Arm® Corstone™ SSE-700

Software Developer Errata Notice

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.

Web address

http://www.arm.com/.

Feedback on this product

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

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

Feedback on this document

If you have comments on content then send an e-mail to errata@arm.com giving:

- The document title.
- The document number: SDEN-1684959.
- If applicable, the page number(s) to which your comments refer.
- A concise explanation of your comments.

Arm also welcomes general suggestions for additions and improvements.

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 on page 8 identifies errata that have been fixed in each product revision.

10-Mar-2021: Changes in document version 5.0				
ID	Status	Area	Cat	Summary of erratum
2080886	New	Programmer	CatB	System Generic Timer - CNTFRQ register in CNTBaseN and CNTCTLBase views inconsistent

13-Nov-2020: Changes in document version 4.0				
ID	Status	Area	Cat	Summary of erratum
1935033	New	Programmer	CatB	Incorrect data can be read from the System ID block

06-Jul-2020: Changes in document version 3.0				
ID	Status	Area	Cat	Summary of erratum
1809641	New	Programmer	CatC	Debug Access to Secure Enclave might get an error response after an nSRST reset request
1863466	New	Programmer	CatC	The Firewall mistakenly fault a transaction whose MasterID is programmed to more than one Master Permission Entry(MPE) in the default region and another non-default region

01-May-2020: Changes in document version 2.0				
ID	Status	Area	Cat	Summary of erratum
1704226	New	Programmer	CatB	Secure Enclave Base System Control HOST_SYS_RST_ST.RST_ACK might report the incorrect Host System Reset status
1755924	New	Programmer	CatB	Firewall always treats the region base address as being aligned to MNRS of a Firewall Component. However, the base address for regions under certain conditions must be aligned to its region size.
1767043	New	Programmer	CatB	IIDR_PRODUCT_ID default value is 0x749, not 0x000
1800078	New	Programmer	CatB	Incorrect transaction fault for unaligned accesses
1794453	New	Programmer	CatB (rare)	Unpredictable behavior caused by setting HOST_SYS_RST_CTRL.CPUWAIT to 0b0 during Host CPU power transition to OFF or OFF_EMU
1748180	New	Programmer	CatC	SSE-700 does not support power mode entry delay in PPUs for Cortex-A32 four CPUs and cluster

1748331	New	Programmer	CatC	Asserting DP ROM CDBGRSTREQ to reset DBGTOP could cause a debug deadlock if DP ROM CDBGPWRUPREQ0 is 0b1.
1795266	New	Programmer	CatC	Trace quad-core Cortex-A32 to AXI memory subsystem via Host ETR might be lost because of the limited trace bandwidth supported in SSE-700

17-Dec-2019: Changes in document version 1.0				
ID	Status	Area	Cat	Summary of erratum
1686226	New	Programmer	CatC	Firewall Controller could block accesses to certain Firewall Controller registers during shadow register initialization

Errata summary table

The errata associated with this product affect product versions as below.

ID	Cat	Summary	Found in versions	Fixed in version
1704226	CatB	Secure Enclave Base System Control HOST_SYS_RST_ST.RST_ACK might report the incorrect Host System Reset status	r0p0	r1p0
1755924	CatB	Firewall always treats the region base address as being aligned to MNRS of a Firewall Component. However, the base address for regions under certain conditions must be aligned to its region size.	r0p0	r1p0
1767043	CatB	IIDR_PRODUCT_ID default value is 0x749, not 0x000	r0p0	r1p0
1800078	CatB	Incorrect transaction fault for unaligned accesses	r0p0	r1p0
1935033	CatB	Incorrect data can be read from the System ID block	r1p0, r0p0	Open
2080886	CatB	System Generic Timer - CNTFRQ register in CNTBaseN and CNTCTLBase views inconsistent	r1p0, r0p0	Open
1794453	CatB (rare)	Unpredictable behavior caused by setting HOST_SYS_RST_CTRL.CPUWAIT to 0b0 during Host CPU power transition to OFF or OFF_EMU	r0p0	r1p0
1686226	CatC	Firewall Controller could block accesses to certain Firewall Controller registers during shadow register initialization	r0p0	r1p0
1748180	CatC	SSE-700 does not support power mode entry delay in PPUs for Cortex-A32 four CPUs and cluster	r0p0	r1p0
1748331	CatC	Asserting DP ROM CDBGRSTREQ to reset DBGTOP could cause a debug deadlock if DP ROM CDBGPWRUPREQ0 is 0b1.	r0p0	r1p0
1795266	CatC	Trace quad-core Cortex-A32 to AXI memory subsystem via Host ETR might be lost because of the limited trace bandwidth supported in SSE-700	r0p0	r1p0
1809641	CatC	Debug Access to Secure Enclave might get an error response after an nSRST reset request	r0p0	r1p0
1863466	CatC	The Firewall mistakenly fault a transaction whose MasterID is programmed to more than one Master Permission Entry(MPE) in the default region and another non-default region	r0p0	r1p0

Errata descriptions

Category A

There are no errata in this category.

Category A (rare)

There are no errata in this category.

Category B

1704226

Secure Enclave Base System Control HOST_SYS_RST_ST.RST_ACK might report the incorrect Host System Reset status

Status

Affects: SSE-700

Fault Type: Programmer Cat B

Fault Status: Present in r0p0. Fixed in r1p0

Description

If a higher priority reset request than Host System Reset is asserted, at the same time a Host System Reset is requested via Secure Enclave Base System Control HOST_SYS_RST_CTRL.RST_REQ.

This higher priority request is denied and de-asserted. SSE-700 should complete the sequence for the higher priority request and then perform the reset sequence for HOST_SYS_RST_REQ to either ACCEPT or DENY the request by setting the Secure Enclave Base System Control HOST_SYS_RST_ST.RST_ACK to `0b01` or `0b10`

As a result of this erratum, when the above scenario happens the HOST_SYS_RST_ST. RST_ACK is `0b01` then changed to `0b00`. The software might see `0b00` and does not know there is a pending Host System Reset. This might cause an issue in an application.

Configurations affected

This issue is present in all configurations of the SSE-700.

Conditions

1. A higher priority reset request than Host System Reset occurs and gets denied.
2. At the same time a Host System Reset via Secure Enclave Base System Control HOST_SYS_RST_CTRL.RST_REQ is requested.
3. The higher priority reset request is de-asserted.

Implication

SW reads `0b00` from Secure Enclave Base System Control HOST_SYS_RST_ST. RST_ACK and the reset is not serviced until the request is cleared at HOST_SYS_RST_ST.RST_REQ and requested again by software.

Workaround

Do not use Secure Enclave Base System Control HOST_SYS_RST_CTRL.RST_REQ to reset the Host System and External System. However, you can use SoC Reset Control (SOC_RST_CTRL.RST_REQ) to reset the entire SoC.

1755924

Firewall always treats the region base address as being aligned to MNRS of a Firewall Component. However, the base address for regions under certain conditions must be aligned to its region size

Status

Affects: SSE-700

Fault Type: Programmer Cat B

Fault Status: Present in r0p0. Fixed in r1p0

Description

When RSE.0 is configured or RSE.1 is configured for a component and MULnPO2 for a region is `0b0`, the Firewall Component should treat the base address of that region as being aligned to the size of that region regardless of what is programmed in the base address register.

When RSE.1 is implemented and MULnPO2 for a region is `0b1`, the Firewall Component treats the base and upper addresses as being aligned to MNRS of the Firewall Component.

The Firewall always treats the base and upper addresses as being aligned to MNRS. If the base address for a Firewall region is not properly programmed (aligned to its region size), under certain conditions, the Firewall could get the incorrect base address and mismatch a region.

Configurations affected

This issue is present in all configurations of the SSE-700.

Conditions

1. FWName_RSE_LVL =0
2. FWName_RSE_LVL =1 and RGN_SIZE(Region Size).MULnPO2 =0b0

FWName is one of the following Firewalls:

- XNVM
- CVM
- EXPMST0
- EXPMST1
- OCVM
- Secure Enclave

Implication

If the base address for a Firewall region is not aligned to its region size, the Firewall might get the incorrect base address and mismatch a region.

Workaround

Ensure that all regions are programmed such that the base address of each region is aligned to that region’s size.

1767043

IIDR_PRODUCT_ID default value is 0x749, not 0x000

Status

Affects: SSE-700

Fault Type: Programmer Cat B

Fault Status: Present in r0p0. Fixed in r1p0

Description

In SSE-700, the default value of System ID Implementer Identification Register (IIDR) PRODUCT_ID bits[31:20] is `0x749`. This is defined by the parameter IIDR_PRODUCT_ID in `$LOGICAL_PATH/top_sse700_r0_<CFG_NAME>/top_sse700_r0_aontop_<CFG_NAME>/verilog/top_sse700_r0_params.vh`.

IIDR_PRODUCT_ID default should not be `0x000`.

Configurations affected

This issue is present in all configurations of the SSE-700.

Conditions

SSE-700 Verilog is implemented.

Implication

Software gets the product ID `0x000` from System ID Implementer Identification Register PRODUCT_ID bits[31:20].

In future releases, the software will get the product ID `0x749` from System ID Implementer Identification Register PRODUCT_ID bits[31:20].

Workaround

Choose one of the following options:

- In `$LOGICAL_PATH/top_sse700_r0_<CFG_NAME>/top_sse700_r0_aontop_<CFG_NAME>/verilog/top_sse700_r0_params.vh`, set the default value of parameter IIDR_PRODUCT_ID to `0x749`.
- To get the product ID, software reads System ID Peripheral ID 0 and Peripheral ID 1 registers rather than IIDR[31:20]. The product ID on the SSE-700 is {PID1[3:0], PID0[7:0]}

  .

1800078

Incorrect transaction fault for unaligned accesses

Status

Affects: SSE-700

Fault Type: Programmer Cat B

Fault Status: Present in r0p0. Fixed in r1p0

Description

This affects accesses that have a starting address which is not aligned to the bus size. Unaligned accesses which are within (2<<**AxSIZE**)*(**AxLEN**+1) of the end of a region will be incorrectly treated as failing the permission checks of the firewall.

Configurations affected

This issue is present in all configurations of the SSE-700.

Conditions

A burst which is unaligned to the bus width is issued with an address which is within the final (2<<**AxSIZE**)*(**AxLEN**+1) of the region.

Implication

An access which should pass the permission checks of the Firewall is blocked and terminated by the firewall.

Workaround

Software can use one of the following workarounds:

1. Don't issue unaligned access to a Firewall Component.
2. When using unaligned burst make sure that the end address of the transaction is not within **AxSIZE** of the end of the region.

1935033

Incorrect data can be read from the System ID block

Status

Affects: CG066 - Corstone-700 Subsystem

Fault Type: Programmer Cat B

Fault Status: Present in r1p0 EAC, r0p0 LAC, r0p0 BET.

Description

The Corstone-700 Subsystem has the following read-only registers in the System ID block that identify the subsystem:

- Implementer Identification Register (IIDR)
- Peripheral ID registers (PID).

The following fields return incorrect data:

- IIDR.VARIANT and IIDR.REVISION fields indicate the major and minor revisions of the subsystem. The value read from this register incorrectly indicates major revision 0 and minor revision 1 (r0p1), but the correct value should indicate major revision 1 and minor revision 0 (r1p0). In LAC (r0p0) and BET (r0p0) these fields would have both read as 0, so this is not an issue.
- PID0.PART_0, PID1.PART_1, PID1.DES_0, PID2.DES_1 and PID4.DES_2 fields indicate the Product ID and the Implementer of the subsystem respectively. Configuring the IIDR_PRODUCT_ID or IIDR_IMPLEMENTER top-level parameters with non-default values does not set the proper values in these PID register fields.

Configurations affected

All configurations are affected.

Conditions

Software uses the System ID block's IIDR or PID registers to identify the subsystem.

Implications

Software might not be able to identify the subsystem or identifies it incorrectly.

Workaround

To identify the SoC that includes a specific instance of the Corstone-700 Subsystem, software should always use the SoC Identification (SOCID) register of the System ID block.

2080886

System Generic Timer - CNTFRQ register in CNTBaseN and CNTCTLBase views inconsistent

Status

Affects: CG066 - Corstone-700 Subsystem

Fault Type: Programmer Cat B

Fault Status: Present in r1p0 EAC, r0p0 LAC, r0p0 BET.

Description

The behavior of Generic Timer register CNTFRQ has been changed for Armv8-A.

In the current Armv7-A implementation, the register is visible in two frames CNTBaseN and CNTCTLBase, which are implemented as independent registers. In Armv8-A these registers are linked and reflect the same value.

Software that expects the Armv8-A behavior: writes the expected value to the CNTFRQ register in the CNTCTLBase frame and then expects this value to be reflected when the value is read from the CNTFRQ register in the CNTBaseN frame.

However, as these registers are independent in the Armv7-A implementation, the values are not reflected.

Configurations affected

All configurations are affected.

Conditions

1. Software writes a value to the CNTFRQ register through the CNTCTLBase frame
2. Software reads the CNTFRQ register through the CNTBaseN frame
3. The value of CNTFRQ read via the CNTBaseN frame does not reflect the value written via the CNTCTLBase frame as these are implemented as independent registers.

Implications

OS software might fail to boot due to inconsistencies in the CNTFRQ views.

Workaround

In the current Armv7-A implementation, although the CNTFRQ is normally 'Read-Only', for initial configuration it can be written through the CNTBaseN frame.

Therefore, software must write the required CNTFRQ value to both the CNTBaseN and CNTCTLBase frames.

This ensures consistency when reading the CNTFRQ value from either CNTBaseN or CNTCTLBase frames.

For example:

```
mmio_write_32(ARM_SYS_TIMCTL_BASE + CNTCTLBASE_CNTFRQ, freq_val);

mmio_write_32(ARM_SYS_CNT_BASE_NS + CNTBASEN_CNTFRQ, freq_val);
```

Category B (rare)

1794453

Unpredictable behavior caused by setting HOST_SYS_RST_CTRL.CPUWAIT to 0b0 during Host CPU power transition to OFF or OFF_EMU

Status

Affects: SSE-700

Fault Type: Programmer Cat B (Rare)

Fault Status: Present in r0p0. Fixed in r1p0

Description

Setting the HOST_SYS_RSTL_CTRL.CPU_WAIT to `0b0`, when a Host CPU core may be transitioning between the ON and OFF power modes, can lead to unpredictable behavior, including deadlocking the Host CPU core and wider SoC. This is caused by the Host CPU core reset being de-asserted and then asserted without the **STANDBYWFI** signal being driven to `0b1`.

Configurations affected

This issue is present in all configurations of the SSE-700.

Conditions

The following conditions must both be true:

- Core PPU is performing an ON to OFF or OFF_EMU power transition for a Host CPU core
- HOST_SYS_RST_CTRL.CPUWAIT bit is cleared during or just before the transition starts

Implication

What occurs at this point is unpredictable. It is possible that deadlock occurs for the Host CPU core or wider parts of the SoC.

Workaround

The Secure Enclave firmware must follow the following sequence after confirming the authenticity of the Host CPU firmware:

1. Set the policy of the CORE {0-3} PPUs to static ON.
2. Wait until all CORE{0-3} PPUs PPU_PWSR register indicates that the PPU is in static ON mode.

3. Set the HOST_SYS_RST_CTRL.CPUWAIT field to `0b0` and wait for each Host CPU core implemented to boot. Arm recommends that this is implemented using a message sent using the Host to Secure Enclave MHU. It can also be implemented using a shared memory location.
4. When all Host CPU cores have booted, the policy of the CORE {0-3} PPUs can be reprogrammed to its original value. Arm recommends this is set back to dynamic OFF.

This workaround requires that the Secure Enclave can access the CORE{0-3}
PPUs and this requires that the Host System Firewall is configured appropriately.

Category C

1686226

Firewall Controller could block accesses to certain Firewall Controller registers during shadow register initialization.

Status

Affects: SSE-700

Fault Type: Programmer Cat C

Fault Status: Present in: r0p0. Fixed in r1p0

Description

This erratum affects the Firewall Controller, which should allow accesses to FW_SR_CTRL, FC_CAP{0-3}, or FC_CFG{0-3}, and the Identification registers, when the Firewall Shadow registers are initializing.

As a result of this erratum, the accesses to Firewall Controller FW_SR_CTRL, FC_CAP{0-3} or FC_CFG{0-3} and Identification registers stall. With the maximum Firewall configuration, access could be stalled for up to 300 **REFCLK** cycles in the SSE-700.

Configurations affected

This issue is present in all configurations of the SSE-700.

Conditions

1. Access to the following registers are issued to the Firewall Controller:

- FW_SR_CTRL register
- FC_CAP{0-3} or FC_CFG{0-3} registers of all Firewall Components
- Identification registers of the Firewall Controller

2. The Firewall Shadow registers are initializing.

Implication

Accesses stall until the completion of Firewall Shadow registers initialization.

Workaround

None.

1748180

SSE-700 does not support power mode entry delay in PPUs for Cortex-A32 four CPUs and cluster

Status

Affects: SSE-700

Fault Type: Programmer Category C

Fault Status: Present in r0p0. Fixed in r1p0

Description

In SSE-700, the following PPUs do not support power mode entry delay:

- Cortex-A32 core 0
- Cortex-A32 core 1
- Cortex-A32 core 2
- Cortex-A32 core 3
- Cortex-A32 cluster

These 5 PPUs currently support the power mode entry delay and the Entry Delay Registers are inadvertently available. Software must not use the Power Mode Entry Delay Register 0 (PPU_EDTR0) and Power Mode Entry Delay Register 1 (PPU_EDTR1) of these PPUs.

Configurations affected

This issue is present in all configurations of the SSE-700.

Conditions

SSE-700 Verilog is implemented.

Implication

PPU_EDTR0 and PPU_EDTR1 fields in these 5 PPUs will be reserved in future SSE-700 revisions. They will be *Read As Zero, Write Ignored* (RAZ/WI).

Workaround

Do not use PPU_EDTR0 and PPU_EDTR1 in the 5 PPUs listed in this erratum.

1748331

Asserting DP ROM CDBGRSTREQ to reset DBGTOP could cause a debug deadlock if DP ROM CDBGPWRUPREQ0 is `0b1`

Status

Affects: SSE-700

Fault Type: Programmer Cat C

Fault Status: Present in r0p0. Fixed in r1p0

Description

SSE-700 should support DP ROM **CDBGRSTREQ** when DP ROM **CDBGPWRUPREQ0** is `0b1`.

Currently, DP ROM **CDBGRSTREQ** is always denied when DP ROM **CDBGPWRUPREQ0** is `0b1`.

Configurations affected

This issue is present in all configurations of the SSE-700.

Conditions

1. DP ROM **CDBGPWRUPREQ0** is `0b1`.

2. DP ROM **CDBGRSTREQ** is asserted.

Implication

If the DP ROM **CDBGRSTREQ** is not serviced, it could cause a debug deadlock.

Workaround

Deassert the DP ROM **CDBGPWRUPREQ0** before asserting the DP ROM **CDBGRSTREQ** to reset SSE-700 DBGTOP.

1795266

Trace quad-core Cortex-A32 to AXI memory subsystem via Host ETR might be lost because of the limited trace bandwidth supported in SSE-700

Status

Affects: SSE-700

Fault Type: Programmer Cat C

Fault Status: Present in r0p0. Fixed in r1p0

Description

In the worst case scenario, the 4 Cortex-A32 cores require 9 trace data bits per CPU cycle for 100% program trace without cycle counting. Typically, the trace data for a Cortex-A32 core is 2-3 bits per CPU cycle.

When tracing 4 Cortex-A32 cores to AXI memory via Host ETR, Corstone-700 can support 4.5 trace data bits when using the following conditions:

- 4 Cortex-A32 cores run at N MHz
- **DBGCLK** is N/2 MHz
- **ACLK** is N/2 MHz
  Where N is the frequency of the Cortex-A32 cores.

It is therefore possible for trace data to be lost or to cause back pressure to the CPU program execution depending on the configuration of the ETM within the Cortex-A32 core.

Configurations affected

This issue is present in all configurations of the SSE-700.

Conditions

SSE-700 Verilog is implemented.

Implication

Some trace packets are lost or program execution is halted while the trace system drains.

Workaround

A debugger can use one of the following workarounds:

- **DBGCLK** and **ACLK** must be set to a frequency high enough to support the trace bandwidth from the Cortex-A32 core.
- The Cortex-A32 ETM is configured to halt instruction execution when back pressure occurs on the trace infrastructure.

1809641

Debug Access to Secure Enclave might get an error response after an nSRST reset request

Status

Affects: SSE-700

Fault Type: Programmer Cat C

Fault Status: Present in r0p0. Fixed in r1p0

Description

After any of the following reset conditions:

- External Power on Reset
- Internal Power on Reset
- Debug Reset

If a debugger requests the DBGTOP and SECENCTOP power domains to enter the ON power mode, SSE-700 waits for the acknowledgement using the DP ROM and EXTDBG ROM tables before attempting an access to the Secure Enclave memory map. An error response can be generated to the access. This is caused by a race condition between the acknowledgement and the SECENCTOP power control logic enabling the bridge between the External Debug Bus and the Secure Enclave.

Configurations affected

This issue is present in all configurations of the SSE-700.

Conditions

All the following conditions are required:

- Any of the following reset conditions have been triggered:
    - External Power on Reset
    - Internal Power on Reset
    - Debug Reset
- DBGTOP and Secure Enclave are in OFF power mode.

Implication

An error response is returned to Debugger in response to the transaction.

Workaround

After any of the following reset conditions:

- External Power on Reset
- Internal Power on Reset
- Debug Reset

If a debugger receives an unexpected error for a a memory access to the Secure Enclave memory map, then it should re-issue the transaction.

1863466

The Firewall mistakenly fault a transaction whose MasterID is programmed to more than one Master Permission Entry(MPE) in the default region and another non-default region

Status

Affects: SSE-700

Fault Type: Programmer Cat C

Fault Status: Present in r0p0. Fixed in r1p0

Description

A transaction which has a MasterID that matches against two or more regions, where one of the regions is the default region (Region 0 in a Firewall Component which supports Protection Extension Level 2), generates a Programming Error when the default region has two or more enabled Master Permission Entries (MPE) with the same MasterID, even if the transaction has passed the protection logic checks using one of the other regions.

Configurations affected

This issue is present in all configurations of the SSE-700.

Conditions

- A Firewall Component which implements PE.2 and is not bypassed.
- Default region is enabled.
- Two or more enabled MPEs, in the default region, are configured with the same MasterID as another enabled MPE in another region X
- The transaction matches against region X.

Implication

For transactions issued to the following Firewalls which implement PE.2 in SSE-700:

- XNVM
- CVM
- DBG
- EXTSYS{0-1}
- EXPSLV{0-1}
- EXPMST{0-1}
- OCVM

The transaction incorrectly generates a Programming Error when a MasterID is programmed to more than one MPE in the default region and another non-default region, and the transaction matches against the non-default region.

Note:

EXPMST0 may be configured to support either PE.1 or PE.2. It is only impacted by this errata when it implements PE.2.

Workaround

Don't program the same MasterID to multiple MPE in default region of a Firewall.