-8 shows the bit assignments.

Table 3-8 Fail address low register bit assignments

Bits	Name	Function
[31:0]	addr_status_low	If a region permission check fails or a region overlap occurs, this field returns the ACE-Lite address bits [31:0] of the first failed access. You must clear the associated interrupt status before this field can return the address of accesses of subsequent permission checks or region overlap failures. This occurs even if the ACTION register does not enable the interrupt. See *Action register* on page 3-6. If the status flag for the filter unit in the INT_STATUS register is already set, new region permission check failures in the same filter unit do not update the associated fail status group of registers.

3.3.8 Fail address high register

Each filter unit has a FAIL_ADDRESS_HIGH_<*x*> register where <*x*> is the filter unit number. The fail address high register characteristics are:

Purpose Contains the most significant 32 bits of the address of the first access that failed a region permission check in the associated filter unit. This occurs even if the ACTION register is set to not drive the interrupt signal. See *Action register* on page 3-6. The first failing access is defined as the first permission failure in the associated filter unit after one of the following occurs:

- Reset.
- The last clearance of an interrupt using the INT_CLEAR register. See *Interrupt clear register* on page 3-9.

Usage constraints There are no usage constraints.

Configurations Available in all configurations of the TZC-400.

Attributes See Table 3-1 on page 3-3.

Figure 3-8 shows the bit assignments.

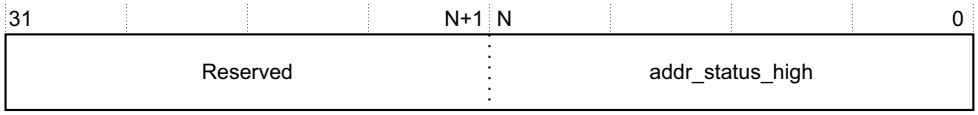


Figure 3-8 Fail address high register bit assignments

Table 3-9 shows the bit assignments.

Table 3-9 Fail address high register bit assignments

Bits	Name	Function
[31:N[a]+1]	-	Reserved.
[N[a]:0]	addr_status_high	If a region permission check fails or a region overlap occurs, this field returns the ACE-Lite address bits [N+32:32] of the first failed access. You must clear the associated interrupt status before this field can return the addresses of the accesses of subsequent permission checks or region overlap failures. This occurs even if the ACTION register does not enable the interrupt. See *Action register* on page 3-6. If the status flag for the filter unit in the INT_STATUS register is already set, new region permission check failures in the same filter unit do not update the associated fail status group of registers.

a. N = AXI_ADDRESS_MSB – 33.

3.3.9 Fail control register

Each filter unit has a FAIL_CONTROL_<*x*> register where <*x*> is the filter unit number. The fail control register characteristics are:

Purpose Contains the control status information of the first access that failed a region permission check in the associated filter unit. This occurs even if the ACTION register is set to not drive the interrupt signal. See *Action register* on page 3-6. The first failing access is defined as the first permission failure in the associated filter unit after one of the following occurs:

- Reset.
- The last clearance of an interrupt using the INT_CLEAR register. See *Interrupt clear register* on page 3-9.

Usage constraints There are no usage constraints.

Configurations Available in all configurations of the TZC-400.

Attributes See Table 3-1 on page 3-3.

Figure 3-9 shows the bit assignments.

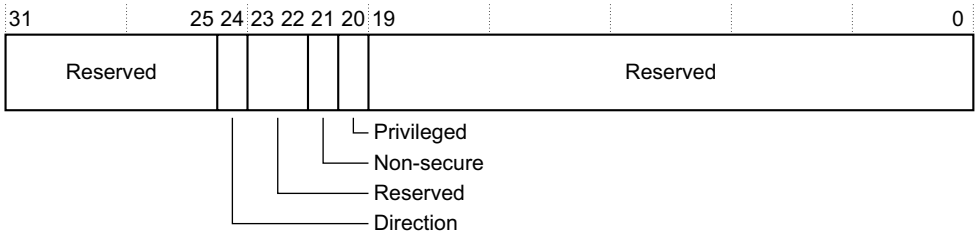


Figure 3-9 Fail control register bit assignments

Table 3-10 shows the bit assignments.

Table 3-10 Fail control register bit assignments

Bits	Name	Function
[31:25]	-	Reserved, SBZ.
[24]	Direction	If a region permission check fails or a region overlap occurs, this field indicates whether the failed access was a read or write access attempt. You must clear the associated interrupt status before this field can return the direction of accesses of subsequent permission checks or region overlap failures. 0 Read access. 1 Write access. If the status flag for the filter unit in the INT_STATUS register is already set, new region permission check failures in the same filter unit do not update the associated fail status group of registers.
[23:22]	-	Reserved, SBZ.
[21]	Non-secure	If a region permission check fails or a region overlap occurs, this field indicates whether it was a Secure or Non-secure access attempt. You must clear the associated interrupt status before this field can return the direction of accesses of subsequent permission checks or region overlap failures. 0 Secure access. 1 Non-secure access. If the status flag for the filter unit in the INT_STATUS register is already set, new region permission check failures in the same filter unit do not update the associated fail status group of registers.
[20]	Privileged	If a region permission check fails or a region overlap occurs, this field indicates whether it was an unprivileged or privileged access attempt. You must clear the associated interrupt status before this field can return the values of accesses of subsequent permission checks or region overlap failures. 0 Unprivileged access. 1 Privileged access. If the status flag for the filter unit in the INT_STATUS register is already set, new region permission check failures in the same filter unit do not update the associated fail status group of registers.
[19:0]	-	Reserved, SBZ.

3.3.10 Fail ID register

Each filter unit has a FAIL_ID_<x> register. The fail ID register characteristics are:

Purpose Contains the master ACE-Lite ARID or AWID of the first access that failed a region permission check in the associated filter unit. This occurs even if the ACTION register is set to not drive the interrupt signal. See *Action register* on page 3-6. The first failing access is defined as the first permission failure in the associated filter unit after one of the following occurs:

- Reset.
- The last clearance of an interrupt using the INT_CLEAR register. See *Interrupt clear register* on page 3-9.

Usage constraints There are no usage constraints.

Configurations Available in all configurations of the TZC-400.

Attributes See Table 3-1 on page 3-3.

Figure 3-10 shows the bit assignments.

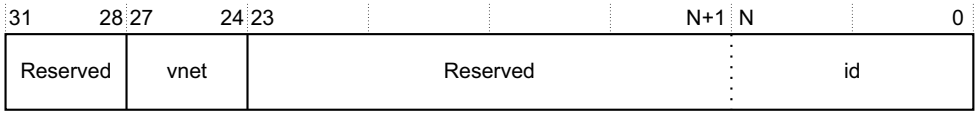


Figure 3-10 Fail ID register bit assignments

Table 3-11 shows the bit assignments.

Table 3-11 Fail ID register bit assignments

Bits	Name	Function
[31:28]	-	Reserved.
[27:24]	vnet	If a region permission check fails or a region overlap occurs, this field returns the VN number of the first failed access, from either **ARVNET<x>** or **AWVNET<x>** as appropriate. If the status flag for the filter unit in the INT_STATUS register is already set, new region permission check failures in the same filter unit do not update the associated fail status group of registers.
[23:N[a]+1]	-	Reserved.
[N[a]:0]	id	If a region permission check fails or a region overlap occurs, this field returns the ACE-Lite ID values of the first failed access. If the status flag for the filter unit in the INT_STATUS register is already set, new region permission check failures in the same filter unit do not update the associated fail status group of registers.

a. N = AID_WIDTH – 1.

3.3.11 Region base address low register

Each region has a REGION_BASE_LOW_<n> register where <*n*> is the region number. The region base address low register characteristics are:

Purpose Controls the base address bits[31:12] of Region <n>. Base address bits[11:0] are always zero because the TZC-400 does not permit the region size to be less than 4KB.

Note

For Region 0, this register is read-only and is hard-wired to all zeros.

Usage constraints There are no usage constraints.

Configurations Available in all configurations of the TZC-400.

Attributes See Table 3-1 on page 3-3.

Figure 3-11 shows the bit assignments.

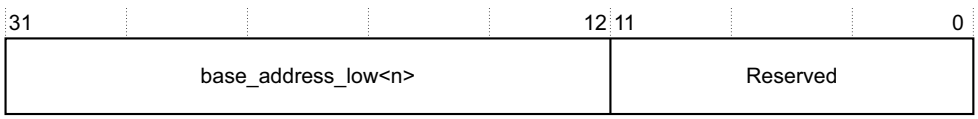


Figure 3-11 Region base address low register bit assignments

Table 3-12 shows the bit assignments.

Table 3-12 Region base address low register bit assignments

Bits	Name	Function
[31:12]	base_address_low<*n*>	Controls the base address bits[31:12] of Region <*n*>[a]. The TZC-400 only permits a region to start at a 4KB aligned address and address bits[11:0] are zeros.
[11:0]	-	Reserved.

a. For Region 0, this field is read-only. The TZC-400 sets the base address of Region 0 to `0x0`.

3.3.12 Region base address high register

Each region has a REGION_BASE_HIGH_<n> register, where <*n*> is the region number. The region base address high register characteristics are:

Purpose Controls the base address bits 32 and higher of region <n>.

Note

For Region 0, this register is read-only and is hard-wired to all zeros.

Usage constraints There are no usage constraints.

Configurations Available in all configurations of the TZC-400.

Attributes See Table 3-1 on page 3-3.

Figure 3-12 shows the bit assignments.

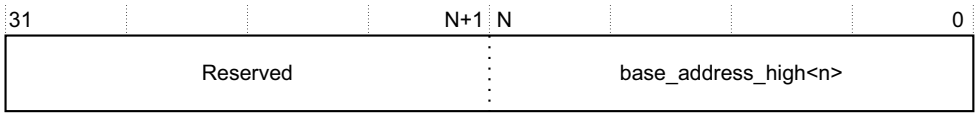


Figure 3-12 Region base address high register bit assignments

Table 3-13 shows the bit assignments.

Table 3-13 Region base address high register bit assignments

Bits	Name	Function
[31:N[a]+1]	-	Reserved, SBZ.
[N[a]:0]	base_address_high<*n*>	Controls the base address bits 32 and higher of Region <*n*>[b].

a. N = AXI_ADDRESS_MSB-33.

b. For Region 0, this field is read-only. The TZC-400 sets the base address of Region 0 to `0x0`.

3.3.13 Region top address low register

Each region has a REGION_TOP_LOW_<n> register, where <*n*> is the region number. The region top address low register characteristics are:

Purpose Controls the region top address bits[31:12] of Region <n>. Region top address bits[11:0] are always `0xFFF` because the TZC-400 does not permit the region size to be less than 4KB, and therefore the region top address points to the top byte of a 4KB region.

Note

For Region 0, this register is read-only. The least significant N bits of this register are always 1 and the most significant bits are 0, where N = AXI_ADDRESS_WIDTH - 32.

Usage constraints There are no usage constraints.

Configurations Available in all configurations of the TZC-400.

Attributes See Table 3-1 on page 3-3.

Figure 3-13 shows the bit assignments.

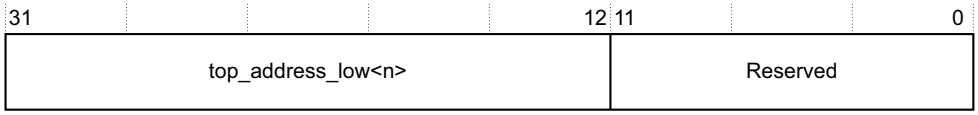


Figure 3-13 Region top address low register bit assignments

Table 3-14 shows the bit assignments.

Table 3-14 Region top address low register bit assignments

Bits	Name	Function
[31:12]	top_address_low<*n*>	Controls the region top address bits[31:12] of region <*n*>[a]. This address points to the start of the next 4KB aligned address immediately outside the region.
[11:0]	Reserved	`0xFFF`. Read only and points to the highest byte of a 4KB-aligned area.

a. For Region 0, this field is read-only and all bits are set HIGH.

3.3.14 Region top address high register

Each region has a REGION_TOP_HIGH_<n> register, where <*n*> is the region number. The region top address high register characteristics are:

Purpose Controls the region top address bits 32 and higher of Region <n>.

Note

For Region 0, this register is read-only and bits N down to 0 are hard-wired to `0xFFFFFFFF`.

Usage constraints There are no usage constraints.

Configurations Available in all configurations of the TZC-400.

Attributes See Table 3-1 on page 3-3.

Figure 3-14 shows the REGION_<n>_TOP_HIGH register bit assignments.

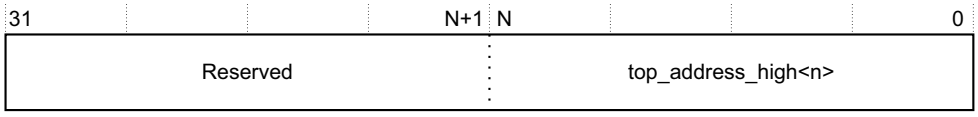


Figure 3-14 Region top address high register bit assignments

Table 3-15 shows the bit assignments.

Table 3-15 Region top address high register bit assignments

Bits	Name	Function
[31:N[a]+1]	-	Reserved, SBZ.
[N[a]:0]	top_address_high<*n*>	Controls the region top address bits 32 and higher of region <*n*>[b]. This address points to the highest address of the region. For region 0, this field is read-only and always returns `0xFFFFFFFF`.

a. N = AXI_ADDRESS_MSB – 33.

b. For Region 0, this field is read-only and all bits are hard-wired to `0xFFFFFFFF`.

3.3.15 Region attributes register

Each region has a REGION_ATTRIBUTES_<n> register, where <*n*> is the region number. The region attributes register characteristics are

Purpose Controls the permissions for Region 0. For all other regions, it controls the permissions and target filter region enables.

Usage constraints There are no usage constraints.

Configurations Available in all configurations of the TZC-400.

Attributes See Table 3-1 on page 3-3.

Figure 3-15 shows the bit assignments.

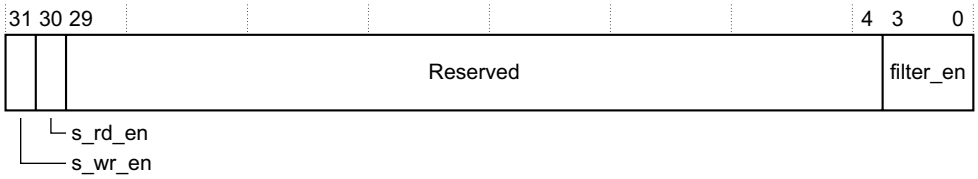


Figure 3-15 Region attributes register bit assignments

Table 3-16 shows the bit assignments.

Table 3-16 Region attributes register bit assignments

Bits	Name	Function
[31]	s_wr_en	Secure global write enable. This control bit defines the permissions for the Secure writes in the region. Set this bit as follows: 0 Secure write to the region is not permitted. 1 Permits Secure write to the region.
[30]	s_rd_en	Secure global read enable. This control bit defines the permissions for the Secure reads in the region. Set this bit as follows: 0 Secure read to the region is not permitted. 1 Permits Secure read to the region.
[29:4]	-	Reserved, SBZ.
[3:0]	filter_en	Independent region enable for each filter unit. Each bit is associated with a filter unit. Set these bits as follows: **Bit 0** For Filter 0. **Bit 1** For Filter 1. **Bit 2** For Filter 2. **Bit 3** For Filter 3. When set HIGH, it enables the use of the current region programming for the associated filter. For Region 0 all bits are set HIGH and cannot be modified.

3.3.16 Region ID access register

Each region has a REGION_ID_ACCESS_<n> register, where <*n*> is the region number. The Region ID Access register characteristics are

Purpose Controls the Non-secure access based on the NSAID inputs.

Usage constraints There are no usage constraints.

Configurations Available in all configurations of the TZC-400.

Attributes See Table 3-1 on page 3-3.

Figure 3-16 shows the bit assignments.

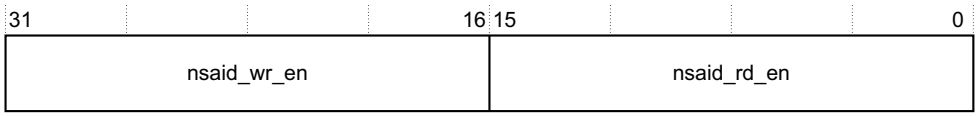


Figure 3-16 Region ID access register bit assignments

Table 3-17 shows the bit assignments.

Table 3-17 Region ID access register bit assignments

Bits	Name	Function
[31:16]	nsaid_wr_en	NSAID write enables. This enables NSAID inputs to define Non-secure write access permission. Each bit of the nsaid_wr_en register field is associated with a value on the **NSAIDW<x>** signal as follows: **Bit 16** Associated with **NSAIDW<x>** = 0. **Bit 17** Associated with **NSAIDW<x>** = 1. **Bit 18** Associated with **NSAIDW<x>** = 2. ... **Bit 31** Associated with **NSAIDW<x>** = 15. <*x*> is the filter unit number. When any bit in this field is set to 1, TZC-400 permits Non-secure write access to any access with the associated **NSAIDW<x>** value. For example, if **NSAIDW<x>** is 3 and the corresponding nsaid_wr_en[3] bit is set HIGH then TZC-400 permits the Non-secure write access to progress.
[15:0]	nsaid_rd_en	NSAID read enables. This enables NSAID inputs to define Non-secure read access permission. Each bit of the nsaid_rd_en register field is associated with a value on the **NSAIDR<x>** signal as follows: **Bit 0** Associated with **NSAIDR<x>** = 0. **Bit 1** Associated with **NSAIDR<x>** = 1. **Bit 2** Associated with **NSAIDR<x>** = 2. ... **Bit 15** Associated with **NSAIDR<x>** = 15. <x> is the filter unit number. When any bit in this field is set HIGH, TZC-400 permits Non-secure read access to any access with the associated **NSAIDR<x>** value. For example, if **NSAIDR<x>** is 3 and the corresponding nsaid_rd_en[3] bit is set HIGH then TZC-400 permits the Non-secure read access to progress.

3.3.17 Peripheral ID 4 register

The PID4 register characteristics are:

Purpose Provides the following information about the peripheral configuration
- 4KB_count.
- Jep106_c_code.

Usage constraints There are no usage constraints.

Configurations Available in all configurations of the TZC-400.

Attributes See Table 3-1 on page 3-3.

Figure 3-17 shows the bit assignments.

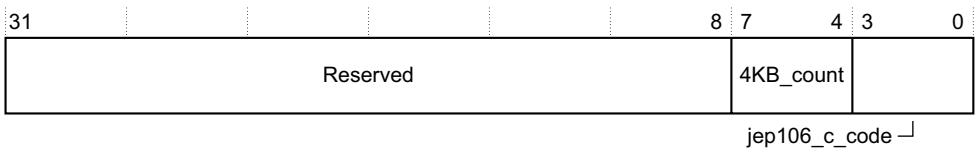


Figure 3-17 Peripheral ID 4 register bit assignments

Table 3-18 shows the bit assignments.

Table 3-18 Peripheral ID 4 register bit assignments

Bits	Name	Function
[31:8]	-	Reserved, SBZ.
[7:4]	4KB_count	The number of 4KB address blocks required to access the registers, expressed in powers of 2. These bits read back as `0x0`. This means that the TZC-400 occupies a single 4KB address block.
[3:0]	jep106_c_code	The JEP106 continuation code value represents how many `0x7F` continuation characters occur in the manufacturer identity code. These bits read back as `0x4`. For information on the JEP106 standard, see *Other Publications* on page viii.

3.3.18 Peripheral ID 5 register

The PID5 register characteristics are:

Purpose Provides information about the peripheral configuration. The TZC-400 does not require this register.

Usage constraints There are no usage constraints.

Configurations Available in all configurations of the TZC-400.

Attributes See Table 3-1 on page 3-3.

3.3.19 Peripheral ID 6 register

The PID6 register characteristics are:

Purpose Provides information about the peripheral configuration. The TZC-400 does not require this register.

Usage constraints There are no usage constraints.

Configurations Available in all configurations of the TZC-400.

Attributes See Table 3-1 on page 3-3.

3.3.20 Peripheral ID 7 register

The PID7 register characteristics are:

Purpose Provides information about the peripheral configuration. The TZC-400 does not require this register.

Usage constraints There are no usage constraints.

Configurations Available in all configurations of the TZC-400.

Attributes See Table 3-1 on page 3-3.

3.3.21 Peripheral ID 0 register

The PID0 register characteristics are:

Purpose The PID0 register provides the following information about the peripheral configuration:

- part_number_0.

Usage constraints There are no usage constraints.

Configurations Available in all configurations of the TZC-400.

Attributes See Table 3-1 on page 3-3.

Figure 3-18 shows the bit assignments.

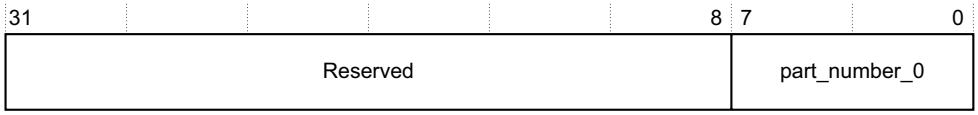


Figure 3-18 Peripheral ID 0 register bit assignments

Table 3-19 shows the PID0 register bit assignments.

Table 3-19 Peripheral ID 0 register bit assignments

Bits	Name	Function
[31:8]	-	Reserved, SBZ
[7:0]	part_number_0	These bits read back as `0x60`

3.3.22 Peripheral ID 1 register

The PID1 register characteristics are:

Purpose The PID1 register provides the following information about the peripheral configuration:

- part_number_1.
- Jep106_id_3_0.

Usage constraints There are no usage constraints.

Configurations Available in all configurations of the TZC-400.

Attributes See Table 3-1 on page 3-3.

Figure 3-19 shows the bit assignments.

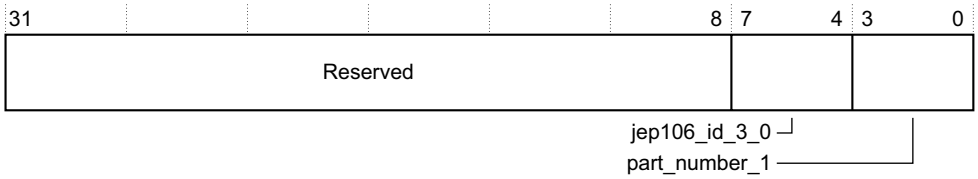


Figure 3-19 Peripheral ID 1 register bit assignments

Table 3-20 shows the bit assignments.

Table 3-20 Peripheral ID 1 register bit assignments

Bits	Name	Function
[31:8]	-	Reserved, SBZ.
[7:4]	jep106_id_3_0	JEP106 identity code [3:0]. See the JEP106, Standard Manufacturer Identification Code. These bits read back as `0xB` because ARM is the peripheral designer.
[3:0]	part_number_1	These bits read back as `0x4`.

3.3.23 Peripheral ID 2 register

The PID2 register characteristics are:

Purpose The PID2 register provides the following information about the peripheral configuration:
- Jep106_id_6_4.
- Revision number.
- JEDEC use flag.

Usage constraints There are no usage constraints.

Configurations Available in all configurations of the TZC-400.

Attributes See Table 3-1 on page 3-3.

Figure 3-20 shows the bit assignments.

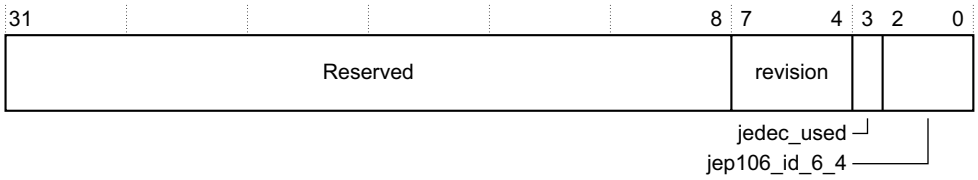


Figure 3-20 Peripheral ID 2 register bit assignments

Table 3-21 shows the bit assignments.

Table 3-21 Peripheral ID 2 register bit assignments

Bits	Name	Function
[31:8]	-	Reserved, SBZ.
[7:4]	revision	Identifies the revision of the TZC-400. For revision r0p1, this field is set to `0x2`.
[3]	jedec_used	This indicates that the TZC-400 uses a manufacturer identity code that was allocated by JEDEC according to JEP106. This bit always reads back as `0x1`.
[2:0]	jep106_id_6_4	JEP106 identity code [6:4]. See the JEP106, Standard Manufacturer Identification Code. These bits read back as `0b011` because ARM is the peripheral designer.

3.3.24 Peripheral ID 3 register

The PID3 register characteristics are:

Purpose The PID3 register provides the following information about the peripheral configuration:
- Mod Number.
- RevAnd.

Usage constraints There are no usage constraints.

Configurations Available in all configurations of the TZC-400.

Attributes See Table 3-1 on page 3-3.

Figure 3-21 shows the bit assignments.

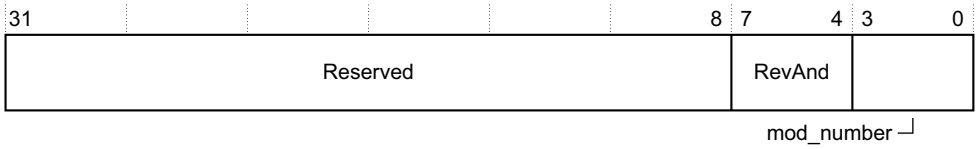


Figure 3-21 Peripheral ID 3 register bit assignments

Table 3-22 shows the bit assignments.

Table 3-22 Peripheral ID 3 register bit assignments

Bits	Name	Function
[31:8]	-	Reserved, SBZ.
[7:4]	RevAnd	The top-level RTL provides a 4-bit input, USERPID3REVAND, that is normally tied LOW and provides a read value of `0x0`. When silicon is available, and if metal fixes are required, the manufacturer can modify the tie-offs to indicate a revision of the silicon.
[3:0]	mod_number	This is set to `0x0`.

3.3.25 Component ID 0 register

The CID0 register characteristics are:

Purpose This is one of four 8-bit registers that together hold a 32 bit component ID value. Use this for automatic BIOS configuration. The full 32-bit component_id is set to `0xB105F00D`.

Usage constraints There are no usage constraints.

Configurations Available in all configurations of the TZC-400.

Attributes See Table 3-1 on page 3-3.

Figure 3-22 shows the bit assignments.

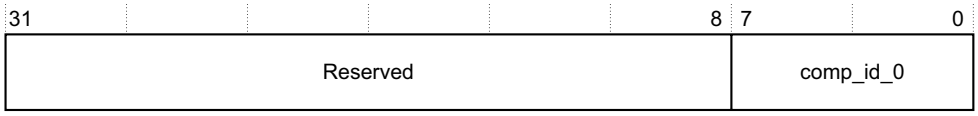


Figure 3-22 Component ID 0 register bit assignments

Table 3-23 shows the bit assignments.

Table 3-23 Component ID 0 register bit assignments

Bits	Name	Function
[31:8]	-	Reserved, SBZ
[7:0]	comp_id_0	These bits read back as `0x0D`

3.3.26 Component ID 1 register

The CID1 register characteristics are:

Purpose This is one of four 8-bit registers that together hold a 32 bit component ID value. Use this for automatic BIOS configuration. The full 32-bit component ID is set to `0xB105F00D`.

Usage constraints There are no usage constraints.

Configurations Available in all configurations of the TZC-400.

Attributes See Table 3-1 on page 3-3.

Figure 3-23 shows the bit assignments.

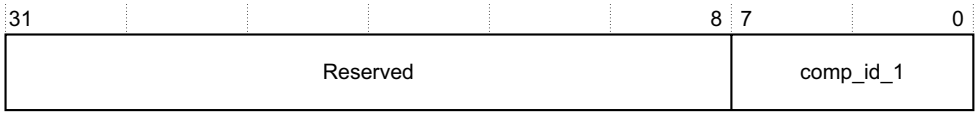


Figure 3-23 Component ID 1 register bit assignments.

Table 3-24 shows the bit assignments.

Table 3-24 Component ID 1 register bit assignments

Bits	Name	Function
[31:8]	-	Reserved, SBZ
[7:0]	comp_id_1	These bits read back as `0xF0`

3.3.27 Component ID 2 register

The CID2 register characteristics are:

Purpose This is one of four 8-bit registers, that together hold a 32-bit component ID value. Use this for automatic BIOS configuration. The full 32-bit component_id is set to `0xB105F00D`.

Usage constraints There are no usage constraints.

Configurations Available in all TZC-400 configurations.

Attributes See Table 3-1 on page 3-3.

Figure 3-24 on page 3-25 shows the bit assignments.

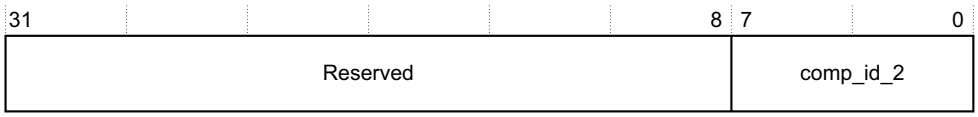


Figure 3-24 Component ID 2 register bit assignments

Table 3-25 shows the bit assignments.

Table 3-25 Component ID 2 register bit assignments

Bits	Name	Function
[31:8]	-	Reserved, SBZ
[7:0]	comp_id_2	These bits read back as `0x05`

3.3.28 Component ID 3 register

The CID3 register characteristics are:

Purpose This is one of four 8-bit registers that together hold a 32-bit component ID value. The full 32-bit component_id is set to `0xB105F00D`.

Usage constraints There are no usage constraints.

Configurations Available in all TZC-400 configurations.

Attributes See Table 3-1 on page 3-3.

Figure 3-25 shows the bit assignments.

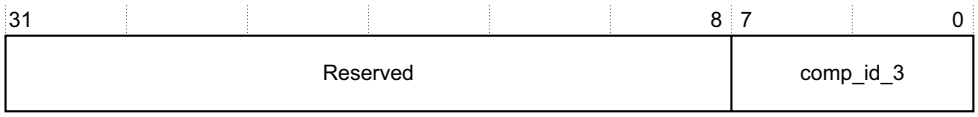


Figure 3-25 Component ID 3 register bit assignments

Table 3-26 shows the bit assignments.

Table 3-26 Component ID 3 register bit assignments

Bits	Name	Function
[31:8]	-	Reserved, SBZ
[7:0]	comp_id_3	These bits read back as `0xB1`

Appendix A
Signal Descriptions

This appendix describes the signals that the TZC-400 provides. It contains the following sections:

A.1 Signal direction

The signals described in the remaining sections can be implemented as inputs or outputs. Signals can have multiple instances and contain replaceable terms that have the following meaning unless stated otherwise:

- <*p*> is either S for slave interface signals or M for master interface signals.
- <*x*> is the filter unit number.

Figure A-1 shows an example of the **AWID<p><x>** signal described in Table A-3 on page A-5 and how this corresponds both with the **AWIDS<x>** and the **AWIDM<x>** signals shown in the diagram.

Table A-3 on page A-5 shows that the entry in the source column **AWIDS<x>** is Master. This means the source of the signal comes from the ACE-Lite master in this example. The name of the signal is **AWIDS<x>** because it is received into the TZC-400 through a slave interface and so it is an input. When the signal leaves the TZC-400, it exits through a master interface. This signal is called **AWIDM<x>** and is an output.

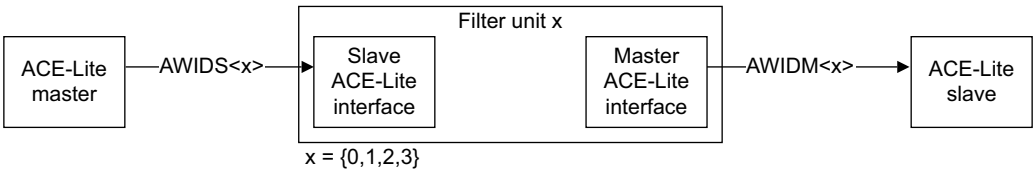


Figure A-1 Master interface and slave interface signal direction

A.2 Clock and reset signals

Table A-1 shows the clock and reset signals for the TZC-400. In this table, <*x*> is the filter unit number and each signal has one instance per filter unit.

Table A-1 Clocks and resets

Signal	Source	Description
ACLK<x>	Clock source	Clock signal for domain <*x*>
ARESET<x>n	Reset source	Reset signal for domain <*x*>
PCLK	Clock source	Clock signal for the control unit
PRESETn	Reset source	Reset signal for the control unit

A.3 AXI low-power interface signals

- Table A-2 lists the AXI low-power interface signals. This interface must operate according to the rules of the AXI low-power interface. See *ARM® AMBA® AXI and ACE Protocol Specification*.

Note

TZC-400 does not issue a denial response to a low-power request. For more information, see *AXI low-power interface signals* on page 2-3.

In this table, <*x*> is the filter unit number or `APB` for the control unit.

Table A-2 Low-power interface signals

Signal	Source	Description
CSYSREQ<x>	Clock or power controller	Low Power Request. Set LOW to request the associated domain to enter idle state. Set HIGH to request to exit idle state.
CSYSACK<x>	TZC-400	Low Power Request Acknowledgment. When LOW, this signal indicates that the domain is now idle, and is ready for you to remove the clock or power. When transitioning HIGH, this signal acknowledges the presence of clock or power and that the TZC-400 is ready to operate.
CACTIVE<x>	TZC-400	Clock active. When HIGH, this signal indicates that clock is required for the clock domain. When LOW, it indicates that the domain is idle. This signal must not be used to directly gate clocks. See *Clock gating* on page 2-18.

A.4 ACE-Lite signals

- Table A-3 lists the ACE-Lite signals. In this table <*p*> is either S for slave interface signals or M for master interface signals, and <*x*> is the filter unit number. For more information on each signal, see the *ARM® AMBA® AXI and ACE Protocol Specification*.

Table A-3 ACE-Lite signals

Signal	Source	Description
AWID<p><x>[ID_WIDTH-1:0]	Master	Write address ID. You can configure the width of this signal.
AWADDR<p><x>[ADDR_WIDTH-1:0]	Master	Write address. You can configure the width of this signal.
AWLEN<p><x>[7:0]	Master	Write burst length.
AWSIZE<p><x>[2:0]	Master	Write burst size.
AWBURST<p><x>[1:0]	Master	Write burst type.
AWLOCK<p><x>	Master	Write lock type.
AWCACHE<p><x>[3:0]	Master	Write cache type.
AWPROT<p><x>[2:0]	Master	Write protection type.
AWQOS<p><x>[3:0]	Master	Write QoS value.
AWREGION<p><x>[3:0]	Master	Write address region.
AWDOMAIN<p><x>[1:0]	Master	Write domain.
AWSNOOP<p><x>[2:0]	Master	Write snoop request type.
AWBAR<p><x>[1:0]	Master	Write barrier type.
AWUSER<p><x>[USER_WIDTH-1:0]	Master	User-specified extension to AW payload. You can configure the width of this signal.
AWVALID<p><x>	Master	Write address valid.
AWREADY<p><x>	Slave	Write address ready.
WDATA<p><x>[DATA_WIDTH-1:0]	Master	Write data. You can configure the width of this signal.
WID<p><x>[ID_WIDTH-1:0]	Master	Write data ID. You can configure the width of this signal.
WSTRB<p><x>[STRB_WIDTH[a]-1:0]	Master	Write byte-lane strobes.
WLAST<p><x>	Master	Write data last transfer indication.
WUSER<p><x>[USER_WIDTH-1:0]	Master	User-specified extension to W payload. You can configure the width of this signal.
WVALID<p><x>	Master	Write data valid.
WREADY<p><x>	Slave	Write data ready.
BID<p><x>[ID_WIDTH-1:0]	Slave	Write response ID. You can configure the width of this signal.
BRESP<p><x>[1:0]	Slave	Write response.
BUSER<p><x>[USER_WIDTH-1:0]	Slave	User-specified extension to B payload. You can configure the width of this signal.
BVALID<p><x>	Slave	Write response valid.

Table A-3 ACE-Lite signals (continued)

Signal	Source	Description
BREADY<p><x>	Master	Write response ready.
ARID<p><x>[ID_WIDTH-1:0]	Master	Read address ID. You can configure the width of this signal.
ARADDR<p><x>[ADDR_WIDTH-1:0]	Master	Read address. You can configure the width of this signal.
ARLEN<p><x>[7:0]	Master	Read burst length.
ARSIZE<p><x>[2:0]	Master	Read burst size.
ARBURST<p><x>[1:0]	Master	Read burst type.
ARLOCK<p><x>	Master	Read lock type.
ARCACHE<p><x>[3:0]	Master	Read cache type.
ARPROT<p><x>[2:0]	Master	Read protection type.
ARQOS<p><x>[3:0]	Master	Read QoS.
ARREGION<p><x>[3:0]	Master	Read address region.
ARDOMAIN<p><x>[1:0]	Master	Read domain.
ARSNOOP<p><x>[3:0]	Master	Read snoop request type.
ARBAR<p><x>[1:0]	Master	Read barriers.
ARUSER<p><x>[USER_WIDTH-1:0]	Master	User-specified extension to AR payload. You can configure the width of this signal.
ARVALID<p><x>	Master	Read address valid.
ARREADY<p><x>	Slave	Read address ready.
RID<p><x>[ID_WIDTH-1:0]	Slave	Read data ID. You can configure the width of this signal.
RDATA<p><x>[DATA_WIDTH-1:0]	Slave	Read data. You can configure the width of this signal.
RRESP<p><x>[1:0]	Slave	Read data response.
RUSER<p><x>[USER_WIDTH-1:0]	Slave	User-specified extension to R payload. You can configure the width of this signal.
RLAST<p><x>	Slave	Read data last transfer indication.
RVALID<p><x>	Slave	Read data valid.
RREADY<p><x>	Master	Read data ready.

a. The TZC-400 automatically defines this width using the formula `STRB_WIDTH = DATA_WIDTH / 8`.

A.5 QoS Virtual Network signals

Table A-4 lists the QVN signals. In this table, <*n*> is the relevant virtual network number, <*p*> is either S for slave interface signals or M for master interface signals, and <*x*> is the filter unit number.

Table A-4 VN signals

Signal	Source	Description
VAWVALIDVN<n><p><x>	Master	Token request valid. This signal indicates that the master requests a token.
VAWREADYVN<n><p><x>	Slave	Token request accepted. This signal indicates that the slave is ready to accept an address and associated control signals.
VAWQOSVN<n><p><x>[3:0]	Master	Quality of Service value.
VWVALIDVN<n><p><x>	Master	Token request valid. This signal indicates that the master requests a token.
VWREADYVN<n><p><x>	Slave	Token request accepted. This signal indicates that the slave is ready to accept a write data transfer and associated control signals.
VARVALIDVN<n><p><x>	Master	Token request valid. This signal indicates that the master requests a token.
VARREADYVN<n><p><x>	Slave	Token request accepted. This signal indicates that the slave is ready to accept an address and associated control signals.
VARQOSVN<n><p><x>[3:0]	Master	Quality of Service value.

A.5.1 AXI VN signals

Table A-5 shows the AXI virtual network QVN signals.

Table A-5 AXI VN signals

Signal	Source	Description
AWVNET<p><x>[3:0]	Master	AW channel virtual network ID
WVNET<p><x>[3:0]	Master	W channel virtual network ID
ARVNET<p><x>[3:0]	Master	AR channel virtual network ID

A.6 APB signals

Table A-6 shows the APB4 interface signals for the TZC-400 control unit.

Table A-6 Control unit APB signals

Signal	Source	Description
PADDR[31:0]	Master	Address
PWDATA[31:0]	Master	Write data
PSTRB[3:0]	Master	Write strobes
PPROT[2:0]	Master	Protection type
PWRITE	Master	Direction
PENABLE	Master	Enable
PSEL	Master	Select
PRDATA[31:0]	Slave	Read data
PSLVERR	Slave	Transfer failure
PREADY	Slave	Ready

A.7 Identity signals

Table A-7 shows the identity input signals on all filter unit interfaces. In this table, <*x*> is the filter unit number.

Table A-7 Identity input signals

Signal	Source	Description
FPID<x>	Master	Fast path identity
NSAIDR<x>[3:0]	Master	Identifies the source of Non-secure read accesses
NSAIDW<x>[3:0]	Master	Identifies the source of Non-secure write accesses

A.8 Interrupt signal

Table A-8 shows the interrupt output signal for TZC-400.

Table A-8 Interrupt signal

Signal	Source	Description
TZCINT	TZC-400	Signals an interrupt condition to an interrupt controller based on your programmed settings

A.9 Configuration signals

Table A-8 on page A-10 shows the static configuration signals for TZC-400.

Table A-9 Static configuration signals

Signal	Source	Description
USERPID3REVAND	Implementer configuration signal	Implementers of this device use this signal to indicate the revision number of any implementation changes they have made
QVNENABLE<x>	Implementer configuration signal	Implementers of this device enable or disable Virtual Networks functionality using this configuration signal
FPVNSEL<x>[1:0]	Implementer configuration signal	Implementers use this signal to define the Virtual Network number that uses the fast path
FPQVNPREALLOC<x>	Implementer configuration signal	Implementers use this signal to define whether QVN token pre-allocation is enabled or disabled for this implementation

Appendix B
Revisions

This appendix describes the technical changes between released issues of this book.

Table B-1 Issue A

Change	Location	Affects
First release	-	-

Table B-2 Differences between issue A and issue B

Change	Location	Affects
Updates to the constraints of use for clock gating	*Clock gating* on page 2-18	All revisions
Updates to the access permissions to regions section	*Access permissions to regions* on page 2-11	All revisions
Updated the revision field for the Peripheral ID 2 register	*Peripheral ID 2 register bit assignments* on page 3-22	r0p1

Table B-3 Differences between issue B and issue C

Change	Location	Affects
Clarified the description of the security state values of the **ARPROTS<x>[1]** and **AWPROTS<x>[1]** signals.	*Access filtering with regions* on page 2-9	All revisions
Added note to clarify that the TZC-400 cannot fix system issues that relate to transactions and security information becoming temporally offset.	*Access permissions to regions* on page 2-11	All revisions
Clarified information about access permissions for regions. Replaced Table 2-4 with new figure 2-5, showing Non-secure accesses.		All revisions