Arm® CoreLink™ CMN-600

Software Developer Errata Notice

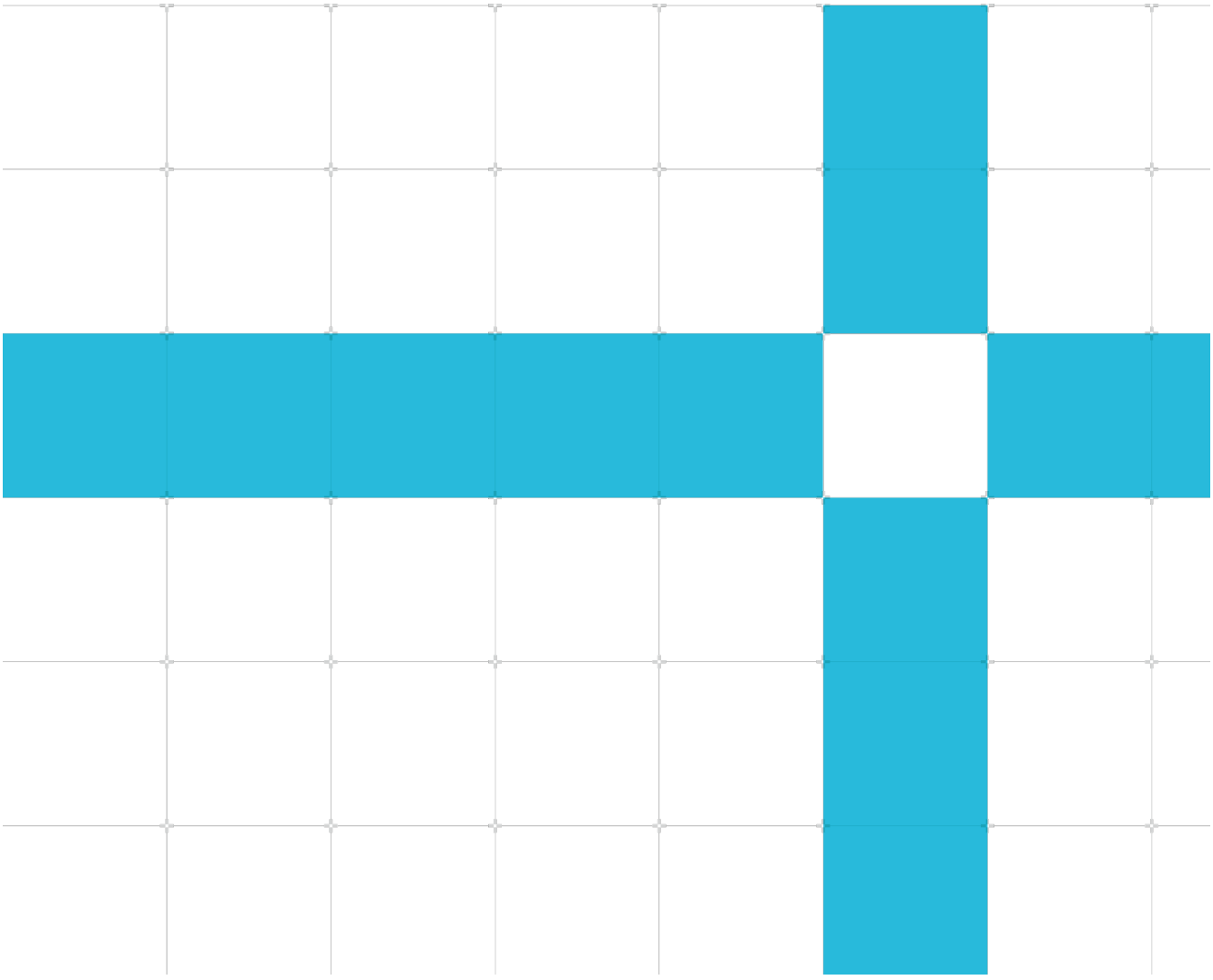
Date of issue: 30-Aug-2023

Non-Confidential

Document version: 13.0

Document ID: SDEN-946098

This document contains all known errata since the r1p0 release of the product.



Non-confidential proprietary notice

Arm Limited. Company 02557590 registered in England.

110 Fulbourn Road, Cambridge, England CB1 9NJ.

(LES-PRE-20349)

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.

Unrestricted Access is an Arm internal classification.

Product status

The information in this document is for a product in development and is not final.

Feedback

Arm welcomes feedback on this product and its documentation. To provide feedback on Arm® CoreLink™ CMN-600, create a ticket on **https://support.developer.arm.com**.

To provide feedback on the document, fill the following survey: **https://developer.arm.com/documentation-feedback-survey**.

Inclusive language commitment

Arm values inclusive communities. Arm recognizes that we and our industry have used language that can be offensive. Arm strives to lead the industry and create change.

If you find offensive language in this document, please email **terms@arm.com**.

Contents

Introduction

Scope

This document describes errata categorized by level of severity. Each description includes:

- The current status of the erratum.
- Where the implementation deviates from the specification and the conditions required for erroneous behavior to occur.
- The implications of the erratum with respect to typical applications.
- The application and limitations of a workaround where possible.

Categorization of errata

Errata are split into three levels of severity and further qualified as common or rare:

Category A	A critical error. No workaround is available or workarounds are impactful. The error is likely to be common for many systems and applications.
Category A (Rare)	A critical error. No workaround is available or workarounds are impactful. The error is likely to be rare for most systems and applications. Rare is determined by analysis, verification and usage.
Category B	A significant error or a critical error with an acceptable workaround. The error is likely to be common for many systems and applications.
Category B (Rare)	A significant error or a critical error with an acceptable workaround. The error is likely to be rare for most systems and applications. Rare is determined by analysis, verification and usage.
Category C	A minor error.

Change Control

Errata are listed in this section if they are new to the document, or marked as "updated" if there has been any change to the erratum text. Fixed errata are not shown as updated unless the erratum text has changed. The **errata summary table** identifies errata that have been fixed in each product revision.

30-Aug-2023: Changes in document version v13.0

ID	Status	Area	Category	Summary
3031697	New	Programmer	Category C	Debug reads with simultaneous coherent traffic or dynamic power transitions can cause deadlock

25-Oct-2022: Changes in document version v12.0

ID	Status	Area	Category	Summary
2741289	New	Programmer	Category C	RAS HN-I and SBSX ERRGSR registers do not capture correct device instance information

08-Oct-2021: Changes in document version v11.0

No new or updated errata in this document version.

01-Apr-2021: Changes in document version v10.0

ID	Status	Area	Category	Summary
2087922	New	Programmer	Category B	PCIe write ordering might not be maintained for writes that target a remote chip

12-Jan-2021: Changes in document version v9.0

No new or updated errata in this document version.

04-Sep-2020: Changes in document version v8.0

ID	Status	Area	Category	Summary
1933951	New	Programmer	Category B	SECC error on ABF operation can cause coherency failures for other memory addresses

17-Apr-2020: Changes in document version v7.0

No new or updated errata in this document version.

27-Sep-2019: Changes in document version v6.0

ID	Status	Area	Category	Summary
1378330	New	Programmer	Category B	32b sized write issues with CMN-600 PPU and DT configuration registers
1572259	New	Programmer	Category B	CMN-600 Address-Based Flush operations may result in deadlock
1393224	New	Programmer	Category C	CML CXHA Non-Secure RAS registers require Secure access
1526051	New	Programmer	Category C	Software error injection feature not functional for 3M or 4M SLC size configurations

30-Nov-2018: Changes in document version v5.0

No new or updated errata in this document version.

12-Oct-2018: Changes in document version v4.0

ID	Status	Area	Category	Summary
1187785	New	Programmer	Category B	ABF Flush does not write back dirty data.
1202667	New	Programmer	Category C	The status bit which indicates the presence of outstanding CopyBack requests at CXRA is incorrect.

23-May-2018: Changes in document version v3.0

ID	Status	Area	Category	Summary
1123342	New	Programmer	Category B	CCIX ReadNoSnp request can be issued with WBnA memory attribute

08-Feb-2018: Changes in document version v2.0

No new or updated errata in this document version.

29-Nov-2017: Changes in document version v1.0

ID	Status	Area	Category	Summary
926702	New	Programmer	Category B	AFREADY may not assert after CMN-600 Debug is disabled
970491	New	Programmer	Category B	Transaction ordering could be violated to physical memory behind HN-I if physical_mem feature is enabled.
980460	New	Programmer	Category B	Power mode transition for 3M System Level Cache could cause SRAM read/write violations
980793	New	Programmer	Category B	Synchronizarion primitives mixing Atomics and Exclusives can cause synchronization to fail among threads
933051	New	Programmer	Category C	HN-F CHI DataSource not consistent for all DAT flits
963908	New	Programmer	Category C	Incorrect data merging in the presence of memory aliasing for CHI-A RN-Fs

Errata summary table

The errata associated with this product affect the product versions described in the following table.

ID	Area	Category	Summary	Found in versions	Fixed in version
1572259	Programmer	Category B	CMN-600 Address-Based Flush operations may result in deadlock	r2p0, r2p1, r3p0, r3p1, r3p2	Open
1378330	Programmer	Category B	32b sized write issues with CMN-600 PPU and DT configuration registers	r1p0, r1p1, r1p2, r1p3, r2p0, r2p1, r3p0, r3p1, r3p2	Open
1187785	Programmer	Category B	ABF Flush does not write back dirty data.	r2p0	r2p1, r3p0
926702	Programmer	Category B	AFREADY may not assert after CMN-600 Debug is disabled	r1p0	r1p1
980793	Programmer	Category B	Synchronizarion primitives mixing Atomics and Exclusives can cause synchronization to fail among threads	r1p0, r1p1	r1p2
980460	Programmer	Category B	Power mode transition for 3M System Level Cache could cause SRAM read/write violations	r1p0, r1p1	r1p2
1123342	Programmer	Category B	CCIX ReadNoSnp request can be issued with WBnA memory attribute	r1p0, r1p1, r1p2, r1p3	r2p0
970491	Programmer	Category B	Transaction ordering could be violated to physical memory behind HN-I if physical_mem feature is enabled.	r1p0, r1p1	r1p2
2087922	Programmer	Category B	PCIe write ordering might not be maintained for writes that target a remote chip	r2p0, r2p1, r3p0, r3p1, r3p2	Open
1933951	Programmer	Category B	SECC error on ABF operation can cause coherency failures for other memory addresses	r2p0, r2p1, r3p0, r3p1, r3p2	Open
1526051	Programmer	Category C	Software error injection feature not functional for 3M or 4M SLC size configurations	r1p0, r1p1, r1p2, r1p3, r2p0, r2p1, r3p0, r3p1, r3p2	Open
1393224	Programmer	Category C	CML CXHA Non-Secure RAS registers require Secure access	r2p0, r2p1, r3p0, r3p1, r3p2	Open
1202667	Programmer	Category C	The status bit which indicates the presence of outstanding CopyBack requests at CXRA is incorrect.	r1p0, r2p0	r2p1, r3p0

ID	Area	Category	Summary	Found in versions	Fixed in version
933051	Programmer	Category C	HN-F CHI DataSource not consistent for all DAT flits	r1p0	r1p1
3031697	Programmer	Category C	Debug reads with simultaneous coherent traffic or dynamic power transitions can cause deadlock	r0p0, r0p1, r1p0, r1p1, r1p2, r1p3, r2p0, r2p1, r3p0, r3p1, r3p2	Open
963908	Programmer	Category C	Incorrect data merging in the presence of memory aliasing for CHI-A RN-Fs	r1p0, r1p1	r1p2
2741289	Programmer	Category C	RAS HN-I and SBSX ERRGSR registers do not capture correct device instance information	r1p0, r1p1, r1p2, r1p3, r2p0, r2p1, r3p0, r3p1, r3p2	Open

Errata descriptions

Category A

There are no errata in this category.

Category A (rare)

There are no errata in this category.

Category B

1572259
CMN-600 Address-Based Flush operations may result in deadlock

Status

Affects: CMN-600
Fault Type: Programmer CAT-B
Fault Status: Present in all CMN-600 R2 and R3 releases. Open.

Description

The CMN Address-Based Flush (ABF) feature ensures all cache lines in an upper/lower address range are flushed from the System Level Cache (SLC) and Snoop Filter (SF). The SF flush sequence can create a hardware resource dependency if the ABF flush operations are issued in the presence of other SF capacity evictions, and result in an overall deadlock.

Configurations Affected

Any CMN-600 configuration that requires the ABF functionality.

Conditions

ABF operations cannot make forward progress if the SEQ is full with SF capacity evictions, resulting in a deadlock.

Implications

The ABF feature may not be usable in the presence of coherent memory transactions.

WorkAround

1. Use address-based Cache Maintenance Operations in place of the ABF flush
2. Put all CPUs into standby state while executing the ABF flush, this will ensure that no transactions will result in SF evictions.

1378330
32b sized write issues with CMN-600 PPU and DT configuration registers

Status

Affects: CMN-600
Fault Type: Programmer CAT-B
Fault Status: Present in all CMN-600 releases. Open.

Description

All 64b of the following registers are written when 32b sized writes are performed:

- por_dt_trigger_status_clr
- por_ppu_qactive_hyst
- por_ppu_int_status
- por_ppu_int_enable

Zero's are written to the non-targeted 32b, which can result in overwriting valid data, or inability to write the full 64b of the register with 32b sized writes.

Configurations Affected

All CMN-600 configurations

Conditions

This erratum occurs when a 32b write is performed on the specified registers.

Implications

The following registers cannot be written using 32b writes for CMN-600 configurations with >32 HN-Fs:

- por_ppu_int_status
- por_ppu_int_enable

The upper 32b of these registers will overwrite valid data in the lower 32b:

- por_dt_trigger_status_clr
- por_ppu_qactive_hyst

Workaround

Use 64b sized writes for these registers for CMN-600 configurations with >32 HNFs:

- por_ppu_int_status
- por_ppu_int_enable

Only write the lower 32b of these registers when performing 32b sized writes:

- por_dt_trigger_status_clr
- por_ppu_qactive_hyst

1187785
ABF Flush does not write back dirty data.

Status:

Affects: CMN-600
Fault Type: System CAT-B
Fault Status: Present in CMN-600 R2P0 EAC release. Fixed in R2P1 and R3P0.

Description:

CMN-600 R2P0 added a new feature for Address Based Flush (ABF) where upper and lower system addresses can be programmed and then request hardware based engine to flush out that address range from all system caches. This ABF state machine aborts if SOC tries to change power state (ex: FAM to HAM request) while ABF is in progress.
This bug appears when abort condition lines up with one specific cycle in ABF state machine and as a result dirty data would not be written back to memory.

Configurations Affected:

Any configuration for CMN-600 R2P0 where ABF interacts with other power state transition requests.

WorkAround:

Do not initiate any power state transitions in HNF while Address Based Flush (ABF) is in progress.

926702
AFREADY may not assert after CMN-600 Debug is disabled

Status:

Affects: CMN-600
Fault Type: System CAT-B
Fault Status: Present in CMN-600 R1P0 release. Fixed in CMN-600 R1P1 release.

Description:

When the CMN-600 debug feature is enabled and then disabled, the ATB AFREADY output could be incorrectly de-asserted, which does not allow completion of an ATB flush request.

Configurations Affected:

Any CMN-600 system that triggers an ATB flush after CMN-600 debug is enabled and then disabled.

Conditions

When the CMN-600 debug feature is enabled and then later disabled, internal ATB AFREADY state may be incorrect based on the timing relationship between the CMN clock domain debug disable and the
ATB domain ATCLKEN.

Implications:

SOC debug logic could deadlock if ATB flushes are issued when CMN-600 debug is disabled.

WorkAround:

1. Do not perform ATB Flush after CMN-600 debug is disabled, not required as all trace data is flushed when CMN-600 debug is disabled.
2. Do no disable CMN-600 debug after enablng, can disable the CMN-600 trace feature to de-activate the ATB interface.

980793
Synchronizarion primitives mixing Atomics and Exclusives can cause synchronization to fail among threads.

Status

Affects: CMN-600
Fault Type: System CAT-B
Fault Status: Present in CMN-600 R1P0 and R1P1 releases. Fixed in CMN-600 R1P2 release.

Description

Synchronization primitives using Global Monitors (ldrex/strex EXCL) and ARM v8.1 Atomics can create synchronization primitive to fail among threads. One thread using Non-Cacheable (NC) EXCL to update a location while another thread using NC atomics to update the same location will end up successfully updating a competing (overlapping) memory location.

Configurations Affected

Any CMN-600 system with RNF (CPU cluster) from non-ARM design. All ARM CPUs use accurate LPID for exclusive transactions.

Conditions

- One thread using NC excl (ldrex/strex) to update location A while another thread updating the same location using ARMv 8.1 atomics to update the same location A.
- Atomics to A will have same LPID in the CHI interface even though it is from a different thread. CHIB spec does not require LPID to be precise with Atomics request (not possible with ARM CPU's as they drive correct LPID but possible with customer CPU)

Implications

1) Synchronization primitive fail as two threads update successfully update a shared memory location. Loss of update form one thread can lead to data corruption and hang the system.

WorkAround

1) Inhibit mixing NC Atomics and NC/dev EXCL for atomic primitives. Use all NC/Dev EXCL or all atomics but never mix.

980460
Power mode transition for 3M system level cache could cause SRAM read/write violations.

Status

Affects: CMN-600
Fault Type: System CAT-B
Fault Status: Present in CMN-600 R1P0 and R1P1 releases. Fixed in CMN-600 R1P2 release.

Description

For 12 way SLC (3M SLC), power transition (like HAM to FAM) could select incorrect way for replacement or it could violate read/write timing.
1) In enhanced LRU mode: Violation could be read/write timing violation when transitioning from HAM to FAM mode in 3M SLC.
2) In LFSR mode: 3M SLC has only ways [11:0] in design but replacement policy could choose ways[15:12], with undesired side-effects.

Configurations Affected

Any CMN-600 system with 3M SLC (12 ways) with support for HAM mode.

Conditions

The issue occurs when system is transitioning away from HAM mode (to FAM or SFONLY mode) in 3M SLC cache.

Implications

1) For Read/Write timing violations case, RAM entries would be read/written at the same time.
2) For Selecting unused ways, we could end up evicting locked (OCM) ways.

WorkAround

1) Not supporting 3M SLC configuration.
2) Only support FAM mode for 3M SLC

1123342
CCIX ReadNoSnp request can be issued with WBnA memory attribute

Status

Affects: CMN-600
Fault Type: System CAT-B
Fault Status: Present in CMN-600 R1P0, R1P1, R1P2, and R1P3 releases. Fixed in CMN-600 R2P0 Release.

Description

Section "3.8.3 Permitted Memory Types for Requests" of the CCIX 1.0 spec it says that "ReadNoSnp/WriteNoSnp can be Normal Non-cacheable or Device." So, this precludes these request types from targeting "WriteBack" memory. CHI allows RNS/WNS to target WriteBack memory type and RA was just passing through the memory type as is.

Configurations Affected

Any configuration that issues RNS/WNS targeting cacheable memory.

Implications

This violates CCIX 1.0 specification and the results could be un-deterministic. If the CCIX Home Agent (HA) on the receiving side treats this as "cacheable" then that can result in memory aliasing issues. Or he can just hang because this is not expected. CCIX Protocol Checker may also fire.

WorkAround

Control this in the page table so that RN never generates a RNS/WNS request targeting cacheable memory. Do not have remote memory that is cacheable and non shareable.

970491
Transaction ordering could be violated to physical memory behind HNI if physical_mem feature is enabled.

Status

Affects: CMN-600
Fault Type: System CAT-C
Fault Status: Present in CMN-600 R1P0 and R1P1 releases. Fixed in CMN-600 R1P2 release.

Description

The HN-I SAM allows downstream memory regions to be mapped as Peripheral memory which guarantees Device memory ordering, or Physical memory (PHYMEM) which guarantees Normal memory ordering. When Peripheral memory (aka non-PHYMEM) requests are intermixed with PHYMEM requests , it is possible for a newer PHYMEM request to bypass older PHYMEM request with same address.

Configurations Affected

Any CMN-600 configuration with PHYMEM region enabled in the HN-I SAM.

Conditions

1. Write to PHYMEM space with address A0 pending in HNI.
2. Read 1 to non-PHYMEM space with address A1 pending in HN-I.
3. Read 2 to PHYMEM space with address A0 arrives in HN-I.
4. Read 2 compares it's 16-bit Addr Hash against Read 1 and matches (even though addresses are different).
5. Read 2 hazards against Read 1 (this is the bug).
6. Read 2 bypasses Write and gets stale data for address A0.

Implications

Read - Write transaction ordering violation resulting in stale data for read.

WorkAround

Do not enable the "physical_mem_en" for any of SAM registers in HN-I, not enabling the PHYMEM performance optimization. By default, physical_mem_en is disabled.

2087922
PCIe write ordering might not be maintained for writes that target a remote chip

Status

Affects: CMN-600
Fault Type: Programmer Category B
Fault Status: Present in r2p0, r2p1, r3p0, r3p1, r3p2. Open.

Description

Two same-**AxID** writes from a PCIe Root Complex (RC) that target a remote chip might be reordered, resulting in a PCIe Ordered Write Observation (OWO) violation.

Configurations Affected

Any multi-chip CML configuration where a CXG is the target for PCIe write traffic.

Conditions

Both of the following conditions must be met for the erratum to exist:

- PCIe write traffic must target CXG (cross-chip traffic).
- RN SAM target type must be programmed to CXRA.

Implications

PCIe ordering violation which might result in data corruption.

Workaround

Set the RN SAM memory region target type to HN-I for the memory region that is targeted by PCIe writes to CXG. This setting has the following effects:

- All writes (WriteNoSnp/WriteUniq/WriteUniqStash) are changed to Non-cacheable WriteNoSnp.
- All reads (RDONCE/ROMI/ROCI) are changed to Non-cacheable ReadNoSnp.
- Reads and writes will still look up the SF and SLC on remote HN-F but will not allocate a line in SLC on a miss.
- Performance implications:
  - Ordered PCIe writes targeting CXG have lower bandwidth since OWO ordering is maintained.
  - Allocating PCIe reads and writes will not allocate in remote SLC.

1933951
SECC error on ABF operation can cause coherency failures for other memory addresses

Status

Affects: CMN-600
Fault Type: Programmer CAT-B
Fault Status: Present in all CMN-600 R2 and R3 releases. Open.

Description

CMN-600 supports Address Based Flush (ABF) where upper and lower system addresses can be programmed and then request hardware-based engine to flush out that address range from all System Level Caches (SLC). This ABF state machine works in the presence of other memory requests.

Single-bit ECC errors on the ABF accesses can corrupt the CMN Snoop Filter state, and result in coherency failures for other unrelated memory addresses.

Configurations Affected

Any configuration of CMN-600 where ABF is used.

Conditions

This bug appears when the following three conditions occur:

- SLC address from flush set/way is outside ABF programmed range AND
- SLC Tag read has single bit ECC error AND
- There is independent request in pipeline N cycles ahead of ABF request (where N is SLC_TAG_RAM_LATENCY)
  In this case, ABF request corrupts SF vector for independent request that's ahead of ABF causing coherency failure.

Implications

The ABF flush sequence can cause coherency fails for unrelated memory addresses during the sequence.

WorkAround

Use the CMN power management features to flush the SLC, flushes the full SLC contents vs. the upper/lower range.

Category B (rare)

There are no errata in this category.

Category C

1526051
Software error injection feature not functional for 3M or 4M SLC size configurations

Status

Affects: CMN-600
Fault Type: Programmer CAT-C
Fault Status: Present in all CMN-600 releases. Open.

Description

The CMN-600 HN-F supports software-configurable error injection to allow testing of software error handling routines. This feature is not functional for 3M or 4M SLC size configurations.

Configurations Affected

Any CMN-600 configuration with 3M or 4M SLC size

Conditions

The erratum occurs when the CMN-600 HN-F error injection register is programmed within a 3M or 4M SLC size configuration. The error will not be injected.

Implications

The CMN-600 Software error injection feature cannot be uses to inject errors and test software handling routines.

WorkAround

Use alternate CMN-600 and/or SOC-level error injection to trigger/test software error handling routines. For example, can use the CMN-600 data byte parity error injection mechanism to inject errors if the CMN-600 configuration has the DATACHECK feature enabled.

1393224
CML CXHA Non-Secure RAS registers require Secure access

Status

Affects: CMN-600
Fault Type: Programmer CAT-C
Fault Status: Present in all CMN-600 R2 and R3 releases. Open.

Description

CMN-600 components have both Secure and Non-secure versions of the ARM RAS registers. The Secure registers log RAS events triggered by Secure accesses, and the Non-secure registers log RAS events triggered by Non-secure accesses. The CML (CCIX interface) CXHA Non-secure RAS registers are incorrectly classified as Secure, and require Secure read/write access.

Configurations Affected

Any CMN-600 configuration that includes CML CCIX interface support.

Conditions

This erratum occurs when Non-secure memory accesses target the Non-secure CXHA RAS registers.

Implications

The software RAS handlers must have Secure access to read/write CXHA RAS registers.

Workaround

The software RAS handler must have Secure access to read/write CXHA RAS registers.

1202667
The status bit which indicates the presence of outstanding CopyBack requests at CXRA is incorrect.

Status

Affects: CMN-600
Fault Type: System CAT-C
Fault Status: Present in CMN-600 R1P0 and CMN-600 R2P0 release. Fixed in R2P1 and R3P0.

Description

CCIX architecture does not have an architectural support of taking down a RA or a chip (comprised of multiple RA) from coherence domain. For power down, it is required that RA is taken out of coherence domain by software or hardware cache flush of all the coherent caches. This cache flush routine needs to ensure all CopyBacks have safely passed on to the target chip through CML CXRA. In order to facilitate that, CML added a status bit in CXRA block to indicate if CopyBacks are pending for software to inspect and take appropriate action. This bit could have been used by CCIX power/link management software to decide when to stop the incoming snoops, in order to take the particular link out of the coherency domain and then eventually power him down. This would have helped to bring down a link or chip without quiescing the entire system. This status bit has a bug where it can be incorrect (i.e falsely indicating that there are no CopyBacks pending).

This bit is useful when all the chips in the system have same/similar indication and in absence of it the entire system must be quiesced to power down any particular link or chip. CCIX going forward will address this architecturally for implementations to follow.

Configurations Affected

CML configuration for CMN-600 R1P0, R2P0.

Implications

System/Software cannot rely on this bit and needs to follow some other mechanism for coherency exit before powering down.

WorkAround

CCIX software must quiesce the entire system before any given chip or link can be powered down.

933051
HN-F CHI DataSource not consistent for all DAT flits

Status:

Affects: CMN-600
Fault Type: System CAT-C
Fault Status: Present in CMN-600 R1P0 release. Fixed in CMN-600 R1P1 release.

Description:

The CMN-600 HN-F could indicate incorrect DataSource values on the non-critical chunk CHI DAT flit. For example, the HN-F could indicate an SLC DataSource value for the non-critical chunk of an SN memory read.

Configurations Affected:

Any CMN-600 system that relies on the non-critical chunk DataSource field to be correct.

Conditions:

The CMN-600 HN-F indicates an SLC DataSource when the DAT flit is scheduled from the internal POCQ. The DataSource is correct if the DAT flit is bypassed when delivered from the SN.

Implications:

PMU counts or prefetch algorithms within the RN-F can be impacted if reliant on the DataSource for the non-critical chunk.

WorkAround:

No workarounds if correct DataSource is required by the RN-F.

3031697
Debug reads with simultaneous coherent traffic or dynamic power transitions can cause deadlock

Status

Affects: CMN-600
Fault Type: Programmer Cat-C
Fault Status: r0p0, r0p1, r1p0, r1p1, r1p2, r1p3, r2p0, r2p1, r3p0, r3p1, r3p2. Open.

Description

HN-F System Level Caches (SLC) and Snoop Filter (SF) Debug Reads with simultaneous coherent traffic or dynamic power retention transitions can cause a deadlock.

Configurations affected

Any configuration.

Conditions

This erratum occurs when one of the following conditions are met:

- Coherent transactions that require HN-F Snoop Filter allocation while performing SLC or SF debug read
- Dynamic retention mode is enabled while performing a SLC or SF debug read

Implications

A deadlock can occur if the conditions are met. Note that expected usage is performing the Debug Reads in the absence of traffic since traffic can change the state of the RAMs.

Workaround

Use the following workarounds to prevent a deadlock:

- Stop CPU (RN-F) and IO (RN-I) coherent traffic before issuing Debug Reads
- Disable Dynamic retention power transitions via por_hnf_ppu_pwpr.dyn_en = 1'b0 (reset value)

963908
Incorrect data merging in the presence of memory aliasing for CHI-A RN-Fs

Status:

Affects: CMN-600
Fault Type: Programmer CAT-C
Fault Status: Present in CMN-600 R1P0 and R1P1 releases. Fixed in CMN-600 R1P2 release.

Description:

Under certain conditions, CMN-600 could incorrectly merge data flits sent by CHI-A RN-F resulting in data corruption or a system hang.

Configurations Affected:

Any CMN-600 with CHI-A RN-F

Conditions:

Software allows memory attribute aliasing and does not follow the ARM ARM cache clean sequence for mismatched
memory attributes. This causes CHI-A RN-F to send multiple transactions with mismatched memory attributes.
Example: CHI-A RNF performs a non-cacheable write when it has the cacheline in modified state due to a
memory attribute change for that page.

Implications:

Write transactions to aliased memory regions accessed with mismatched memory attributes could result in
data corruption or a system hang.

WorkAround:

Ensure that software running on CHI-A RN-F follows the cache clean sequence for mismatched memory attributes as specified in ARM ARM, section E2.8.

2741289
RAS HN-I and SBSX ERRGSR registers do not capture correct device instance information

Status

Affects: CMN-600
Fault Type: Programmer Category C
Fault Status: Present in r1p0, r1p1, r1p2, r1p3, r2p0, r2p1, r3p0, r3p1, r3p2. Open.

Description

The CMN Error Group Status Registers (ERRGSR) capture device instance error information for RAS events. The registers indicate the device instance within a device group. The registers are not updated correctly for the HN-I and SBSX device groups, so cannot be used to determine the device instances for RAS events.

Configurations Affected

All CMN-600 configurations that use RAS error logging.

Conditions

A RAS event triggered by an HN-I or SBSX device.

Implications

Software cannot use the HN-I or SBSX ERRGSR registers.

Workaround

The RAS handler must read the individual HN-I and SBSX instance RAS logging registers when RAS interrupts occur.