

SmartFusion®2 Device Errata

Introduction

The following table lists the device specific errata and the affected SmartFusion2 devices. See [SmartFusion2 SoC FPGAs Data Security Devices Product Brief](#) for the die revision part marking specification.

Table 1. Summary of SmartFusion2 Devices Errata

Errata No.	Errata	Silicon Revisions														Software Errata
		M2S005		M2S010			M2S025		M2S060	M2S090			M2S150			
		0	1, 2	0	1, 2	3	0	1, 2	0	0	1, 2	3	0	1, 2		
1.1	1.1. VPP Must Be Set to 2.5V While Programming and Writing the eNVM at Industrial Temperatures Range	X	—	X	—	—	X	—	—	—	—	—	—	—	—	—
1.2	1.2. Over-Voltage Support on MSIOs During Flash*Freeze	X	—	X	—	—	X	—	—	—	—	—	—	—	—	—
1.3	1.3. Verification of the FPGA Fabric at Junction Temperatures Higher than 50°C Erroneously Indicates a failure	X	—	X	—	—	X	—	—	—	—	—	—	—	—	—
1.4	1.4. DDR_OUT and I/O-Reg Functional Errata Due to a Software Bug	—	—	—	—	—	—	—	—	—	—	—	—	—	—	X
1.5	1.5. Dedicated Differential I/O Driving the Reference Clock of the CCC May Cause a Functional Failure Due to a Software Bug	—	—	—	—	—	—	—	—	—	—	—	—	—	—	X
1.6	1.6. Power-Up Digest is Not Supported	X	—	X	—	—	X	—	—	—	X	—	—	X	—	—
1.7	1.7. Programming of the eNVM Must Only Occur as Part of a Bitstream also Containing the FPGA Fabric	—	—	—	—	—	—	—	—	—	—	—	—	—	—	X
1.8	1.8. Updating eNVM from the MSS or the FPGA Fabric Requires Changes of the FREQRNG Register	X	X	X	X	X	X	X	X	X	X	X	X	X	X	—
1.9	1.9. SYSCTRL_RESET_STATUS Macro is Not Supported	X	—	X	—	—	X	—	—	—	X	—	—	X	—	—
1.10	1.10. Zeroization is Not Supported	X	—	X	—	—	X	—	—	—	X	X	—	X	—	—
1.11	1.11. Arm® Cortex®-M3 Register Corruption Under Very Specific Literal Loads from eNVM and Cache Miss/Hit Sequences	—	—	—	—	—	—	—	—	—	—	—	—	—	—	X
1.12	1.12. The System Controller RC Oscillator Runs at 25 MHz After a Programming Recovery Operation	—	—	NS	X	—	—	—	—	—	NS	X	—	—	—	—

.....continued

Errata No.	Errata	Silicon Revisions												Software Errata	
		M2S005		M2S010			M2S025		M2S060	M2S090			M2S150		
		0	1, 2	0	1, 2	3	0	1, 2	0	0	1, 2	3	0		1, 2
1.13	1.13. ECC Point-Multiplication Service and ECC Point-Addition System Service are not Supported	—	—	—	—	—	—	—	—	X	—	—	X	—	—
1.14	1.14. Programming Silicon Requires Cortex-M3 Firmware Code	—	—	—	—	—	—	—	—	X	—	—	X	—	—
1.15	1.15. Programming of the FPGA Fabric Can Occur Only at Room Temperature	—	—	—	—	—	—	—	—	X	—	—	X	—	—
1.16	1.16. Programming of the eNVM Blocks needs to Occur Independent of the Fabric	—	—	—	—	—	—	—	—	X	—	—	X	—	—
1.17	1.17. PCIe Hot Reset Support Requires a Soft Reset Solution	—	—	X	X	X	X	X	X	X	X	X	X	X	—
1.18	1.18. Executing SRAM-PUF Services Fails While the Cortex-M3 Code is Executed from eNVM_1	—	—	—	—	—	—	—	—	X	X	X	X	X	—
1.19	1.19. After Successful Completion of 2-step IAP or CM3 ISP (without a SYSRESET), LSRAM Read and Write Access Fails from the Fabric Path	X	X	X	X	X	X	X	X	X	X	X	X	X	—
1.20	1.20. SRAM-PUF System Services May Take Two to Three Seconds to Complete	—	—	—	—	—	—	—	—	X	X	X	X	X	—
1.21	1.21. Disable Cortex-M3 While Programming eNVM Only	X	X	X	X	X	X	X	X	X	X	X	X	X	—
1.22	1.22. The I/Os State During Programming is Changed from Z to Weak Pull-Up	X	—	X	—	—	X	—	—	—	—	—	X	—	—
1.23	1.23. For S (security) Grade Devices, User Must not Enable Write Protection for Protected 4K Regions, Also Known as Special Sectors in the eNVM	X	X	X	X	X	X	X	X	X	X	X	X	X	—
1.24	1.24. Users Must Not Set Page Lock in eNVM0 for the 060 Device and eNVM1 for 090/150 Devices	—	—	—	—	—	—	—	X	X	X	X	X	X	—

Notes: In the preceding table,

- X indicates that the errata is available for that device and revision number.
- "—" indicates that errata is not available or the feature does not exist for that device and revision number.
- NS (Not Supported) indicates that the Programming Recovery Mode is not available in this revision.
- Software errata can be avoided by using Libero® SoC v11.4 SPI or later.
- Contact [Microchip SoC Technical Support](#) for any additional questions. To order a specific die, contact your local Microchip sales office.

Table 2. Revisions Released per Device

Silicon Devices	Revisions	Device Status
M2S005 (S)	Commercial/Industrial	Production
M2S010 (S, T, TS)	Commercial/Industrial	Production
M2S025 (T, TS)	Commercial/Industrial	Production
M2S060 (T, TS)	Commercial/Industrial	Production
M2S090 (T, TS)	Commercial/Industrial	Production
M2S150 (T, TS)	Commercial/Industrial	Production

Table of Contents

Introduction.....	1
1. Errata Descriptions and Solutions.....	6
1.1. VPP Must Be Set to 2.5V While Programming and Writing the eNVM at Industrial Temperatures Range	6
1.2. Over-Voltage Support on MSIOs During Flash*Freeze.....	6
1.3. Verification of the FPGA Fabric at Junction Temperatures Higher than 50°C Erroneously Indicates a failure.....	6
1.4. DDR_OUT and I/O-Reg Functional Errata Due to a Software Bug.....	6
1.5. Dedicated Differential I/O Driving the Reference Clock of the CCC May Cause a Functional Failure Due to a Software Bug.....	6
1.6. Power-Up Digest is Not Supported.....	7
1.7. Programming of the eNVM Must Only Occur as Part of a Bitstream also Containing the FPGA Fabric.....	7
1.8. Updating eNVM from the MSS or the FPGA Fabric Requires Changes of the FREQRNG Register.....	7
1.9. SYSCTRL_RESET_STATUS Macro is Not Supported.....	7
1.10. Zeroization is Not Supported.....	7
1.11. Arm® Cortex®-M3 Register Corruption Under Very Specific Literal Loads from eNVM and Cache Miss/Hit Sequences.....	7
1.12. The System Controller RC Oscillator Runs at 25 MHz After a Programming Recovery Operation.....	10
1.13. ECC Point-Multiplication Service and ECC Point-Addition System Service are not Supported	10
1.14. Programming Silicon Requires Cortex-M3 Firmware Code.....	10
1.15. Programming of the FPGA Fabric Can Occur Only at Room Temperature.....	10
1.16. Programming of the eNVM Blocks needs to Occur Independent of the Fabric.....	10
1.17. PCIe Hot Reset Support Requires a Soft Reset Solution.....	10
1.18. Executing SRAM-PUF Services Fails While the Cortex-M3 Code is Executed from eNVM_1..	11
1.19. After Successful Completion of 2-step IAP or CM3 ISP (without a SYSRESET), LSRAM Read and Write Access Fails from the Fabric Path.....	11
1.20. SRAM-PUF System Services May Take Two to Three Seconds to Complete.....	12
1.21. Disable Cortex-M3 While Programming eNVM Only.....	12
1.22. The I/Os State During Programming is Changed from Z to Weak Pull-Up.....	12
1.23. For S (security) Grade Devices, User Must not Enable Write Protection for Protected 4K Regions, Also Known as Special Sectors in the eNVM.....	12
1.24. Users Must Not Set Page Lock in eNVM0 for the 060 Device and eNVM1 for 090/150 Devices	12
2. Usage Guidelines for SmartFusion2 Devices.....	13
2.1. Programming Support.....	13
2.2. SHA-256 System Service.....	14
2.3. MSS Reset Mode.....	14
2.4. Accessing the PCIe Bridge Register in the High-Speed Serial Interface.....	14
3. Revision History.....	15

The Microchip Website.....	16
Product Change Notification Service.....	16
Customer Support.....	16
Microchip Devices Code Protection Feature.....	16
Legal Notice.....	17
Trademarks.....	17
Quality Management System.....	18
Worldwide Sales and Service.....	19

1. Errata Descriptions and Solutions

This section describes the Errata and solutions of SmartFusion2 device.

1.1 VPP Must Be Set to 2.5V While Programming and Writing the eNVM at Industrial Temperatures Range

VPP can be set to 2.5V or 3.3V. However, while writing or programming the eNVM of Revision 0 of the M2S005, M2S010, and M2S025 devices below 0°C, VPP must be set to 2.5V. See [DS0128: IGLOO2 and SmartFusion2 Datasheet](#) for VPP minimum and maximum settings.

Note: eNVM reading with VPP set to 3.3V or 2.5V operates as intended.

1.2 Over-Voltage Support on MSIOs During Flash*Freeze

When the input voltage is driven above the reference voltage for that bank, additional current can be consumed in the Flash*Freeze mode for Revision 0 of the following devices: M2S005, M2S010, and M2S025.

1.3 Verification of the FPGA Fabric at Junction Temperatures Higher than 50°C Erroneously Indicates a failure

In Revision 0: M2S005, M2S010, and M2S025 devices, standalone verification (STAPL VERIFY action) must be run at temperatures lower than 50 °C. If a VERIFY action is run at temperatures higher than 50 °C, a false verify failure may be reported.

Note: The Check Digest system services can be used to confirm design integrity at temperatures within the recommended operation conditions.

1.4 DDR_OUT and I/O-Reg Functional Errata Due to a Software Bug

This Errata only applies if you created or updated your design using Libero SoC v11.1 SP1 or v11.1 SP2. If you have one of the following in your design, the corresponding I/O will not function properly in the silicon due to the wrong software implementation of the I/O macro.

- If you use DDR_OUT macro in your design.
- If you combine an output or output enable register with an I/O using the PDC command `set_io <portName> -register yes`

Workaround

Both the Erratas are fixed in Libero SoC v11.1 SP3. Migrate your design to Libero SoC v11.1 SP3 or newer version, and re-run compile and layout.

1.5 Dedicated Differential I/O Driving the Reference Clock of the CCC May Cause a Functional Failure Due to a Software Bug

If your design has the dedicated differential I/O pair driving the reference clock of the CCC, the input clock may not propagate to CCC due to a software bug and the device will fail during silicon testing. There are several options to drive the ref clock of the CCC. One of the options is to drive from "Dedicated Input PAD x" (x = 0 to 3); this uses hardwired routing. In this option, choose single-ended I/O or differential I/O as the ref clock. This Errata exists when you choose the differential I/O option, meaning the dedicated differential I/O is used as CCC reference clock input. This Errata cannot be detected in any functional simulation and can only be detected in silicon testing.

Workaround

The Errata is fixed in the Libero SoC v11.1 SP3. Migrate your design to the Libero SoC v11.1 SP3 or newer version, and re-run compile and layout.

1.6 Power-Up Digest is Not Supported

Power-up digest is not supported in Revision 0 of the M2S005, M2S010, M2S025, M2S090, and M2S150 devices.

Workaround

Use NVM Data Integrity Check System service after the device is ON and check the data integrity.

1.7 Programming of the eNVM Must Only Occur as Part of a Bitstream also Containing the FPGA Fabric

The Bitstream Configuration Dialog Box in the Libero SoC allows programming eNVM and the FPGA fabric, separately. However, if using Libero v11.1 SP2 or an older version, program the eNVM along with the FPGA fabric for the M2S005, M2S010, M2S025, and M2S050 devices. The fabric can be programmed separately, if needed.

Workaround

The Errata is fixed in the Libero SoC v11.1 SP3. Migrate your design to the Libero SoC v11.1 SP3 or newer version, and re-run compile and layout.

1.8 Updating eNVM from the MSS or the FPGA Fabric Requires Changes of the FREQRNG Register

While updating the eNVM from the FPGA fabric, the NV_FREQRNG register must be changed from the default value 0x07 to 0x0F; eNVM reads are not affected. SmartFusion2 eNVM firmware driver v2.2 has been updated with the correct NV_FREQRNG settings. See Appendix B of [AC429](#) for more details on eNVM Read/Write Operation and eSRAM Read/Write Operations.

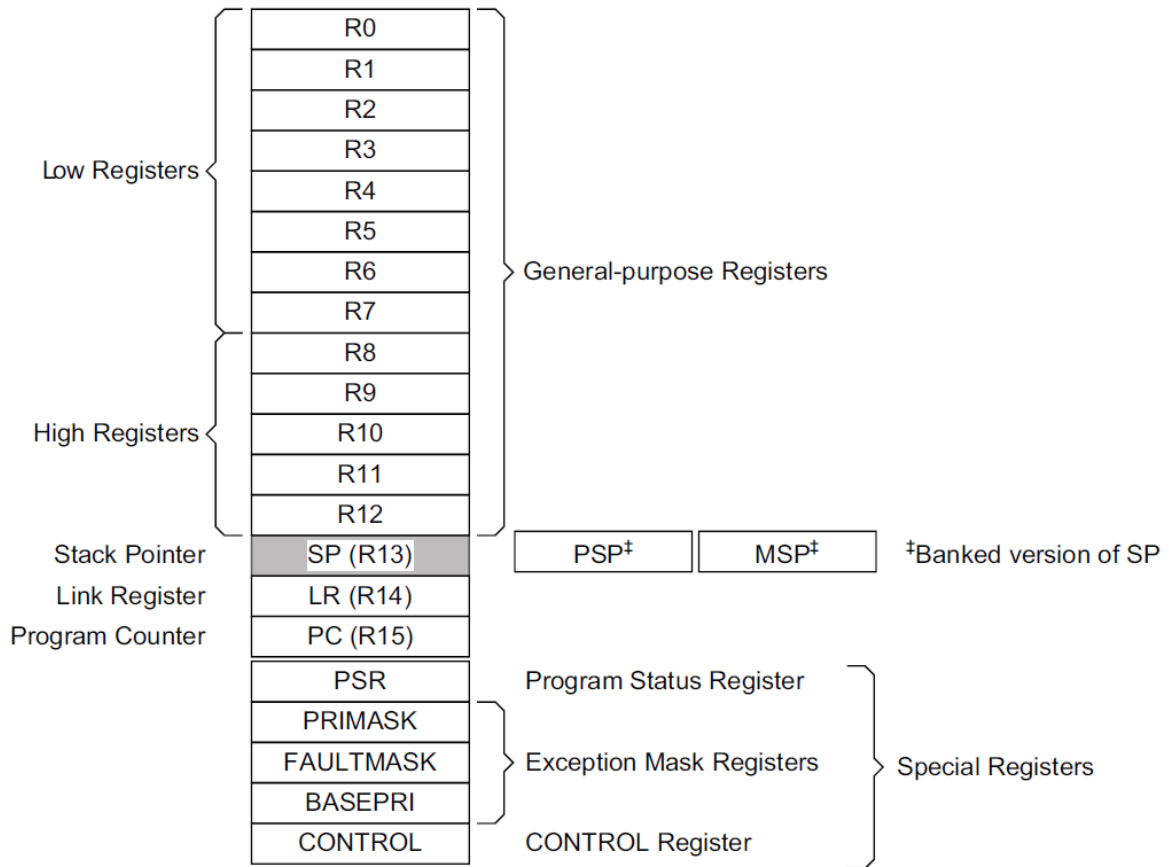
1.9 SYSCTRL_RESET_STATUS Macro is Not Supported

1.10 Zeroization is Not Supported

1.11 Arm® Cortex®-M3 Register Corruption Under Very Specific Literal Loads from eNVM and Cache Miss/Hit Sequences

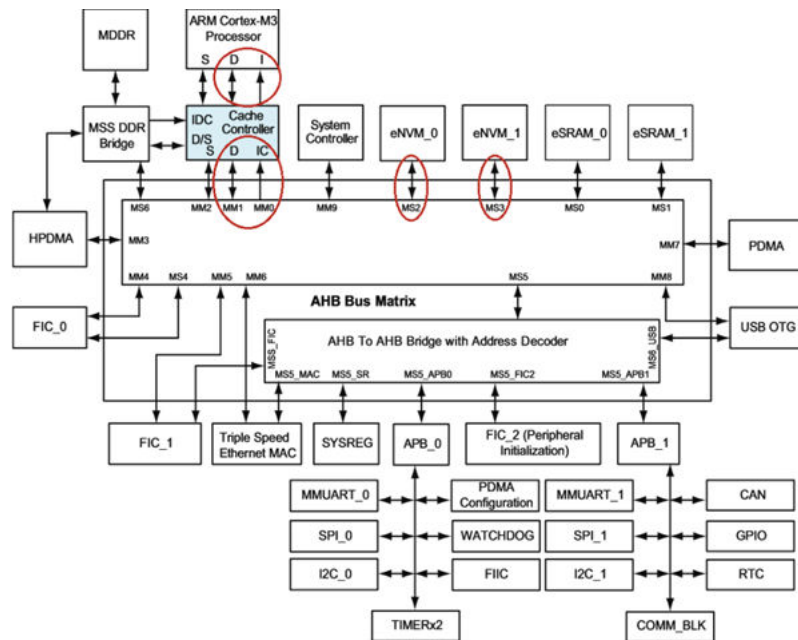
Cortex-M3 internal general-purpose registers (for example R6) gets corrupted when two nested D-Bus (must be a non-64-bit-aligned access) and I-Bus cache miss cycles occur in cache controller fetching from eNVM followed immediately by a D-Bus read without cache miss.

Figure 1-1. Cortex-M3 Core Register Set



SmartFusion2 system implements a cache controller in between Cortex-M3 and the memory subsystems (eNVM, eSRAM, Fabric sRAM, and DDR). An AHB matrix is used to arbitrate between eNVM, eSRAM, and Fabric sRAM access while a separate dedicated bus interfaces with DDR.

Figure 1-2. Cache Controller Interfaces and Paths Affected by CN (Red Circles)



SmartFusion2 Cache Controller allows mapping these memories, that is eNVM, on cacheable code regions. All M2S devices, apart from M2S050 (see [Microchip SmartFusion2 Microcontroller Subsystem User Guide \(UG0331\)](#)), come with a Cortex-M3 configuration that explicitly avoids simultaneous I-Bus and D-Bus address phases to ease arbitration of cache resource.

When the cache controller is enabled and mapped to eNVM, the following sequence of operations causes I-Bus and D-Bus accesses to be queued internally, leading to a state analogous to an I-Bus and D-Bus concurrent access.

1. A D-Bus miss has occurred to a non-aligned 64-bit address causing the cache controller to fetch the data from eNVM. This misaligned transaction extends the memory bus cycle.
2. While the cache logic is completing the cache fill operation after fetching from eNVM, an I-Bus miss occurs. The I-Bus operation is put on hold while waiting for cache filling operation to complete.
3. While I-Bus operation is in a wait state, a D-Bus read without a cache miss occurs. For this event to occur the D-Bus read must be within three cycles (the number of Cortex-M3 pipeline stages) to the I-Bus read/miss, a situation that mimics a simultaneous I-Bus and D-Bus read access.

A D-Bus read takes the precedence over an I-Bus but the data loaded into the Cortex-M3 internal register (for example, R6) is erroneously the I-Bus data which causes the corruption and consequently the application fails in an unpredictable manner.

Impact

The occurrence of this scenario described is rare. Moreover, the applications that meet any one of the four conditions listed are **not** impacted:

- The application executable has been 100% functionally tested across all supported operating conditions on every production unit and no such failures are observed.
- The cache controller is disabled in the design MSS configuration.
- The application is executed in any memory space other than eNVM.
- D-Bus literal loads are disabled during the compile of the code.

However, the corruption happens every time the specific cache miss/hit sequence occur regardless of the operating conditions or clock frequency.

Workaround

1. Add one the following compiling options depending on the toolchain used. This option prevents a D-Bus read to happen after I-Bus read. The following is a list of most common compilers used.

- Keil, `--no_integer_literal_pools` or similar options
- IAR, `--no_literal_pool`
- GCC-ARM, `-mpure-code`

2. Recompile the code and update the executable code on the boot medium.

If using SoftConsole, you might need to update the project to the v5.1 or newer version, since the `-mpure-code` option is available only in recent gcc-arm toolchains.

1.12 The System Controller RC Oscillator Runs at 25 MHz After a Programming Recovery Operation

After a programming recovery event, the system controller will be operating at 25 MHz. Ideally the system controller must operate at 50 MHz after a programming recovery event.

Workaround

If operating the system controller at 50 MHz is important to your design, contact soc_tech@microsemi.com.

1.13 ECC Point-Multiplication Service and ECC Point-Addition System Service are not Supported

1.14 Programming Silicon Requires Cortex-M3 Firmware Code

For the Revision 0 of the M2S090 and M2S150 devices, the eNVM needs to contain valid Cortex-M3 code. By default, SmartFusion2 parts are shipped with a default boot-up program stored at the eNVM address 0x60000000. If this default program is no longer valid or overwritten by the user, and there is no valid user boot code, the Cortex-M3 does not execute to a valid state. This leads to unexpected behavior including the programming lockout condition in Revision 0 of the M2S090 and M2S150 devices.

Workaround

The firmware code must be programmed into the eNVM prior to re-programming a commercial device. A while(1) statement will work. See *Knowledge Base (KB) SmartFusion2: Managing Cortex-M3*, while accessing MSS from fabric, when there is no default or valid boot code for Cortex-M3 to execute for details.

1.15 Programming of the FPGA Fabric Can Occur Only at Room Temperature

1.16 Programming of the eNVM Blocks needs to Occur Independent of the Fabric

Customer using Revision 0 of M2S090 or M2S150 devices must Program the eNVM block independently in Libero v11.6 or older. Contact Microchip SoC Technical Support, to program the eNVM block independently in Revision 0 of M2S090 and M2S150 devices using Libero v11.7.

1.17 PCIe Hot Reset Support Requires a Soft Reset Solution

On SmartFusion2 devices, a PCIe Hot Reset requires a soft FPGA logic reset scheme which clears the sticky bits of the PCI configuration space.

Workaround

On SmartFusion2 devices, a PCIe Hot Reset requires a soft FPGA logic reset scheme which clears the sticky bits of the PCI configuration space.

The application note [AN437 – Implementing PCIe Reset Sequence in SmartFusion2 and IGLOO2 Devices](#) describes the PCIe Hot Reset reset scheme. However, this reset scheme causes PCIe violations in some cases.

- For the M2S060/090T(S) devices there are no violations.
- For the M2S010/025/150T(S) devices at Gen1 rates there are no violations.
- For the M2S/025/150T(S) devices at Gen2 rates there are two PCIe CV violations.
 - Test case 1: TD_1_7 (Advanced Error Reporting Capability)
 - Test case 2: TD_1_41 (LinkCap2Control2Status2 Reg).

1.18 Executing SRAM-PUF Services Fails While the Cortex-M3 Code is Executed from eNVM_1

In the SmartFusion2 M2S090/M2S150 devices, the system controller does not release the eNVM1 access after executing the following SRAM-PUF system services:

- Create User AC (Activation Code) service
- Delete User AC service
- Create User KC for an Intrinsic Key service
- Create User KC for an Extrinsic Key service
- Delete User KC service

The above system services get executed successfully but the eNVM1 becomes inaccessible to Cortex-M3 and to fabric master.

- Any subsequent access to eNVM1 after this point, where eNVM1 is locked by System Controller, results in a stall, and a Power on Reset (POR) is needed to remove the stall.

Workaround

Execute “Get Number of the Key Code (GET_NUMBER_OF_KC)” SRAM-PUF system services immediately after the above services.

- The additional GET_NUMBER_OF_KC services releases the eNVM1 access from the System Controller.
- The firmware code for running SRAM-PUF services workaround must be executed from eNVM0, eSRAM, or DDR memories only, as Cortex-M3 does not get access to the eNVM1 that time.

1.19 After Successful Completion of 2-step IAP or CM3 ISP (without a SYSRESET), LSRAM Read and Write Access Fails from the Fabric Path

If LSRAM Read and Write access fails from the fabric path after performing 2-step IAP or CM3 ISP, perform a system reset or F*F Entry/Exit.

Workaround

The user application must execute System Reset as soon as the IAP/ISP system service is completed. Otherwise, user write and read accesses to LSRAM/uRAM is not possible. The System Reset can be generated using the tamper macro (available in the Libero SoC Catalog). Immediately after the IAP/ISP service, the user logic checks the LSRAM/uRAM access. If access is denied, the user logic sends the reset request/interrupt to the system controller through the tamper macro (by enabling the RESET function in the tamper macro configuration window) and then the system controller executes the system level reset. For more information, see [UG0451: IGLOO2 and SmartFusion2 Programming User Guide](#).

The following application notes have more information and design examples on how to implement the workaround:

- [SmartFusion2 SoC FPGA - In-System Programming Using USB OTG Controller Interface - Libero SoC v11.5 Demo Guide](#).
- [SmartFusion2 SoC FPGA - In-System Programming Using UART Interface Demo - Libero SoCv11.5 Demo Guide](#).
- [SmartFusion2 SoC FPGA In-Application Programming Using PCIe Interface - Libero SoC v11.5 Demo Guide](#).

1.20 SRAM-PUF System Services May Take Two to Three Seconds to Complete

This Errata is fixed in the newer date code devices, where SRAM-PUF system services will run faster. Contact soc_tech@microsemi.com for more information.

1.21 Disable Cortex-M3 While Programming eNVM Only

The user uses the Bitstream Configuration dialog box in the Libero SoC tool and generates an eNVM only stapl file. During programming, the system controller takes control of the eNVM block. If the user design has the application code running from the eNVM block, the Cortex-M3 processor halts as it cannot access the eNVM block. When the eNVM block programming is completed, the system controller releases the eNVM. The Cortex-M3 continues running from the same address from where it was halted at unless the device is re-started. If the device is not re-started, the Cortex-M3 behavior will be unpredictable as the eNVM is updated with the new code.

Workaround

- Use the M3_Reset_N signal to hold the Cortex-M3 processor in reset before programming the eNVM block.
- Force a device to re-start.
- Program eNVM and fabric. Libero v11.7 will fix the unpredictable behavior issue by forcing a re-start of the device after eNVM programming.

1.22 The I/Os State During Programming is Changed from Z to Weak Pull-Up

The I/O state during programming is changed from Z to weak pull-up in the latest die revisions. Affected die revisions (marked with "X" in [Table 1](#)) have I/Os that are tristated during programming.

1.23 For S (security) Grade Devices, User Must not Enable Write Protection for Protected 4K Regions, Also Known as Special Sectors in the eNVM

For S (security) devices, there are two or four 4 KB regions per eNVM array that can be protected for read and write, these regions are known as Protected 4K Regions or Special Sectors. If write protection is enabled for any of these regions, none of the locked pages inside the same eNVM block can be unlocked.

1.24 Users Must Not Set Page Lock in eNVM0 for the 060 Device and eNVM1 for 090/150 Devices

For 060, 090, and 150 device densities: Each eNVM memory block has a user page lock bit (see PAGE_LOCK_SET register) to lock a page and prevent accidental writing. After the page lock is set in eNVM0 for the 060 device or eNVM1 for 090/150 devices, the user will not be able to clear the lock for subsequent page updates later.

Workaround

To use page lock feature, the user can use eNVM0 of 090/150 device and set/clear page lock using the master (for example, M3 or fabric). There is no workaround for the 060 device. User must contact SoC tech support to unlock if they already used page lock in the 060 device.

2. Usage Guidelines for SmartFusion2 Devices

The following section details the usage guidelines for SmartFusion2 devices.

2.1 Programming Support

Table 2-1. Revision 0 Devices

Programming Mode	JTAG	SPI Slave	Auto Programming	Auto Update	2-Step IAP	Programming Recovery	M3 ISP
Programming Interface	JTAG	SPI_SC	SPI_0	SPI_0	SPI_0	SPI_0	N/A
M2S005(S)	Yes	Yes	No	No	No	No	Yes
M2S010 (S,T,TS)	Yes	Yes	No	No	No	No	Yes
M2S025 (T,TS)	Yes	Yes	No	No	No	No	Yes
M2S060 (T, TS)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
M2S090 (T,TS)	Yes	Yes	No	No	No	Yes ¹	Yes
M2S150 (T,TS)	Yes	Yes	No	No	No	No	Yes

Notes:

1. See Errata item [1.12. The System Controller RC Oscillator Runs at 25 MHz After a Programming Recovery Operation.](#)
2. Package dependencies that might not expose certain programming interfaces might be present. See the [PB0115: SmartFusion2 System-on-Chip FPGAs Product Brief](#) for device/package specific features.

Table 2-2. Revision 1 Devices

Programming Mode	JTAG	SPI Slave	Auto Programming	Auto Update	2-Step IAP	Programming Recovery	M3 ISP
Programming Interface	JTAG	SC_SPI	SPI_0	SPI_0	SPI_0	SPI_0	N/A
M2S005 (S)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
M2S010 (S,T,TS)	Yes	Yes	Yes	Yes	Yes	Yes ¹	Yes
M2S025 (T,TS)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
M2S090 (T,TS)	Yes	Yes	Yes	Yes	Yes	Yes ¹	Yes
M2S0150 (T,TS)	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Note: See Errata item [1.12. The System Controller RC Oscillator Runs at 25 MHz After a Programming Recovery Operation.](#)

Table 2-3. Revision 2 Devices

Programming Mode	JTAG	SPI Slave	Auto Programming	Auto Update	2-Step IAP	Programming Recovery	M3 ISP
Programming Interface	JTAG	SC_SPI	SPI_0	SPI_0	SPI_0	SPI_0	N/A
M2S005 (S)	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Usage Guidelines for SmartFusion2 Devices

.....continued

Programming Mode	JTAG	SPI Slave	Auto Programming	Auto Update	2-Step IAP	Programming Recovery	M3 ISP
M2S010 (S,T,TS)	Yes	Yes	Yes	Yes	Yes	Yes ¹	Yes
M2S025 (T,TS)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
M2S090 (T,TS)	Yes	Yes	Yes	Yes	Yes	Yes ¹	Yes
M2S150 (T,TS)	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Note: See Errata item [1.12. The System Controller RC Oscillator Runs at 25 MHz After a Programming Recovery Operation.](#)

Table 2-4. Revision 3 Devices

Programming Mode	JTAG	SPI Slave	Auto Programming	Auto Update	2-Step IAP	Programming Recovery	M3 ISP
Programming Interface	JTAG	SC_SPI	SPI_0	SPI_0	SPI_0	SPI_0	N/A
M2S010 (T, TS)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
M2S090 (T,TS)	Yes	Yes	Yes	Yes	Yes	Yes	Yes

2.2 SHA-256 System Service

Microchip recommends the message required to be on byte boundary when using SHA-256 System Service for the SmartFusion2 devices.

2.3 MSS Reset Mode

To keep the MSS in reset during normal operation, it is necessary to wait for the device to power up, and then apply the reset. The US_POR_B signal from the MSS (the power-on-reset for the FPGA fabric) can be used to check the device's powered up state.

2.4 Accessing the PCIe Bridge Register in the High-Speed Serial Interface

The PCIe Bridge registers must not be accessed before the PHY is ready. Wait for the PHY_READY signal (which indicates when PHY is ready) to be asserted before updating the PCIe Bridge registers.

The PHY_READY signal is normally asserted within 200 μ s after the device is powered up, so wait for 200 μ s before accessing the PCIe Bridge registers.

3. Revision History

Revision	Date	Description
A	10/2021	The following is the summary of changes in revision A: <ul style="list-style-type: none"> The document was updated to Microchip template. The document number was changed from 55900196 to DS80000978. Updated content in 1.11. Arm® Cortex®-M3 Register Corruption Under Very Specific Literal Loads from eNVM and Cache Miss/Hit Sequences section.
1.5	9/16	Updated text for item 1.11. Arm® Cortex®-M3 Register Corruption Under Very Specific Literal Loads from eNVM and Cache Miss/Hit Sequences .
1.4	7/16	Updated text for item 1.22. The I/Os State During Programming is Changed from Z to Weak Pull-Up .
1.3	4/16	Added Errata items 1.23. For S (security) Grade Devices, User Must not Enable Write Protection for Protected 4K Regions, Also Known as Special Sectors in the eNVM and 1.24. Users Must Not Set Page Lock in eNVM0 for the 060 Device and eNVM1 for 090/150 Devices .
1.2	12/15	The following items are added in revision 1.2 of this document: <ul style="list-style-type: none"> Updated Table 1 to include the M2S010 device in revision 3. Added errata items Disable Cortex-M3 when programming eNVM only and The I/Os state during programming is changed from Z to weak pull-up. Updated Table 2-4 to include the M2S010 (T, TS) device. Added solution for item 1.7. Programming of the eNVM Must Only Occur as Part of a Bitstream also Containing the FPGA Fabric.
1.1	5/15	Updated M2S060 revision from ES to revision 0.
1.0	5/15	The following items are added in revision 1.0 of this document: <ul style="list-style-type: none"> Combined M2S005, M2S010, M2S025, M2S060, M2S090, and M2S150 devices and die revisions to one centralized document. Created a separate Errata for the M2S050 device.

The Microchip Website

Microchip provides online support via our website at www.microchip.com/. This website is used to make files and information easily available to customers. Some of the content available includes:

- **Product Support** – Data sheets and errata, application notes and sample programs, design resources, user's guides and hardware support documents, latest software releases and archived software
- **General Technical Support** – Frequently Asked Questions (FAQs), technical support requests, online discussion groups, Microchip design partner program member listing
- **Business of Microchip** – Product selector and ordering guides, latest Microchip press releases, listing of seminars and events, listings of Microchip sales offices, distributors and factory representatives

Product Change Notification Service

Microchip's product change notification service helps keep customers current on Microchip products. Subscribers will receive email notification whenever there are changes, updates, revisions or errata related to a specified product family or development tool of interest.

To register, go to www.microchip.com/pcn and follow the registration instructions.

Customer Support

Users of Microchip products can receive assistance through several channels:

- Distributor or Representative
- Local Sales Office
- Embedded Solutions Engineer (ESE)
- Technical Support

Customers should contact their distributor, representative or ESE for support. Local sales offices are also available to help customers. A listing of sales offices and locations is included in this document.

Technical support is available through the website at: www.microchip.com/support

Microchip Devices Code Protection Feature

Note the following details of the code protection feature on Microchip devices:

- Microchip products meet the specifications contained in their particular Microchip Data Sheet.
- Microchip believes that its family of products is secure when used in the intended manner and under normal conditions.
- There are dishonest and possibly illegal methods being used in attempts to breach the code protection features of the Microchip devices. We believe that these methods require using the Microchip products in a manner outside the operating specifications contained in Microchip's Data Sheets. Attempts to breach these code protection features, most likely, cannot be accomplished without violating Microchip's intellectual property rights.
- Microchip is willing to work with any customer who is concerned about the integrity of its code.
- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of its code. Code protection does not mean that we are guaranteeing the product is "unbreakable." Code protection is constantly evolving. We at Microchip are committed to continuously improving the code protection features of our products. Attempts to break Microchip's code protection feature may be a violation of the Digital Millennium Copyright Act. If such acts allow unauthorized access to your software or other copyrighted work, you may have a right to sue for relief under that Act.

Legal Notice

Information contained in this publication is provided for the sole purpose of designing with and using Microchip products. Information regarding device applications and the like is provided only for your convenience and may be superseded by updates. It is your responsibility to ensure that your application meets with your specifications.

THIS INFORMATION IS PROVIDED BY MICROCHIP "AS IS". MICROCHIP MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WHETHER EXPRESS OR IMPLIED, WRITTEN OR ORAL, STATUTORY OR OTHERWISE, RELATED TO THE INFORMATION INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE OR WARRANTIES RELATED TO ITS CONDITION, QUALITY, OR PERFORMANCE.

IN NO EVENT WILL MICROCHIP BE LIABLE FOR ANY INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL OR CONSEQUENTIAL LOSS, DAMAGE, COST OR EXPENSE OF ANY KIND WHATSOEVER RELATED TO THE INFORMATION OR ITS USE, HOWEVER CAUSED, EVEN IF MICROCHIP HAS BEEN ADVISED OF THE POSSIBILITY OR THE DAMAGES ARE FORESEEABLE. TO THE FULLEST EXTENT ALLOWED BY LAW, MICROCHIP'S TOTAL LIABILITY ON ALL CLAIMS IN ANY WAY RELATED TO THE INFORMATION OR ITS USE WILL NOT EXCEED THE AMOUNT OF FEES, IF ANY, THAT YOU HAVE PAID DIRECTLY TO MICROCHIP FOR THE INFORMATION. Use of Microchip devices in life support and/or safety applications is entirely at the buyer's risk, and the buyer agrees to defend, indemnify and hold harmless Microchip from any and all damages, claims, suits, or expenses resulting from such use. No licenses are conveyed, implicitly or otherwise, under any Microchip intellectual property rights unless otherwise stated.

Trademarks

The Microchip name and logo, the Microchip logo, Adaptec, AnyRate, AVR, AVR logo, AVR Freaks, BesTime, BitCloud, chipKIT, chipKIT logo, CryptoMemory, CryptoRF, dsPIC, FlashFlex, flexPWR, HELDO, IGLOO, JukeBlox, KeeLoq, Klear, LANCheck, LinkMD, maXStylus, maXTouch, MediaLB, megaAVR, Microsemi, Microsemi logo, MOST, MOST logo, MPLAB, OptoLyzer, PackeTime, PIC, picoPower, PICSTART, PIC32 logo, PolarFire, Prochip Designer, QTouch, SAM-BA, SenGenuity, SpyNIC, SST, SST Logo, SuperFlash, Symmetricom, SyncServer, Tachyon, TimeSource, tinyAVR, UNI/O, Vectron, and XMEGA are registered trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

AgileSwitch, APT, ClockWorks, The Embedded Control Solutions Company, EtherSynch, FlashTec, Hyper Speed Control, HyperLight Load, IntelliMOS, Libero, motorBench, mTouch, Powermite 3, Precision Edge, ProASIC, ProASIC Plus, ProASIC Plus logo, Quiet-Wire, SmartFusion, SyncWorld, Temux, TimeCesium, TimeHub, TimePictra, TimeProvider, WinPath, and ZL are registered trademarks of Microchip Technology Incorporated in the U.S.A.

Adjacent Key Suppression, AKS, Analog-for-the-Digital Age, Any Capacitor, AnyIn, AnyOut, Augmented Switching, BlueSky, BodyCom, CodeGuard, CryptoAuthentication, CryptoAutomotive, CryptoCompanion, CryptoController, dsPICDEM, dsPICDEM.net, Dynamic Average Matching, DAM, ECAN, Espresso T1S, EtherGREEN, IdealBridge, In-Circuit Serial Programming, ICSP, INICnet, Intelligent Paralleling, Inter-Chip Connectivity, JitterBlocker, maxCrypto, maxView, memBrain, Mindi, MiWi, MPASM, MPF, MPLAB Certified logo, MPLIB, MPLINK, MultiTRAK, NetDetach, Omniscient Code Generation, PICDEM, PICDEM.net, PICKit, PICtail, PowerSmart, PureSilicon, QMatrix, REAL ICE, Ripple Blocker, RTAX, RTG4, SAM-ICE, Serial Quad I/O, simpleMAP, SimpliPHY, SmartBuffer, SMART-I.S., storClad, SQL, SuperSwitcher, SuperSwitcher II, Switchtec, SynchroPHY, Total Endurance, TSHARC, USBCheck, VariSense, VectorBlox, VeriPHY, ViewSpan, WiperLock, XpressConnect, and ZENA are trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

SQTP is a service mark of Microchip Technology Incorporated in the U.S.A.

The Adaptec logo, Frequency on Demand, Silicon Storage Technology, and Symmcom are registered trademarks of Microchip Technology Inc. in other countries.

GestIC is a registered trademark of Microchip Technology Germany II GmbH & Co. KG, a subsidiary of Microchip Technology Inc., in other countries.

All other trademarks mentioned herein are property of their respective companies.

© 2021, Microchip Technology Incorporated, Printed in the U.S.A., All Rights Reserved.

ISBN: 978-1-5224-9193-4

Quality Management System

For information regarding Microchip's Quality Management Systems, please visit www.microchip.com/quality.

Worldwide Sales and Service

AMERICAS	ASIA/PACIFIC	ASIA/PACIFIC	EUROPE
Corporate Office 2355 West Chandler Blvd. Chandler, AZ 85224-6199 Tel: 480-792-7200 Fax: 480-792-7277 Technical Support: www.microchip.com/support Web Address: www.microchip.com	Australia - Sydney Tel: 61-2-9868-6733 China - Beijing Tel: 86-10-8569-7000 China - Chengdu Tel: 86-28-8665-5511 China - Chongqing Tel: 86-23-8980-9588 China - Dongguan Tel: 86-769-8702-9880 China - Guangzhou Tel: 86-20-8755-8029 China - Hangzhou Tel: 86-571-8792-8115 China - Hong Kong SAR Tel: 852-2943-5100 China - Nanjing Tel: 86-25-8473-2460 China - Qingdao Tel: 86-532-8502-7355 China - Shanghai Tel: 86-21-3326-8000 China - Shenyang Tel: 86-24-2334-2829 China - Shenzhen Tel: 86-755-8864-2200 China - Suzhou Tel: 86-186-6233-1526 China - Wuhan Tel: 86-27-5980-5300 China - Xian Tel: 86-29-8833-7252 China - Xiamen Tel: 86-592-2388138 China - Zhuhai Tel: 86-756-3210040	India - Bangalore Tel: 91-80-3090-4444 India - New Delhi Tel: 91-11-4160-8631 India - Pune Tel: 91-20-4121-0141 Japan - Osaka Tel: 81-6-6152-7160 Japan - Tokyo Tel: 81-3-6880-3770 Korea - Daegu Tel: 82-53-744-4301 Korea - Seoul Tel: 82-2-554-7200 Malaysia - Kuala Lumpur Tel: 60-3-7651-7906 Malaysia - Penang Tel: 60-4-227-8870 Philippines - Manila Tel: 63-2-634-9065 Singapore Tel: 65-6334-8870 Taiwan - Hsin Chu Tel: 886-3-577-8366 Taiwan - Kaohsiung Tel: 886-7-213-7830 Taiwan - Taipei Tel: 886-2-2508-8600 Thailand - Bangkok Tel: 66-2-694-1351 Vietnam - Ho Chi Minh Tel: 84-28-5448-2100	Austria - Wels Tel: 43-7242-2244-39 Fax: 43-7242-2244-393 Denmark - Copenhagen Tel: 45-4485-5910 Fax: 45-4485-2829 Finland - Espoo Tel: 358-9-4520-820 France - Paris Tel: 33-1-69-53-63-20 Fax: 33-1-69-30-90-79 Germany - Garching Tel: 49-8931-9700 Germany - Haan Tel: 49-2129-3766400 Germany - Heilbronn Tel: 49-7131-72400 Germany - Karlsruhe Tel: 49-721-625370 Germany - Munich Tel: 49-89-627-144-0 Fax: 49-89-627-144-44 Germany - Rosenheim Tel: 49-8031-354-560 Israel - Ra'anana Tel: 972-9-744-7705 Italy - Milan Tel: 39-0331-742611 Fax: 39-0331-466781 Italy - Padova Tel: 39-049-7625286 Netherlands - Drunen Tel: 31-416-690399 Fax: 31-416-690340 Norway - Trondheim Tel: 47-72884388 Poland - Warsaw Tel: 48-22-3325737 Romania - Bucharest Tel: 40-21-407-87-50 Spain - Madrid Tel: 34-91-708-08-90 Fax: 34-91-708-08-91 Sweden - Gothenberg Tel: 46-31-704-60-40 Sweden - Stockholm Tel: 46-8-5090-4654 UK - Wokingham Tel: 44-118-921-5800 Fax: 44-118-921-5820