Introduction

This document contains errata that affect designs using the Ampere Computing® AmpereOne® AC04 and AC04_1 devices.

Each erratum includes an overview, a description of the system impact, and a description of possible workaround(s).

Refer to *Table 2, "Errata Summary", on page 3* for the list of errata.

Errata are organized by the item designator in an alphabetical order. The item designator consists of an acronym for the affected functional unit and a numeric value. Numeric values are assigned to all errata.

Note: *Unless otherwise indicated, the errata listed in this document apply to both the AC04 and AC04_1 devices.*

List of Functional Unit Acronyms

- CPU — AmpereOne AC04 or AmpereOne AC04_1 Processing Element (PE) within the Processor Complex (PCP)
- DEBUG — Debug Access Port (DAP) and other Debug Components
- MCU — Memory Controller Unit
- MESH — Coherent Mesh Network
- PCIe — PCI Express Controller
- SoC — System-on-Chip

Category Definitions

Errata are classified according to system impact and the availability of a workaround.

1. Major impact, no workaround is available. An issue is said to have a major impact if it results in a system crash, a hard failure, an unrecoverable soft failure, significant performance degradation, or the storage of incorrect data.
2. Major impact, workaround is impractical to implement. A substantial risk of encountering the same or additional issues, including performance issues, exist after the workaround is implemented.
3. Major impact, workaround available. Application of the workaround either eliminates the issue, or reduces it to a minor impact issue, or results in significant performance degradation.
4. Minor impact, no workaround is available. Minor impact issues result in slight to moderate performance degradation, or are a functional variance from specification.
5. Minor impact, workaround is available. Minor impact issues result in slight to moderate performance degradation, or are a functional variance from specification.
6. Design enhancement.

List of Abbreviations and Acronyms

Table 1: List of Abbreviations and Acronyms Used in the Document (Sheet 1 of 3)

TERM	DESCRIPTION
1P	Single-Socket Platform
2P	Dual-Socket Platform
ASID	Address Space Identifier
ATB	Advanced Trace Bus

Table 1: List of Abbreviations and Acronyms Used in the Document (Sheet 2 of 3)

TERM	DESCRIPTION
BAR	Base Address Register
BHB	Branch History Buffer
BMC	Baseboard Management Controller
BTB	Branch Target Buffer
CA	Completer Abort
CCM	Core Cluster Module
CE	Corrected Error
CFI	Fault Handling Interrupt Corrected Errors
CPLD	Complex Programmable Logic Device
CTO	Completion Timeout
DC IVAC	Data or Unified Cache Line Invalidate by VA
DC ZVA	Data Cache Zero by VA
DE	Deferred Error
ECC	Error Correcting Code
EL2	Exception Level 2
ELR	Exception Link Register
ERRIIDR	Implementation Identification Register
ETB	Embedded Trace Buffer
ETM	Embedded Trace Macrocell
ETR	Embedded Trace Router
FAR	Fault Address Register
FHI	Fault Handling Interrupt
GIC	Generic Interrupt Controller
HPFAR	Hypervisor IPA Fault Address Register
IPA	Intermediate Physical Address
L2C	Level 2 Cache
LDRAA/LDRAB	Load Register, with Pointer Authentication
MIDR	Main ID Register
MMIO	Memory Mapped I/O

Table 1: List of Abbreviations and Acronyms Used in the Document (Sheet 3 of 3)

TERM	DESCRIPTION
NOP	No Operation
PAC	Pointer Authentication Code
PE	Processing Element
PIO	Programmed Input/Output
PMU	Performance Monitoring Unit
RP	Root Port
SBSA	Server Base System Architecture
SECpro	Security Processor
TLP	Transaction Layer Packet
UE	Uncorrected Error
UR	Unsupported Request
VA	Virtual Address
VMID	Virtual Machine Identifier
WFE	Wait For Event
WFI	Wait For Interrupt

Errata Summary

Table 2: Errata Summary

ERRATA NO.	CATEGORY	DESCRIPTION	PAGE
AC04_CPU_1	4	L1D_CACHE_INVAL PMU overcounts in some situations.	*4*
AC04_CPU_10	3	Certain bits in the Virtualization Translation Control Register and Translation Control Registers do not follow RES0 semantics.	*5*
AC04_CPU_14	3	Timer CVAL programming of a delta greater than 2^{63} will result in incorrect behavior.	*6*
AC04_CPU_19	5	Software reads of ICC_PMR_EL1 return incorrect value in some situations.	*7*
AC04_MCU_2	3	Non-cacheable writes to DDR memory with SKME enabled may result in corruption.	*8*
AC04_MESH_1	5	Incorrect number of children reported in the mesh crosspoint connected to HN-P nodes.	*9*

AC04_CPU_1: L1D_CACHE_INVAL PMU overcounts in some situations.

Functional Unit: CPU

Category: 4

Overview:

L1D_CACHE_INVAL PMU counter may overcount L1D cache invalidations by an amount anywhere from 0 up to L2C_DATA_REFILL + L2D_CACHE_INVAL.

Impact:

L1D_CACHE_INVAL PMU may be unreliable for performance tuning.

Workaround:

None.

AC04_CPU_10: Certain bits in the Virtualization Translation Control Register and Translation Control Registers do not follow RES0 semantics.

Functional Unit: CPU

Category: 3

Overview:

ID_AA64_MMFR1_EL1.HAFDBS will report a value of 0b0000 indicating that the hardware update of the access flag and dirty state are not supported. With FEAT_HAFDBS not supported, the register bits in the Virtualization Translation Control Register (VTCR_EL2) and Translation Control Registers (TCR_EL1, TCR_EL2) for enabling/disabling hardware management of access flag and dirty state – specifically VTCR_EL2.{HA, HD}, TCR_EL1.{HA, HD} and TCR_EL2.{HA, HD}, respectively must follow the RES0 semantics. These bits do not follow the RES0 semantics.

Impact:

Setting VTCR_EL2.{HA, HD}, TCR_EL1.{HA, HD} or TCR_EL2.{HA, HD} can lead to unpredictable behavior.

Workaround:

System software/virtualization system software must not set the TCR_EL1.{HA, HD}, TCR_EL2.{HA, HD} or VTCR_EL2.{HA, HD} bits.

AC04_CPU_14: Timer CVAL programming of a delta greater than 2^{63} will result in incorrect behavior.

Functional Unit: CPU

Category: 3

Overview:

In scenarios where the CompareValue (*CVAL) is greater than or equal to 2^{63} (or 292 years) difference from the counter being compared against, the AmpereOne TimerConditionMet calculation will be wrong (precisely opposite of the expected behavior). This limits Timer functionality to only configure timer interrupts to be within 292 years into the future.

Impact:

There is no expected practical use case for setting a CVAL delta this large. If there is any code that attempts to disable the timer by setting a value > 292 years into the future instead of actually masking it, then it is possible that would result in the timer firing immediately.

Workaround:

Software must enforce that the CVAL value programmed does not exceed a delta of 2^{63} with the counter being compared against.

AC04_CPU_19: Software reads of ICC_PMR_EL1 return incorrect value in some situations.

Functional Unit: CPU

Category: 5

Overview:

Non-secure MRS reads of ICC_PMR_EL1 while SCR_EL3.FIQ==1, when ICC_PMR_EL1 contains the Idle priority, will return 0xF8 instead of the correct non-secure view value of 0xF0.

Impact:

There are no known software impacts. Save/restore operations will restore the correct value in ICC_PMR_EL1 because of the shifting/masking that occurs on MSR writes to that register. Sanity checks in open source software do not commonly hit this case.

Workaround:

When reading ICC_PMR_EL1 from the non-secure security state with SCR_EL3.FIQ==1, treat a read of the value 0xF8 as if it read 0xF0.

AC04_MCU_2: Non-cacheable writes to DDR memory with SKME enabled may result in corruption.

Functional Unit: MCU

Category: 3

Overview:

When Single-Key-Memory-Encryption (SKME) is enabled, non-cacheable writes to encrypted DDR memory may result in SRAM parity errors at the Memory Controller Unit (MCU) or may lead to silent data corruption.

The conditions for this erratum to manifest are:

- SKME enabled in boot firmware via NVPARAM option
- A high rate of back-to-back partial (non-cacheable) writes to DDR memory

Impact:

If SKME is enabled, specialized software or tools that map DDR memory as non-cacheable may result in unreliable system functionality.

Mainstream OS and hypervisor software (such as Linux) will not be impacted due to lack of support for mapping “normal memory” as non-cacheable. Software will typically map DDR memory as cacheable and honor the recommended memory attributes provided by UEFI via the firmware memory map. While it is possible for some specialized software to map DDR memory as non-cacheable or “device” per the architecture, this would be an impractical software design choice on a fully coherent system.

Debug tools (such as OpenOCD) that attempt to trace to memory when memory encryption is enabled would be impacted if the Embedded Trace Router (ETR) is configured to write trace data with the non-cacheable attribute.

Workaround:

Always access DDR memory using cacheable transactions from software (using appropriate page table attributes in both the MMU and SMMU) and debug tools (using ETR settings).

AmpereOne reference UEFI firmware will map all DDR memory regions as cacheable, and OS software is expected to honor these memory map attributes when setting up heap memory. In addition, reference UEFI firmware will set up the ACPI IO Remapping Table (IORT) and PCIe Root Port configuration to always perform cacheable accesses as well.

AC04_MESH_1: Incorrect number of children reported in the mesh crosspoint connected to HN-P nodes.

Functional Unit: Mesh

Category: 5

Overview:

Each mesh crosspoint has a register named “por_mxp_child_info”, which includes a field named “child_count”. This field is intended to report the number of child pointers associated with this crosspoint. For crosspoints that report connected devices of “device_type” 5’b01011 (HN-P type), the child_count value will be incorrectly reported as 8. The correct value must be 2.

Impact:

During software or firmware mesh discovery software flows, this may result in software attempting to dereference the third child pointer, which returns zero. This will result in incorrect discovery behavior and may result in invalid discovery information. The invalid discovery information may result in improper behavior of software or firmware dependent on this information.

Workaround:

In conditions where:

- The device_type is HN-P, or
- The value of the child pointer is zero

Software must ignore and skip the remaining child pointers within the child_info structure.

Revision History

ISSUE	DATE	DESCRIPTION OF MODIFICATIONS
1.00	August 27, 2024	Added erratum AC04_CPU_1 on *page 4*.
		Added erratum AC04_CPU_10 on *page 5*.
		Added erratum AC04_CPU_14 on *page 6*.
		Added erratum AC04_CPU_19 on *page 7*.
		Added erratum AC04_MCU_2 on *page 8*.
		Added erratum AC04_MESH_1 on *page 9*.

August 27, 2024

Ampere Computing reserves the right to change or discontinue this product without notice.

While the information contained herein is believed to be accurate, such information is preliminary, and should not be relied upon for accuracy or completeness, and no representations or warranties of accuracy or completeness are made.

The information contained in this document is subject to change or withdrawal at any time without notice and is being provided on an "AS IS" basis without warranty or indemnity of any kind, whether express or implied, including without limitation, the implied warranties of non-infringement, merchantability, or fitness for a particular purpose.

Any products, services, or programs discussed in this document are sold or licensed under Ampere Computing's standard terms and conditions, copies of which may be obtained from your local Ampere Computing representative. Nothing in this document shall operate as an expressed or implied license or indemnity under the intellectual property rights of Ampere Computing or third parties.

Without limiting the generality of the foregoing, any performance data contained in this document was determined in a specific or controlled environment and not submitted to any formal Ampere Computing test. Therefore, the results obtained in other operating environments may vary significantly. Under no circumstances will Ampere Computing be liable for any damages whatsoever arising out of or resulting from any use of the document or the information contained herein.

AMPERE®

Ampere Computing
4655 Great America Parkway, Santa Clara, CA 95054
Phone: (669) 770-3700
https://www.amperecomputing.com

Ampere Computing reserves the right to make changes to its products, its datasheets, or related documentation, without notice and warrants its products solely pursuant to its terms and conditions of sale, only to substantially comply with the latest available datasheet.

Ampere, Ampere Computing, the Ampere Computing and 'A' logos, Altra, and AmpereOne are registered trademarks of Ampere Computing.

Arm is a registered trademark of Arm Limited (or its subsidiaries) in the US and/or elsewhere. All other trademarks are the property of their respective holders.