ARM DSU (MP090)

Software Developer Errata Notice

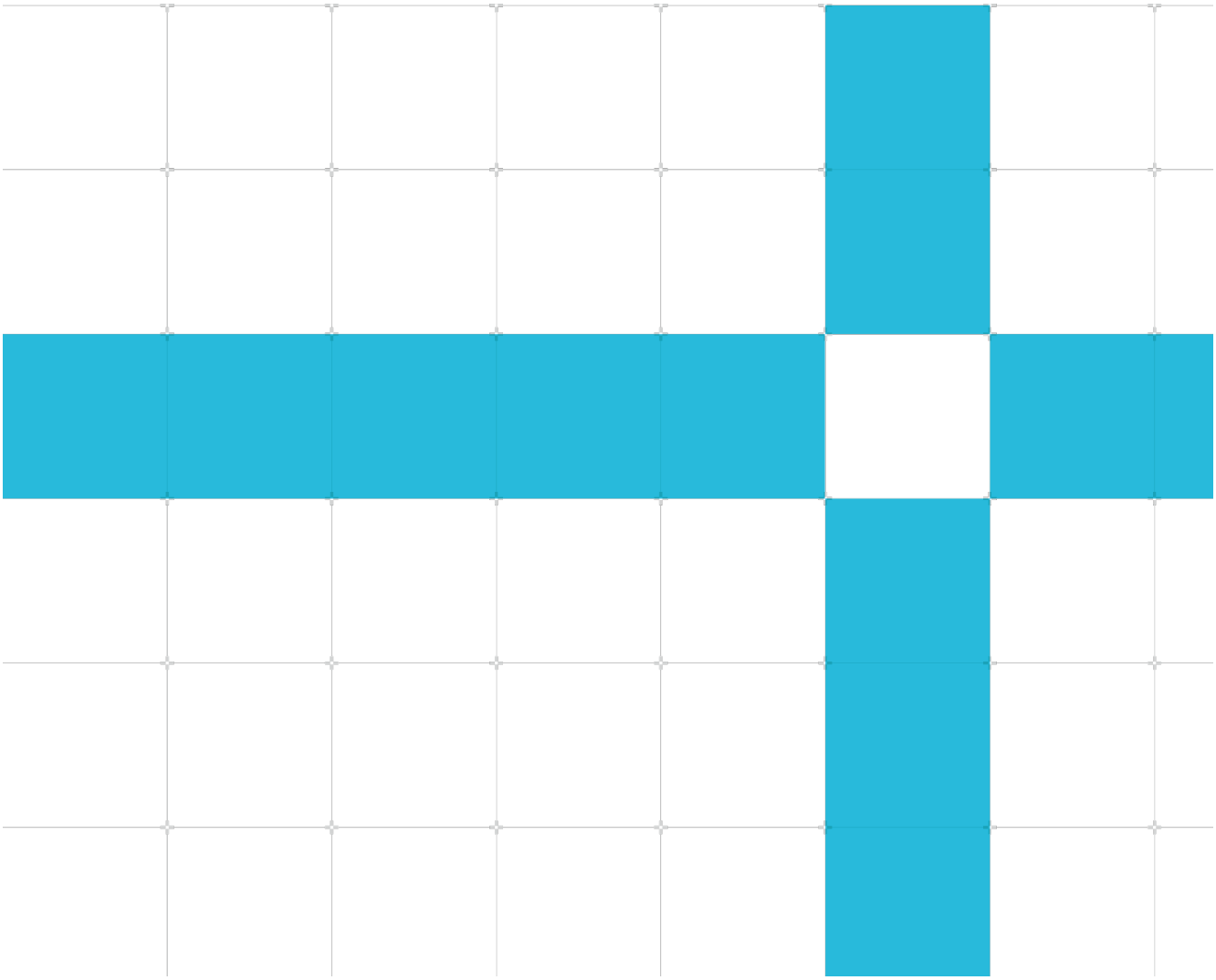
Date of issue: 26-Jun-2023

Non-Confidential

Document version: 20.0

Document ID: SDEN-854652

This document contains all known errata since the r0p0 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.

Feedback

Arm welcomes feedback on this product and its documentation. To provide feedback on ARM DSU (MP090), 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

r3p0 implementation fixes

Note the following errata might be fixed in some implementations of r3p0. This can be determined by reading the CLUSTERREVIDR register where a set bit indicates that the erratum is fixed in this part.

REVIDR[0]	1190471 Core power down might cause data corruption

Note that there is no change to the CLUSTERIDR which remains at r3p0 but the CLUSTERREVIDR is updated to indicate which errata are corrected. Software will identify this release through the combination of CLUSTERIDR/CLUSTERIDR_EL1 and CLUSTERREVIDR/CLUSTERREVIDR_EL1.

r2p0 implementation fixes

Note the following errata might be fixed in some implementations of r2p0. This can be determined by reading the CLUSTERREVIDR register where a set bit indicates that the erratum is fixed in this part.

REVIDR[0]	1190471 Core power down might cause data corruption

Note that there is no change to the CLUSTERIDR which remains at r2p0 but the CLUSTERREVIDR is updated to indicate which errata are corrected. Software will identify this release through the combination of CLUSTERIDR/CLUSTERIDR_EL1 and CLUSTERREVIDR/CLUSTERREVIDR_EL1.

r0p1 implementation fixes

Note the following errata might be fixed in some implementations of r0p1. This can be determined by reading the CLUSTERREVIDR register where a set bit indicates that the erratum is fixed in this part.

REVIDR[1]	848504 Debug request trigger event may fail to halt a core leaving reset

Note that there is no change to the CLUSTERIDR which remains at r0p1 but the CLUSTERREVIDR is updated to indicate which errata are corrected. Software will identify this release through the combination of CLUSTERIDR/CLUSTERIDR_EL1 and CLUSTERREVIDR/CLUSTERREVIDR_EL1.

r0p0 implementation fixes

Note the following errata might be fixed in some implementations of r0p0. This can be determined by reading the CLUSTERREVIDR register where a set bit indicates that the erratum is fixed in this part.

REVIDR[0]	773120 Combinations of external snoops and L1/L2 linefills can cause loss of coherency

Note that there is no change to the CLUSTERIDR which remains at r0p0 but the CLUSTERREVIDR is updated to indicate which errata are corrected. Software will identify this release through the combination of CLUSTERIDR/CLUSTERIDR_EL1 and CLUSTERREVIDR/CLUSTERREVIDR_EL1.

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.

26-Jun-2023: Changes in document version v20.0

ID	Status	Area	Category	Summary
2976798	New	Programmer	Category C	Error record registers indicate pseudo-fault generation support in configurations without cache protection

08-Feb-2023: Changes in document version v19.0

ID	Status	Area	Category	Summary
2832900	New	Programmer	Category C	Interconnect bus errors during write back not recorded in RAS registers
1933378	Updated	Programmer	Category C	Interconnect DErr on dirty data not reported in RAS registers

23-Mar-2022: Changes in document version v18.0

ID	Status	Area	Category	Summary
1162044	Updated	Programmer	Category B	Incorrect ordering of data cache maintenance operations
1741320	New	Programmer	Category B	Use of FUNC_RET power mode prevents thread wakeup in a multithreaded core
2123467	New	Programmer	Category C	No response to Debug APB access during a core reset, in Direct connect configuration
1933378	New	Programmer	Category C	Interconnect DErr on dirty data not reported in RAS registers

23-Oct-2019: Changes in document version v17.0

ID	Status	Area	Category	Summary
1580900	New	Programmer	Category C	Incorrect EDPFR value

12-Aug-2019: Changes in document version v16.0

ID	Status	Area	Category	Summary
1314123	New	Programmer	Category C	Incorrect ordering after change in cacheability

19-Nov-2018: Changes in document version v15.0

ID	Status	Area	Category	Summary
1299953	New	Programmer	Category C	DSU might not report Uncontainable error on atomic instruction

19-Sep-2018: Changes in document version v14.0

ID	Status	Area	Category	Summary
1162044	New	Programmer	Category B	Incorrect ordering of data cache maintenance operations
1219898	New	Programmer	Category C	DSU might fail to detect ECC error
1249448	New	Programmer	Category C	Poison information might get lost in CHI.C direct connect configurations

20-Jul-2018: Changes in document version v13.0

ID	Status	Area	Category	Summary
1190471	New	Programmer	Category A	Core power down might cause data corruption
1116019	New	Programmer	Category B	WFE event might be missed in a multithreaded core
1147200	New	Programmer	Category B	Disabling SIMD retention support while in retention might cause deadlock

22-Jan-2018: Changes in document version v12.0

No new or updated errata in this document version.

16-Oct-2017: Changes in document version v11.0

No new or updated errata in this document version.

07-Aug-2017: Changes in document version v10.0

ID	Status	Area	Category	Summary
936184	New	Programmer	Category B	DSU might lose ACP transactions during clock gating

21-Jun-2017: Changes in document version v9.0

ID	Status	Area	Category	Summary
874812	New	Programmer	Category C	Cluster ELA/CTI ROM table entries present when ELADISABLE is high

26-May-2017: Changes in document version v8.0

ID	Status	Area	Category	Summary
814818	Updated	Programmer	Category B	Allocating streaming write might deadlock

12-May-2017: Changes in document version v7.0

ID	Status	Area	Category	Summary
850423	New	Programmer	Category B	MV/PN bits in ERR1STATUS not implemented as write-one-to-clear

23-Mar-2017: Changes in document version v6.0

ID	Status	Area	Category	Summary
848504	New	Programmer	Category B	Debug request trigger event may fail to halt a core leaving reset
824788	New	Programmer	Category C	Error record overflow field increments on incorrect event

31-Jan-2017: Changes in document version v5.0

ID	Status	Area	Category	Summary
791818	New	Programmer	Category A (rare)	DSU might snoop a core being powered off
795148	New	Programmer	Category A (rare)	DSU might fail to respond to a snoop
798953	New	Programmer	Category B	DSU clock gating might miss transfers on ACE master or Peripheral ports
814818	New	Programmer	Category B	Allocating streaming write might deadlock
792397	New	Programmer	Category C	Reading some ROM table registers always returns 0 when v7 memory map is used

05-Dec-2016: Changes in document version v4.0

ID	Status	Area	Category	Summary
766359	New	Programmer	Category C	ERR1PFGCTLR might inject wrong fault type
774763	New	Programmer	Category C	ECC errors in LTDB RAMs can cause data corruption and/or deadlock
776914	New	Programmer	Category C	CHAIN PMU event counts incorrectly
787516	New	Programmer	Category C	ECC errors in LTDB RAMs can cause spurious reports of correctable errors

09-Nov-2016: Changes in document version v3.0

ID	Status	Area	Category	Summary
773120	New	Programmer	Category A (rare)	Combinations of external snoops and L1/L2 linefills can cause loss of coherency

13-Oct-2016: Changes in document version v2.0

ID	Status	Area	Category	Summary
761074	New	Programmer	Category B	Data corruption to a cacheable line in the lowest 256k of physical address space

06-Oct-2016: Changes in document version v1.0

No errata in this document version.

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
1190471	Programmer	Category A	Core power down might cause data corruption	r0p0, r0p1, r0p2, r1p0, r2p0, r3p0	r4p0
795148	Programmer	Category A (rare)	DSU might fail to respond to a snoop	r0p0	r0p1
791818	Programmer	Category A (rare)	DSU might snoop a core being powered off	r0p0	r0p1
773120	Programmer	Category A (rare)	Combinations of external snoops and L1/L2 linefills can cause loss of coherency	r0p0	r0p1
1741320	Programmer	Category B	Use of FUNC_RET power mode prevents thread wakeup in a multithreaded core	r0p0, r0p1, r0p2, r1p0, r2p0, r3p0, r4p0, r4p1	Open
1162044	Programmer	Category B	Incorrect ordering of data cache maintenance operations	r0p0, r0p1, r1p0, r2p0, r3p0, r4p0, r4p1	Open
850423	Programmer	Category B	MV/PN bits in ERR1STATUS not implemented as write-one-to-clear	r0p0, r0p1	r0p2, r1p0
848504	Programmer	Category B	Debug request trigger event may fail to halt a core leaving reset	r0p0, r0p1	r0p2, r1p0
1147200	Programmer	Category B	Disabling SIMD retention support while in retention might cause deadlock	r0p0, r0p1, r0p2, r1p0, r2p0, r3p0	r4p0
814818	Programmer	Category B	Allocating streaming write might deadlock	r0p0	r0p1
1116019	Programmer	Category B	WFE event might be missed in a multithreaded core	r3p0	r4p0
936184	Programmer	Category B	DSU might lose ACP transactions during clock gating	r0p1, r0p2, r1p0	r2p0
798953	Programmer	Category B	DSU clock gating might miss transfers on ACE master or Peripheral ports	r0p0	r0p1
761074	Programmer	Category B	Data corruption to a cacheable line in the lowest 256k of physical address space	r0p0	r0p1

ID	Area	Category	Summary	Found in versions	Fixed in version
1933378	Programmer	Category C	Interconnect DErr on dirty data not reported in RAS registers	r0p0, r0p1, r0p2, r1p0, r2p0, r3p0, r4p0, r4p1	Open
1580900	Programmer	Category C	Incorrect EDPFR value	r4p0	r4p1
2123467	Programmer	Category C	No response to Debug APB access during a core reset, in Direct connect configuration	r0p0, r0p1, r0p2, r1p0, r2p0, r3p0, r4p0, r4p1	Open
1219898	Programmer	Category C	DSU might fail to detect ECC error	r0p0, r0p1, r0p2, r1p0, r2p0, r3p0	r4p0
1314123	Programmer	Category C	Incorrect ordering after change in cacheability	r0p0, r0p1, r0p2, r1p0, r2p0, r3p0, r4p0	Open
874812	Programmer	Category C	Cluster ELA/CTI ROM table entries present when ELADISABLE is high	r0p0, r0p1	r0p2
824788	Programmer	Category C	Error record overflow field increments on incorrect event	r0p0, r0p1	r0p2, r1p0
1299953	Programmer	Category C	DSU might not report Uncontainable error on atomic instruction	r0p0, r0p1, r0p2, r1p0, r2p0, r3p0	r4p0
1249448	Programmer	Category C	Poison information might get lost in CHI.C direct connect configurations	r2p0, r3p0	r4p0
792397	Programmer	Category C	Reading some ROM table registers always returns 0 when v7 memory map is used	r0p0	r0p1
787516	Programmer	Category C	ECC errors in LTDB RAMs can cause spurious reports of correctable errors	r0p0	r0p1
774763	Programmer	Category C	ECC errors in LTDB RAMs can cause data corruption and/or deadlock	r0p0	r0p1
776914	Programmer	Category C	CHAIN PMU event counts incorrectly	r0p0	r0p1
766359	Programmer	Category C	ERR1PFGCTLR might inject wrong fault type	r0p0	r0p1
2976798	Programmer	Category C	Error record registers indicate pseudo-fault generation support in configurations without cache protection	r0p0, r0p1, r0p2, r1p0, r2p0, r3p0, r4p0, r4p1	Open
2832900	Programmer	Category C	Interconnect bus errors during write back not recorded in RAS registers	r0p0, r0p1, r0p2, r1p0, r2p0, r3p0, r4p0, r4p1	Open

Errata descriptions

Category A

1190471
Core power down might cause data corruption

Status

Affects: DSU
Fault Type: Programmer Category A
Fault Status: Present in r0p0, r0p1, r0p2, r1p0, r2p0, and r3p0. Fixed in r4p0.

Description

If a core silently evicts a cache line and is later powered off, then the line might remain present in the DSU snoop filter. If there is further activity to this cache line while the core is powered off, then that can later cause a loss of cache coherency to that line when the core is powered on.

Configurations Affected

This erratum affects all configurations of the DSU when the DSU **BROADCASTOUTER** input pin is 1, indicating it is connected to a coherent interconnect, and either:

- The interconnect has a snoop filter.
- There is another fully coherent master connected to the interconnect.

Note that the types of cores present in the cluster affect the severity of this erratum. If no Cortex-A75 cores are configured, then this reduces the severity to a Category C erratum.

Conditions

1. A core performs a read of a cache line.
2. The core evicts the line from its L1 and L2 cache without notifying the DSU (this is referred to as a silent eviction).
3. The core is powered down.
4. No other cores in the cluster have a copy of the cache line.
5. Another core in the cluster or another master accesses the cache line.
6. The core is powered up.
7. Another core in the cluster or another master accesses the cache line.

If these conditions are met, in combination with the configurations affected, then in some cases the DSU might cause loss of coherency for the cache line between the DSU and another master connected to the interconnect.

Implications

If the erratum occurs, then the loss of coherency can lead to data corruption and in some systems potentially deadlock.
One of the conditions required is a silent eviction from a core. The conditions and implications therefore also depend on the type of cores present:

- For Cortex-A75, silent evictions are possible when heavy memory traffic causes internal buffers to fill up.
- For all other types of cores, a silent eviction is only possible when some types of uncorrectable ECC errors are detected. Therefore, the only implications for these cores are a small increase in detected uncorrected error (DUE) failure in time (FIT) rate.

Workaround

There is no workaround for this erratum.

Category A (rare)

795148
DSU might fail to respond to a snoop

Status

Affects: DSU
Fault Type: Programmer Category A Rare
Fault Status: Present in r0p0. Fixed in r0p1.

Description

In rare situations, it is possible for the DSU to fail to respond to a snoop from the interconnect because of a livelock in the DSU, leading to a system deadlock.

Configurations Affected

This erratum affects systems that have a coherent interconnect connected to the ACE master port.

Conditions

1. The interconnect connected to the DSU ACE master port(s) sends a snoop to the DSU. The interconnect requires the snoop to make progress before it will make progress on certain transactions from the DSU.
2. There are transactions inside the DSU that incorrectly happen to block the snoop from making progress. This is most likely if these transactions all share the same L3 index, that is the lower bits of the cache-line address are the same.

Implications

If the erratum occurs, the DSU will not make any progress on the snoop transaction and so the system will deadlock.
Note that this is categorized as rare on the assumption that the revisions affected are only used for engineering samples, and not production.

Workaround

There is no workaround for this erratum.

791818
DSU might snoop a core being powered off

Status

Affects: DSU
Fault Type: Programmer Category A Rare
Fault Status: Present in r0p0. Fixed in r0p1.

Description

Under rare conditions, it is possible for the DSU to send a snoop to a core that is being powered off, leading to deadlock.

Configurations Affected

This erratum affects all configurations of the DSU.
Note that the types of cores present in the cluster affect the severity of this erratum. If only Cortex-A55 cores are configured, then this reduces the severity to a Category C erratum.

Conditions

1. A core in the DSU cluster silently evicts a cache-line from its L1 and L2 cache without notifying the DSU (this is referred to as a silent eviction).
2. Later, the power controller uses the core P-channel interface to request to power off that core.
3. During the power off sequence, the DSU sends a snoop to the core after the core does not expect any more snoop requests.

Implications

If the erratum occurs, the core or cluster can deadlock. Note that this erratum is categorized as rare and is not expected to impact engineering samples.
One of the conditions required is a silent eviction from a core. The conditions and implications therefore also depend on the type of cores present:

- For Cortex-A55, a silent eviction is only possible when some types of uncorrectable ECC errors are detected. Therefore the only implications for Cortex-A55 are a small increase in detected uncorrected error (DUE) failure in time (FIT) rate.
- For Cortex-A75, silent evictions are also possible when heavy memory traffic causes internal buffers to fill up.

Workaround

There is no workaround for this erratum.

773120
Combinations of external snoops and L1/L2 linefills can cause loss of coherency

Status

Affects: DSU
Fault Type: Programmer Category A (Rare)
Fault Status: Present in r0p0. Fixed in r0p1.

Description

Under rare conditions, it is possible for the DSU to cause a loss of cache coherency, leading to data corruption and potentially deadlock.

Configurations Affected

This erratum affects all configurations of the DSU when connected to a coherent interconnect.
Note that the types of cores present in the cluster affect the severity of this erratum. If only Cortex-A55 cores are configured, then this reduces the severity to a Category C erratum.

Conditions

1. A core starts a linefill for a cache line at an address A0.
2. A core starts a linefill for a cache line at an address A1.
3. Address A1 is different to A0, but some of the lower address bits are the same so that they both map to the same set in the DSU snoop filter.
4. The set in the snoop filter is full with other addresses, so that the access to A1 causes a capacity eviction of the entry containing address A0.
5. The core that previously requested a linefill for the cache line at address A0 evicts the line from its L1 and L2 cache without notifying the DSU (this is referred to as a silent eviction).
6. A core requests a new linefill for address A0.
7. There is an external interconnect snoop for the cache line at address A0 at a time so that the previous linefill from the core for the same cache line is still outstanding in the interconnect.

If these conditions are met under certain timing conditions, the DSU might cause loss of coherency for the cache line at address A0. This loss of coherency can lead to data corruption as well as potential deadlock in the L1 and L2 memory systems of the connected cores.

Implications

If the erratum occurs, the loss of coherency can lead to data corruption and/or deadlock.
One of the conditions required is a silent eviction from a core. The conditions and implications therefore also depend on the type of cores present:

- For Cortex-A55, a silent eviction is only possible when some types of uncorrectable ECC errors are detected. Therefore the only implications for Cortex-A55 are a small increase in detected uncorrected error (DUE) failure in time (FIT) rate.
- For Cortex-A75, silent evictions are also possible when heavy memory traffic causes internal buffers to fill up.

Workaround

There is no workaround for this erratum.

Category B

1741320
Use of FUNC_RET power mode prevents thread wakeup in a multithreaded core

Status

Affects: DSU
Fault Type: Programmer Category B
Fault Status: Present in r0p0, r0p1, r0p2, r1p0, r2p0, r3p0, r4p0, and r4p1. Open.

Description

A core can implement support for the FUNC_RET and/or the FULL_RET power modes. When FUNC_RET is disabled in the CPUPWRCTLR_EL1.SIMD_RET_CTRL field (which is the default), power transitions are allowed directly between the ON and FULL_RET power modes. When FUNC_RET is enabled, transitions between FULL_RET and ON must go through FUNC_RET, and any direct transitions will be denied as documented in the DSU Technical Reference Manual.
When the DSU is configured with a multithreaded core, the state of the two threads can be controlled with the operating mode in the core P-Channel. If the multithreaded core is in the FULL_RET power mode, then the core must be moved to the ON power mode before the operating mode can be changed. When used with the Arm Power Policy Unit (PPU) in the PCK-600 product, the PPU will not be aware of the CPUPWRCTLR_EL1.SIMD_RET_CTRL status and will always request a direct transition from FULL_RET to ON in this situation. The transition will be repeatedly denied by the core, which can lead to a system deadlock.

Configurations Affected

This erratum only affects configurations that include a multithreaded core and implement functional retention mode support in the core.

Conditions

1. One thread in the core is active.
2. The CPUPWRCTLR_EL1.SIMD_RET_CTRL field is set to a nonzero value.
3. The CPUPWRCTLR_EL1.WFI_RET_CTRL field or the CPUPWRCTLR_EL1.WFE_RET_CTRL field is set to a nonzero value.
4. The active thread executes a WFI or WFE instruction which causes the core to enter FULL_RET power mode.
5. The PPU receives a wake request for the other thread, and so requests that the core moves to the ON power mode directly from the FULL_RET mode.

Implications

The core will repeatedly deny the transition to ON. If there is no activity that causes the first thread to leave WFE or WFI, then the system will not be able to activate the second thread, which might lead to a system deadlock.

For implementors targeting functional safety applications:
An additional source for existing failure mode end effects of Livelock and Deadlock should be added in the 'cb_sys' part and 'cb_sys_cpm' sub-parts of the Cortex-A65 FMEDA Report. 'Incorrect power p-channel response can cause power mode transitions to be constantly denied'. This additional source will not change the diagnostic metrics reported in the FMEDA Report for Cortex-A65.

Workaround

The software should avoid setting the CPUPWRCTLR_EL1.SIMD_RET_CTRL register. If the implementation supported the FUNC_RET power mode, then this will prevent the benefit of the lower leakage power savings from that mode.
If the implementation wants to support the FUNC_RET mode, then additional system logic between the cluster and the PPU is possible, please contact Arm for more details about this.

1162044
Incorrect ordering of data cache maintenance operations

Status

Affects: DSU
Fault Type: Programmer Category B
Fault Status: Present in r0p0, r0p1, r0p2, r1p0, r2p0, r3p0, r4p0 and r4p1. Open.

Description

When using Cortex-A55 cores or Cortex-A75 cores with certain uncommon memory types that are not cached in the cluster, the DSU might perform a data Cache Maintenance Operation (CMO) before a store instruction to the same address, even when the Arm architecture requires that these instructions occur in program order. The types of memory and CMOs that are affected depend on the configuration of the system. Instruction CMOs, branch prediction maintenance operations, and data CMOs by set/way are not affected.

Configurations Affected

This erratum only affects DSU clusters that contain at least one Cortex-A55 core or Cortex-A75 core and where:

- The DSU input signal **BROADCASTPERSIST**=1, indicating that the system implements the Point of Persistence. In this case, the AArch64-only Clean to the Point of Persistence instruction `DC CVAP` is affected.
- A system cache is present and it caches transactions based on bit [6] of the appropriate DSU output signal **SRCATTR**. In this case, all data CMOs that specify an address are affected except CMOs to the Point of Persistence (`DC CVAP`), which depend on the previous condition. If the DSU input signal **BROADCASTCACHEMAINTPOU**=0, then data CMOs to the Point of Unification are not affected either.

This erratum only occurs if one, but not both, of the above conditions are true.

Conditions

1. A Cortex-A55 core or Cortex-A75 core executes a store instruction to memory that is one of the types listed below.
2. The same core subsequently executes an affected CMO to the same cache line address without a `DMB` or `DSB` instruction in between.

If the Clean to the Point of Persistence instruction (`DC CVAP`) is affected, then the erratum can occur when used with one the following memory types:

- For AArch64 only:
  - Inner Write-Back, Outer Write-Through.
  - Inner Write-Back, Outer Non-cacheable.
  - Inner Write-Through, Outer Write-Back.
  - Inner Write-Through, Outer Write-Through.
  - Inner Write-Through, Outer Non-cacheable.

If other types of CMO are affected, then the erratum can occur when used with one of the following memory types:

- For AArch64:
  - Inner Write-Back, Outer Write-Through.
  - Inner Write-Through, Outer Write-Back.
  - Inner Write-Through, Outer Write-Through.
- For AArch32:
  - Inner Write-Back, Outer Write-Through.
  - Inner Write-Through, Outer Write-Back.
  - Inner Write-Through, Outer Write-Through.
  - Inner Non-cacheable, Outer Write-Back.
  - Inner Non-cacheable, Outer Write-Through.

Implications

These memory types are not expected to be common, so most software should not be affected. If these memory types are used, then the CMO might occur before the store, even though they should occur in program order.

Where CMOs to the Point of Persistence are affected, the CMO does not guarantee that a previous store to the same address has reached the Point of Persistence. As a result, some stores might not have reached persistent memory when software believes they have, which might lead to corruption of persistent storage during powerdown or a power failure.

Where other types of CMOs are affected, the cache line might not be cleaned or invalidated from the system cache. As a result, software using CMOs might lose coherency between the DSU and other masters that access memory without accessing the system cache.

Workaround

If possible, software should use Inner Write-Back, Outer Write-Back memory or Inner Non-Cacheable, Outer Non-Cacheable memory. If this is not possible, then software can work around this erratum by inserting a `DMB` instruction before an affected CMO, which ensures that any previous stores are ordered before the CMO.

850423
MV/PN bits in ERR1STATUS not implemented as write-one-to-clear

Status

Affects: DSU
Fault Type: Programmer Category B
Fault Status: Present in r0p0, r0p1. Fixed in r1p0 and r0p2.

Description

The DSU implements the ERR1STATUS system register to provide status information for the DSU error record. The MV and PN bits in that register are meant to be write-one-to-clear, but are incorrectly implemented as write-zero-to-clear.

Configurations Affected

All configurations of the DSU are affected.

Conditions

1. The ERR1STATUS MV bit or PN bit is 1.
2. Software writes to the ERR1STATUS. Note: the MV and PN bits ignore writes if any of ERR1STATUS. {CE, DE, UE}

   are set to 1, and the highest priority of these is not being cleared to 0 in the same write.

   - If the write value of the MV or PN bit is 0 and the bit was previously 1, the bit will be cleared, which is incorrect.
   - If the write value of the MV or PN bit is 1 and the bit was previously 1, the bit will not be cleared, which is incorrect.

Implications

The DSU will not clear the MV and PN bits when software expects. The DSU might clear the MV and PN bits when software does not expect.
This means that the PN bit might remain incorrectly set for later correctable or deferred errors, and software might infer that more Uncorrectable or Deferred errors are caused by poison than is the case.

Workaround

Software should treat the MV and PN bits as write-zero-to-clear instead of write-one-to-clear.

848504
Debug request trigger event might fail to halt a core leaving reset

Status

Affects: DSU
Fault Type: Programmer Category B
Fault Status: Present in r0p0 and r0p1. Fixed in r1p0 and r0p2.

Description

The debug request trigger event is an output trigger event from the CTI. It is asserted by the CTI to force a core into Debug state. If the debug request trigger event is asserted when the core is powered-off or in a Cold reset, then when the core leaves reset the trigger event might halt the wrong core.

Configurations Affected

The erratum affects all configurations of the DSU with more than one core present.

Conditions

1. A debug request trigger event is asserted for any core except core 0.
2. The core is powered-off or in a Cold reset.
3. The core leaves reset.

Implications

The trigger will be sent to core 0 rather than the intended core, which results in the intended core not entering Debug state when it leaves reset. This impacts the ability to debug over powerdown scenarios.

Workaround

When the CTI trigger is programmed, the DBGPRCR_EL1.CORENPDRQ or EDPRCR.CORENPDRQ bit should be set on each core. This prevents the core from powering off, instead going to the emulated power off state. When the core leaves the emulated power off state, it will be warm reset rather than cold reset, and so will not trigger the erratum.

An alternative workaround is also available that avoids emulated power off. The debugger can set the EDECR.RCE bit on all cores to enable the Reset Catch debug event. This will cause all cores to enter Debug state every time they leave a Cold reset. The debugger can then read the CTITRIGOUTSTATUS[0] bit to determine whether the core should remain in Debug state because of a cross trigger, or it should exit from Debug state and continue to boot normally. This will have an impact on performance when a core boots up.

1147200
Disabling SIMD retention support while in retention might cause deadlock

Status

Affects: DSU
Fault Type: Programmer Category B
Fault Status: Present in r0p0, r0p1, r0p2, r1p0, r2p0, and r3p0. Fixed in r4p0.

Description

LITTLE cores in a DSU cluster support putting the SIMD/FP logic into a retention state. If this SIMD/FP retention mode is disabled by software while the SIMD/FP logic is already in retention and Core retention mode is enabled, then it can lead to a deadlock.

Configurations Affected

This erratum only affects LITTLE cores that implement functional retention support for the SIMD/FP logic.

Conditions

1. The CPUPWRCTLR_EL1 SIMD_RET_CTLR field is programmed to a nonzero value.
2. The CPUPWRCTLR_EL1 WFE_RET_CTLR or WFI_RET_CTLR fields are programmed to a nonzero value.
3. No SIMD or FP instructions are executed for a time longer than programmed in the CPUPWRCTLR_EL1 register, so the power controller puts the core into the FUNC_RET power mode.
4. The CPUPWRCTLR_EL1 SIMD_RET_CTLR field is programmed to zero.
5. A WFE or WFI instruction is executed.
6. The power controller puts the core into the FULL_RET power mode.
7. Some activity occurs that requires the core to leave FULL_RET. This could be a wakeup event or interrupt for the WFE/WFI, or could be a temporary wakeup, for example, to process a snoop.

Implications

The **COREPACTIVEx[8]** bit is set indicating the ON power mode is requested, however if the power controller requests to go directly from the FULL_RET mode to ON, then the DSU denies the request. This might lead to a deadlock.

Workaround

In many implementations, the SIMD retention enable is a static setting so no workaround is needed. If software needs to dynamically disable SIMD retention, then it should execute a SIMD or FP instruction immediately after writing to the CPUPWRCTLR_EL1.SIMD_RET_CTLR field. This ensures that the SIMD/FP logic is not in retention by the time a WFI or WFE is executed. Note that interrupts might need to be disabled during this sequence to ensure that a WFI/WFE cannot be executed by a different context before the SIMD logic has left the retention state.
If a software workaround is not possible, then a hardware fix is possible. If the power controller makes a request to go directly from FULL_RET to ON, and the request gets unexpectedly denied, then it should instead try to go from FULL_RET to FUNC_RET, and then to ON, and the requests are accepted.

814818
Allocating streaming write might deadlock

Status

Affects: DSU
Fault Type: Programmer Category B
Fault Status: Present in r0p0. Fixed in r0p1.

Description

In rare situations, it is possible for the DSU to fail to complete a streaming write transaction, leading to a system deadlock.

Configurations Affected

This erratum affects systems that have a coherent interconnect connected to the ACE master port.

Conditions

1. A core executes a full cache line of stores and these do not allocate into the L1 or L2 caches in the core, but do allocate into the L3 cache in the DSU.
2. Other microarchitectural timing conditions occur.
3. Another transaction is executed to the same L3 index, or a request is made to power down the cluster.

Implications

If the erratum occurs, the subsequent transaction or powerdown will not complete, and so the system will deadlock.

Workaround

For Cortex-A55 cores, you must ensure that for Normal Inner Write-Back Outer Write-Back memory the Outer Write-Allocate policy is No Allocate. This can be done by programming the Memory Attribute Indirection Registers appropriately. Note that if using virtualization then trapping accesses to these registers may impact the ability to run such workloads.
For Cortex-A75 cores, you must program the Cortex-A75 register field CPUECTLR.L3_STREAM to 0b11.

1116019
WFE event might be missed in a multithreaded core

Status

Affects: DSU
Fault Type: Programmer Category B
Fault Status: Present in r3p0. Fixed in r4p0.

Description

When the DSU is configured with a multithreaded core, the state of the two threads can be controlled with the operating mode in the core P-Channel. If the multithreaded core is in the On power mode, then a WFE wakeup event to a thread can be lost if the second thread is being activated or deactivated using the **COREPSTATEx[5:4]** bits at the same time.

Configurations affected

This erratum only affects configurations that include a multithreaded core.

Conditions

1. The core is in the On power mode.
2. Thread 0 is in WFE state.
3. Thread 1 is being activated or deactivated using **COREPSTATEx[5:4]** bits.
4. A WFE wakeup event arrives for Thread 0 at the same time Thread 1 is undergoing the power mode transition.
   Alternatively, Thread 0 can be in WFE while Thread 1 is being activated or deactivated.

Implications

If the above conditions are met, then under specific microarchitectural timing conditions, Thread 0 will miss the wakeup event and remain in WFE.
The following wakeup events will still wake the thread up:

1. Physical and virtual interrupts, depending on the software settings in the core execution pipeline.
2. External debug request, when halting is allowed.
3. Any of the following events for the thread in WFE, if they arrive after the thread activation/deactivation for the second thread is complete:
   - An event from SEV instruction from any thread in the system.
   - An event sent by the timer event stream for the thread.
   - An event caused by the clearing of the global monitor for the thread.

Workaround

Software should program the timer to generate an event stream for the PE.

936184
DSU might lose ACP transactions during clock gating

Status

Affects: DSU
Fault Type: Programmer Category B
Fault Status: Present in r0p1, r0p2, and r1p0. Fixed in r2p0.

Description

Under certain near idle conditions, it is possible for the DSU to miss an address transfer on the ACP interface, leading to deadlock. In addition, if multiple transactions are sent with the same ACP ID then data corruption might occur.

Configurations Affected

This erratum only affects configurations of the DSU that contain the ACP interface.

Conditions

1. The DSU is idle, which allows the hardware to gate the DSU clock.
2. Around the same time, the DSU receives an ACP address transfer for a new transaction.

Implications

If the erratum occurs, the DSU will lose the last address transfer and so the system might deadlock. If another address transfer is sent on the same channel with the same ID, then data corruption might occur.

Workaround

The erratum can be prevented by software writing the DSU register CLUSTERACTLR[16:15] to 0b11 to disable high-level clock gating of the DSU. This will increase the power consumption of the DSU when idle.

798953
DSU clock gating might miss transfers on ACE master or Peripheral ports

Status

Affects: DSU
Fault Type: Programmer Category B
Fault Status: Present in r0p0. Fixed in r0p1.

Description

Under certain near idle conditions, it is possible for the DSU to miss response transfers on the ACE master port or Peripheral port, leading to deadlock.

Configurations Affected

This erratum affects all configurations of the DSU.

Conditions

1. The DSU issues one or more transactions on the ACE master port or the Peripheral port.
2. The DSU is otherwise idle, and attempts to gate the clock internally.
3. The system returns a response on the B-channel or R-channel while the DSU is clock-gated and so the DSU does not notice the response.

Implications

If the erratum occurs, the DSU will not notice the response and so the system can deadlock.

Workaround

This erratum can be prevented by software writing the DSU register CLUSTERACTLR[15] to 0b1 to disable high-level clock gating of the DSU. This will increase the power consumption of the DSU when idle. Note that there is a small risk of encountering this erratum before the register write is performed.

761074
Data corruption to a cacheable line in the lowest 256K of physical address space

Status

Affects: DSU
Fault Type: System Category B
Fault Status: Present in r0p0. Fixed in r0p1.

Description

If a combination of multiple linefills occurs to different but related addresses, then it can cause data corruption if one of the linefills is in the lowest 256K of physical address space.

Configurations Affected

This erratum affects all configurations of the DSU.

Conditions

1. One or more pages in the range 0x0 to 0x3FFFF of the physical address map are marked as writeback cacheable memory.
2. A core performs linefills to at least three different addresses that map to the same index in the DSU snoop filter and cause the snoop filter to perform at least two back invalidations because of reaching capacity at that index.
3. The interconnect sends a snoop to the same index as one of the linefills.
4. There is a dependency in the interconnect so that one of the linefills cannot complete until after the snoop has completed.

Implications

Some SoCs might have peripherals or other non-memory components at the lowest parts of the address map, and therefore will not be affected by this erratum. For those SoCs that are affected, this erratum can result in data corruption to a cacheable line in the lowest 256K of physical address space.

Workaround

If a workaround is required, then the firmware or OS must ensure that the lowest 256K of physical address space is never marked as writeback cacheable memory.
Note that if this address range contained flash memory containing boot code, then the memory could be marked as Write-Through cacheable. This would work around this erratum and still allow it to be cached in the instruction cache but not in the data cache.

Category B (rare)

There are no errata in this category.

Category C

1933378
Interconnect DErr on dirty data not reported in RAS registers

Status

Fault Type: Programmer Category C
Fault Status: Present in r0p0, r0p1, r0p2, r1p0, r2p0, r3p0, r4p0, and r4p1. Open.

Description

Some errors reported by the interconnect on reads that allocate to L3 will not be reported in the DSU RAS Error Record Registers.

Configurations Affected

This erratum affects configurations of the DSU with at least one CHI master port configured. It does not affect Direct connect configurations.
It also requires the interconnect to use DErr responses rather than the poison support on CHI.

Conditions

1. Either of the following occurs:
    - The DSU requests a linefill that allocates to L3. This could be generated from a PRFM instruction targeting L3 or, on some cores, the hardware prefetcher can generate these requests.
    - The interconnect sends a stashing snoop to the DSU and the DSU responds by requesting a Data Pull.
2. The interconnect returns dirty data with a DErr response indicating that there is an error in the data.

Implications

The DSU will not allocate the line to L3 because of the error, and so the dirty data will be discarded. The DSU RAS Error Record Registers are not correctly updated to indicate that the dirty data was lost. The original cause of the error happened outside of the DSU and should have been logged by the component that detected the error, although, this might have been recorded as a deferred error.
For systems that use DErr responses, there might be a negligible increase in overall system failure rate because of this erratum. However, any system where RAS is particularly important would be expected to use the poison field rather than signal a DErr, since the poison allows the line to be allocated into L3 and the error can remain deferred.

Workaround

No workaround is necessary.

1580900
Incorrect EDPFR value

Status

Affects: DSU
Fault Type: Programmer Category C
Fault Status: Present in r4p0. Fixed in r4p1.

Description

The EDPFR register is an external debug register that provides information about implemented PE features. When the DSU is used with a core that implements the Armv8.4-A architecture, the EDPFR.GIC field will indicate that the GICv4 system register interface is supported even when the GICv4.1 system register interface is supported.

Configurations Affected

The DSU is configured with a core that supports the Armv8.4-A architecture and the **GICCDISABLE** input pin is tied LOW.

Conditions

The external debugger reads the EDPFR register and uses the contents of the GIC field (bits [27:24]).

Implications

Arm does not expect the external debugger will need to use the contents of the GIC field. If it does, then it might incorrectly decide that GICv4.1 features are not supported by the core. The system register ID_AA64PFR0_EL1 is unaffected and provides the correct information about the GIC system register interface support implemented.

Workaround

No workaround is necessary.

2123467
No response to Debug APB access during a core reset, in Direct connect configuration

Status

Affects: DSU
Fault Type: Programmer Category C
Fault Status: Present in r0p0, r0p1, r0p2, r1p0, r2p0, r3p0, r4p0, and r4p1. Open.

Description

If there is traffic to a core on the Debug APB bus when the core is powered off, the access should receive a PSLVERR response. If the core reset is applied, then the APB bus will not provide a response, which can lead to a system deadlock.

Configurations Affected

This erratum only affects Direct connect configurations. It also requires the DebugBlock to be implemented in a separate power domain from the cluster.

Conditions

The erratum occurs under the following conditions:

1. The core is in the OFF power mode.
2. The system is asserting the **nCPUPORESET** core reset signal LOW.
3. The DebugBlock remains powered ON.
4. An access is made to the core on the Debug APB bus.

Implications

The **PREADYDC** and **PSLVERRDC** signals on the cluster APB interface are incorrectly driven LOW during reset, which means that any access in the interface will not receive a response. This can lead to a system deadlock.

Workaround

If the system and software can ensure that no APB accesses can be made while the core is powered off, then this will avoid this erratum.
If the system can assert the **nPRESET** signal to the DebugBlock whenever the core is powered off, then this will also avoid this erratum.

1219898
DSU might fail to detect ECC error

Status

Affects: DSU
Fault Type: Programmer Category C
Fault Status: Present in r0p0, r0p1, r0p2, r1p0, r2p0, and r3p0. Fixed in r4p0.

Description

If a core silently evicts a cache line and then a snoop request from the interconnect accesses that cache line, then the DSU might not detect an ECC error in the L3 tag RAM or snoop filter RAM.

Configurations Affected

This erratum only affects configurations where the DSU is connected to a coherent ACE interconnect and the DSU is configured with ECC by setting SCU_CACHE_PROTECTION to TRUE.

Conditions

1. A core performs a read of a cache line.
2. The core evicts the line from its L1 and L2 cache without notifying the DSU. This is referred to as a silent eviction.
3. The ACE interconnect sends a snoop transaction to the DSU for the same cache line.
4. The DSU reads the L3 tag RAM or snoop filter RAM for the snoop transaction.
5. The L3 tag RAM or snoop filter RAM contains an ECC error at the index accessed.
6. There is at least one other snoop transaction outstanding.

Implications

If these conditions are met, then in some cases the DSU might not detect or report the single-bit or double-bit ECC error. This might cause a loss of coherency or data corruption and can lead to deadlock.

There is still substantial benefit being gained from the ECC logic.
This erratum might cause a negligible increase in overall system failure rate.

One of the conditions required is a silent eviction from a core. The conditions and implications therefore also depend on the type of cores present:

- For Cortex-A75, silent evictions are possible when heavy memory traffic causes internal buffers to fill up.
- For all other types of cores, a silent eviction is only possible when some types of uncorrectable ECC errors are detected in the core. Therefore, the only implications for these cores are a negligible

increase in Detected Uncorrected Error (DUE) Failure In Time (FIT) rate.

Workaround

No workaround is required.

1314123
Incorrect ordering after change in cacheability

Status

Affects: DSU
Fault Type: Programmer Category C
Fault Status: Present in r0p0, r0p1, r0p2, r1p0, r2p0, r3p0, and r4p0. Open.

Description

If the memory type of an address region is changed from Cacheable to Non-cacheable, and then back again, and rare microarchitectural conditions occur, then stale data might be observed in a cache.

Configurations Affected

This erratum affects all configurations except Direct Connect configurations.

Conditions

1. An address region of memory is marked in the translation tables as Write-Back Cacheable memory.
2. The hardware prefetcher starts a data prefetch to an address within this region. This must generate a StashOnce CHI transaction from the core to the DSU, and in some cases the DSU might pass the StashOnce on to the interconnect if the DSU is configured with a CHI master.
3. The translation tables are updated to change the memory type to Non-cacheable or Device memory. This would involve a break-before-make sequence.
4. A sequence of cache clean and invalidate instructions are executed to ensure that any Cacheable data in the memory region does not remain in the caches.
5. The StashOnce transaction and the clean and invalidate transaction to the same address get reordered within the DSU or externally if the StashOnce was sent to the interconnect. This means that the StashOnce transaction can cause the line to be allocated into the cache after the cache maintenance has completed.
6. A core or other master in the system writes to the region that is now marked Non-cacheable or Device.
7. The translation tables are changed a second time, to mark the memory as Write-Back Cacheable again.
8. A load instruction is executed. The load might observe the stale data that was prefetched into the cache, rather than the Non-cacheable data that was written.

Implications

The above sequence is very specific and would typically take a very long time to execute. It requires that the StashOnce transaction is started before the translation table modification, yet does not complete until after both the translation table modification and the cache maintenance. Additionally, the StashOnce and cache maintenance transactions must be reordered by the DSU or interconnect, and this is an unlikely event, especially if they are not started at a similar time. Therefore the combination of these conditions is going to be extremely rare. Furthermore, the change in memory type implies a change of use of the memory, and many such changes of use will not require preservation of the data between uses.

Workaround

No workaround is necessary.

Note that this erratum is caused by a deficiency in the CHI architecture and will be corrected in CHI Issue D onward.

874812
Cluster ELA/CTI ROM table entries present when ELADISABLE is HIGH

Status

Affects: DSU
Fault Type: Programmer Category C
Fault Status: Present in r0p0, r0p1. Fixed in r0p2.

Description

The DSU supports an integrated ELA-500 component in the cluster. If the ELA is present but is disabled by the ELADISABLE pin, then reading the ROM table entries would incorrectly indicate that the ELA and associated cluster CTI are present.

Configurations Affected

This erratum only affects configurations of the DSU with the cluster ELA present.

Conditions

1. The ELADISABLE pin is HIGH.
2. A debug APB read is made to ROMENTRY0/ROMENTRY1 (when the LEGACY_V7_DEBUG_MAP configuration is FALSE) or ROMENTRY5/ROMENTRY6 (when the LEGACY_V7_DEBUG_MAP configuration is TRUE).

Implications

The ROM table will indicate that the ELA and associated CTI are present, but any attempted access to them will read as zero and ignore writes.

Workaround

Any discovery code must be written to be tolerant of these components not being found.

824788
Error record overflow field increments on incorrect event

Status

Affects: DSU
Fault Type: Programmer Category C
Fault Status: Present in r0p0, r0p1. Fixed in r1p0 and r0p2.

Description

The DSU contains a register field, ERR1STATUS.OF, that is set when the error record has overflowed with multiple errors. If the DSU detects multiple Deferred or Uncorrected errors, the DSU sets ERR1STATUS.OF to 1, which is correct. If the DSU detects multiple Corrected errors, the DSU should only increment the Corrected error count, ERR1MISC0.CECR or ERR1MISC0.CECO, but the DSU also sets the ERR1STATUS.OF to 1, which is incorrect. The DSU also fails to set the ERR1STATUS.OF when one of the Corrected error counters, ERR1MISC0.CECR or ERR1MISC0.CECO, overflows.

Configurations Affected

This erratum only affects configurations of the DSU with SCU_CACHE_PROTECTION enabled.

Conditions

The ERR1STATUS.OF becomes 1 incorrectly when:

1. The ERR1STATUS register indicates a valid entry (ERR1STATUS.V=0b1) and the relevant counter in ERR1MISC0 (ERR1MISC0.CECR or ERR1MISC0.CECO) is not at its maximum value (ERR1MISC0.CECR!=0xFF or ERR1MISC0.CECO!=0xFF).
2. A Corrected error is detected.

The DSU fails to set ERR1STATUS.OF to 1 either when:

1. The ERR1STATUS register is marked as invalid (ERR1STATUS.V=0b0) and the ERR1MISC0.CECR is at the maximum value (ERR1MISC0.CECR=0xFF).
2. A Corrected error is detected which matches ERR1MISC0.INDX and ERR1MISC0.WAY.

OR:

1. The ERR1STATUS register is marked as invalid (ERR1STATUS.V=0b0) and the ERR1MISC0.CECO is at the maximum value (ERR1MISC0.CECO=0xFF).
2. A Corrected error is detected which does not match ERR1MISC0.INDX and ERR1MISC0.WAY.

Implications

In the presence of multiple errors, the reporting of overflow can be inaccurate, which could lead to error handling software overestimating or underestimating the number of errors that have occurred. This could result in a negligible increase in the failure in time (FIT) rate.

Workaround

There is no workaround.

1299953
DSU might not report Uncontainable error on atomic instruction

Status

Affects: DSU
Fault Type: Programmer Category C
Fault Status: Present in r0p0, r0p1, r0p2, r1p0, r2p0, and r3p0. Fixed in r4p0.

Description

If the DSU receives read data from the interconnect where some but not all beats of the data indicate an error then, for certain types of atomic instruction, the DSU might not report the error.

Configurations Affected

This erratum affects all configurations except Direct Connect configurations. However if the system interconnect supports poisoning then it is unlikely to meet the other conditions required.

Conditions

1. A core executes an atomic store, atomic swap, or atomic compare instruction to Inner Write-Back, Outer Write-Back cacheable memory.
2. Either:
   - The DSU is configured with an ACE master port.
   - The DSU is configured with a CHI master port and the **BROADCASTATOMIC** input pin is LOW or the CLUSTERECTLR system register bit [7] is 1.
3. The DSU sends a 64-byte ReadUnique or ReadNoSnp transaction to the interconnect to fetch the data for the atomic instruction.
4. The interconnect returns data where the data needed by the atomic does not contain an error, but some of the other data beats in the same transaction indicate an error. On CHI, this means some data flits indicate DERR or NDERR. On ACE, this means some data transfers indicate SLVERR or DECERR.

Implications

If these conditions are met, then the DSU will discard the data from the interconnect, so data in the same cache line might be corrupted, potentially causing the loss of data previously written to that cache line. The atomic instruction will also not update memory. However, the destination register of the atomic instruction will be updated with the correct data.

The DSU will not record the Uncontainable error in the error record register, ERR1STATUS, or signal an error recovery interrupt (**nERRIRQ**) or fault handling interrupt (**nFAULTIRQ**). Also, the core executing the atomic instruction will not receive an External abort or System Error interrupt. This means that software will continue executing, unaware that memory has been corrupted.

This erratum cannot occur if the system does not return errors for only some but not all beats of data for cacheable read transactions. It is expected that this will be the case for many systems. Systems using a CHI interface and configured with ECC support would be expected to poison data that got an uncorrectable error rather than return a DERR or NDERR on only some of the beats of the transaction. These systems using poison would not be impacted by this erratum.

There is still substantial benefit being gained from the ECC logic, if configured.
In systems that meet the configurations described, this erratum might cause a negligible increase in overall system failure rate.

Workaround

No workaround is necessary.

1249448
Poison information might get lost in CHI.C direct connect configurations

Status

Affects: DSU
Fault Type: Programmer Category C
Fault Status: Present in r2p0 and r3p0. Fixed in r4p0.

Description

When the DSU is configured as CHI.C direct connect, the TraceTag information and the poison information on some parts of cache lines with uncorrectable ECC errors get lost when the data enters or leaves the core.

Configurations affected

This erratum only affects direct connect configurations with a core that has a CHI.C interface.

Conditions

Scenario 1
The TraceTag field is set in a snoop from the interconnect, and the snoop returns data.

Scenario 2

1. An uncorrectable ECC error is detected in any data cache in the system, either in the core or any other core or system cache.
2. This error causes the doubleword quantity to be marked as poisoned.
3. The error is in the fourth or eighth doubleword of the cache line.
4. The cache line is brought into the core as a linefill, or evicted from the core.

Implications

The TraceTag information is not propagated correctly, leading to reduced debug capabilities.

The poison information for the fourth and eighth doublewords of the cache line is incorrectly cleared, which can result in the erroneous data later being used without an abort being indicated.
There is still substantial benefit being gained from the ECC logic. This erratum might cause a small increase in overall system failure rate.
The detection of the errors within the core is still reported in the error record registers.

Workaround

There is no workaround.

792397
Reading some ROM table registers always returns 0 when v7 memory map is used

Status

Affects: DSU
Fault Type: Programmer Category C
Fault Status: Present in r0p0. Fixed in r0p1.

Description

Reading some ROM table registers in the legacy v7 memory map will return incorrect values.

Configurations Affected

This erratum only affects configurations with the legacy v7 debug memory map configuration option LEGACY_V7_DEBUG_MAP set to TRUE.

Conditions

A read is made on the debug APB interface to one of the following ROM table registers: PRIDR0, DEVARCH, DEVID, DEVTYPE, DBGPCR, or DBGPSR.

Implications

Reading these registers will return 0, which might lead to a debugger misidentifying the components.

Workaround

There is no workaround for this erratum.

787516
ECC errors in LTDB RAMs can cause spurious reports of correctable errors

Status

Affects: DSU
Fault Type: Programmer Category C
Fault Status: Present in r0p0. Fixed in r0p1.

Description

Under rare conditions, single and double-bit errors detected by the DSU in the LTDB RAMs can lead to spurious reports of correctable errors by setting the ERR1STATUS_EL1.OF flag incorrectly.

Configurations Affected

This erratum affects all configurations of the DSU with SCU_CACHE_PROTECTION enabled.

Conditions

1. The DSU transfers read data to a core in response to a core read request, or write data to the external ACE interface as a result of a cache eviction or streaming write using the LTDB RAMs.
2. A single or double-bit ECC error is detected on data read from the LTDB RAMs for the transfer, or the transfer carried poison from an earlier ECC error on any RAM in the system.
3. At the same time, the DSU transfers read data to a core in response to a core read request.

If these conditions are met, in addition to certain rare timing conditions, the DSU might set the ERR1STATUS_EL1.OF overflow flag when only a single error was detected.

Implications

There is still substantial benefit being gained from the ECC logic. The erratum only causes overly pessimistic error reporting.

Workaround

No workaround is required for the majority of systems. For designs where RAS is of significant importance and overly pessimistic error reporting is undesirable, this erratum can be worked around by setting bit [4] of CLUSTERACTLR_EL1. This will increase the latency of some transaction types and will have a small impact on performance.

774763
ECC errors in LTDB RAMs can cause data corruption and/or deadlock

Status

Affects: DSU
Fault Type: Programmer Category C
Fault Status: Present in r0p0. Fixed in r0p1.

Description

Under rare conditions, single and double-bit errors detected by the DSU in the LTDB RAMs can lead to data corruption and potentially deadlock.

Configurations Affected

This erratum affects all configurations of the DSU with SCU_CACHE_PROTECTION enabled.

Conditions

1. A core starts an Instruction-side linefill or a non-cacheable read of more than 128 bits.
2. The DSU transfers data to the core in response to the above request using the LTDB RAMs.
3. An ECC error is detected on data read from the LTDB RAMs for the transfer.
4. The same core starts a second linefill or a non-cacheable read (of any length).
5. The second linefill does not hit in the L3 cache, and completes before the first linefill data has been accepted by the core.

If these conditions are met, in addition to certain rare timing conditions, the DSU might cause data corruption and/or deadlock.

Implications

There is still substantial benefit being gained from the ECC logic. There might be a negligible increase in overall system failure rate because of this erratum.
The LTDB RAMs are very small, and might typically be implemented with more robust bitcells than larger RAMs. Therefore, the probability of an ECC error on these RAMs is significantly less than on other RAMs in the design.

Workaround

No workaround is required for the majority of systems. For designs where RAS is of significant importance, this erratum can be worked around by setting bit [4] of CLUSTERACTLR_EL1. This will increase the latency of some transaction types and will have a small impact on performance.

776914
CHAIN PMU event counts incorrectly

Status

Affects: DSU
Fault Type: Programmer Category C
Fault Status: Present in r0p0. Fixed in r0p1.

Description

The DSU provides a CHAIN PMU event for odd-numbered counters, allowing two 32-bit counters to be paired to provide a 64-bit counter. Because of this erratum, the CHAIN event might count incorrectly.

Configurations Affected

All configurations are affected.

Conditions

1. One of the odd-numbered PMU event counters is configured to count the CHAIN event.
2. The preceding even-numbered counter overflows.

If these conditions are met, the odd-numbered counter will increment every cycle until the overflow condition is cleared by writing to the CLUSTERPMOVSCLR_EL1 register.

Implications

When using a pair of counters to give a 64-bit count, the upper 32 bits of the counter value will be incorrect.

Workaround

No workaround is available.

766359
ERR1PFGCTLR might inject wrong fault type

Status

Affects: DSU
Fault Type: Programmer Category C
Fault Status: Present in r0p0. Fixed in r0p1.

Description

The ERR1PFGCTLR register provides a mechanism for software to generate faults in the DSU. Software controls the type of fault generated by setting different bits in the register.

When software programs the ERR1PFGCTLR to generate a Deferred Error (DE), the DSU might generate a DE or generate an Uncontainable Error (UC).

When software programs the ERR1PFGCTLR to generate an Unrecoverable Error (UEU), the DSU will generate an Uncontainable Error (UC).

Configurations Affected

This erratum affects all configurations of the DSU.

Conditions

The Error Pseudo Fault Generation Control Register must be programmed to generate DE or UEU errors:

1. ERR1PFGCTLR[5] must be set to 0b1 or ERR1PFGCTLR[2] must be set to 0b1.
2. ERR1PFGCTLR[31] must be set to 0b1.

Implications

Software that is testing the behavior of DE or UEU errors might see an unexpected UC error. Software might not expect the error type reported in the Error Record Primary Status Register, ERR1STATUS. The Uncontainable Error might have more severe consequences to the software and system than a DE or UEU.

Workaround

Software must not enable UEU injection as the DSU never generates UEU errors. Therefore ERR1PFGCTLR[2] must be set to 0b0.

There is no workaround to prevent DE generation sometimes causing UC errors.

2976798
Error record registers indicate pseudo-fault generation support in configurations without cache protection

Status

Affects: DSU
Fault Type: Programmer Category C
Fault Status: Present in r0p0, r0p1, r0p2, r1p0, r2p0, r3p0, r4p0 and r4p1. Open.

Description

Pseudo-fault generation is a mechanism that software can use to generate an entry in the RAS error record. This makes it possible to test how software would behave if a real fault was reported in the RAS error record registers.

In configurations without cache protection, the DSU does not support pseudo-fault generation, even though the RAS registers for pseudo-fault generation exist. The ERR1PFGFR register incorrectly indicates that pseudo-fault generation is supported by the DSU. The other DSU pseudo-fault generation registers, ERR1PFGCTLR and ERR1PFGCDNR, can be read and written, but will not generate a pseudo-fault in this configuration.

Configurations Affected

All non-Direct Connect configurations with the SCU_CACHE_PROTECTION parameter set to FALSE are affected.

Conditions

The incorrect behaviour of these registers always occurs in affected configurations.

Implications

In configurations without cache protection, software might incorrectly assume that pseudo-fault generation will work. This might lead to an unexpected error injection test result if a test attempts to inject an error but no error record is created.

Workaround

There is no workaround.

2832900
Interconnect bus errors during write back not recorded in RAS registers

Status

Fault Type: Programmer Category C
Fault Status: Present in r0p0, r0p1, r0p2, r1p0, r2p0, r3p0, r4p0, and r4p1. Open.

Description

When the DSU is writing back data to the system interconnect, errors from the interconnect might not be reported in the DSU RAS Error Record Registers.

Configurations Affected

This erratum affects all configurations of the DSU except Direct connect configurations.

Conditions

1. The DSU starts a WriteBackFull, WriteCleanFull, or cacheable WriteNoSnpFull transaction to the interconnect. This might be caused by an internally generated transaction, by a CPU transaction, or by an ACP transaction.
2. The interconnect returns an error response, indicating there has been an error during the transaction. For a CHI interconnect, the error response might be NDErr or DErr. For AXI or ACE interconnects, the error response might be SLVERR or DECERR.

Implications

The DSU will complete the transaction and will transfer the dirty data to the interconnect. The DSU RAS Error Record Registers are not updated to report the error from the interconnect. If the interconnect might lose the dirty data due to the error, the dirty data might be lost without this being reported in the DSU RAS registers.

The original cause of the error happened outside of the DSU, so this should have been logged by the component that detected the error. Therefore, the system should be able to detect the potential data loss.

Workaround

No workaround is necessary.