Application Note

AM263x Revision 1.1 to 1.3 Migration Guide

Abstract

This application note describes the differences between Texas Instruments' AM263x Revision 1.1 , Revision 1.2 (Not in Production) and Revision 1.3 microcontrollers to outline changes, improvements, and what needs to be considered when migrating from AM263x Rev 1.1 to AM263x Rev 1.3. Both hardware and software changes are covered for the purpose of application migration.

Table of Contents

1 Introduction 2
2 Feature Differences Between AM263x Rev 1.0, Rev 1.1, Rev 1.2, and Rev 1.3 3
2.1 Security Enhancements 3
2.2 Ethernet Subsystem Fixes 3
2.3 RAM SEC Fixes 5
3 Software Migration Recommendations 6
3.1 SBL-Related Fixes 6
3.2 TIFS-Related Changes 6
3.3 CPSW-Related Fixes 6
4 Board Changes 7
5 Silicon Version Identification 8
6 Summary 9
7 References 10

Trademarks

Sitara™ is a trademark of Texas Instruments.
All trademarks are the property of their respective owners.

Copyright © 2026 Texas Instruments Incorporated

1 Introduction

This application note serves as a comprehensive guide for customers working with Texas Instruments' AM263x microcontrollers who need to understand the differences between Revision 1.1 and Revision 1.3. The AM263x is part of TI's Sitara™ family of microcontrollers designed for industrial applications requiring robust connectivity, enhanced security features, and reliable performance.

The document outlines the key changes introduced in Revision 1.3, including security enhancements and fixes to the Ethernet subsystem.

Customers migrating from AM263x Rev 1.1 to Rev 1.3 can find detailed information on both hardware and software changes, along with specific recommendations for software migration to provide seamless transition between revisions. This guide is particularly valuable for applications that utilize the security features or Ethernet connectivity of the AM263x platform, as there are improvements in the latest revision.

By understanding these differences, customers can make informed decisions about silicon revision selection and software updates to take full advantage of the enhancements offered in AM263x Revision 1.3.

Copyright © 2026 Texas Instruments Incorporated

2 Feature Differences Between AM263x Rev 1.0, Rev 1.1, Rev 1.2, and Rev 1.3

2.1 Security Enhancements

Table 2-1 provides a feature-level comparison between the AM263x 1.0, AM263x 1.1, AM263x 1.2, and AM263x 1.3.

Table 2-1. Device Comparison (Security)

Sr. No.	Module	Feature Description	Silicon Version Support			
			AM263x 1.0A (B)	AM263x 1.1 (C)	AM263x 1.2 (D)(1)	AM263x 1.3 (E)
1	M4 ROM	i2403 - SBL redundant boot image feature support on HSSE devices	Present	Present	Fixed	Fixed

(1) This silicon version is not in production

2.1.1 SBL Redundant Boot Image Support on HSSE Devices

Redundant boot was not available on High-Security Security-Enabled (HSSE) devices in AM263x 1.1 (Please refer to i2403 errata).

Any corruption on the primary image at the following locations, SBL boot fails to boot from redundant flash region:

- Image corruption at middle of the certificate
- Image corruption at end of the certificate
- Image corruption at start of the sbl binary
- Image corruption at middle of the sbl binary
- Image corruption at end of the sbl binary

This erratum has been fixed in AM263x 1.2 and AM263x 1.3 to support redundant boot in case of failure in primary image

Software Impact: None

2.1.2 Root-Of-Trust (RoT) Switching Service with Dual Signed Certificate

Dual signed certificate is not supported in AM263x 1.1.

Feature enhancement in AM263x 1.2 and AM263x 1.3 : Root-Of-Trust(RoT) switching service with the authentication of dual signed certificate, that is, with the primary and backup keys supported in 1.2 and 1.3.

This is a feature enhancement and enables switching between SMPK and BMPK. Refer to the latest TIFS version for implementation details.

Software Impact: Yes

2.1.3 Application Decryption with the Original Symmetric Key

Application decryption with original key is not supported in Rev 1.1

Feature enhancement in AM263x 1.2 and AM263x 1.3 : TIFS can now support application decryption with the original symmetric key. Refer to the latest TIFS version for implementation details.

Software Impact: Yes

2.2 Ethernet Subsystem Fixes

Table 2-2 provides a list of known issues in AM263x 1.0 and AM263x 1.1 and fixes in AM263x 1.2, AM263x 1.3 with respect to the CPSW module. The full details for the errata items are provided in the AM263x Sitara™ Microcontroller Silicon Revision 1.0A, 1.1, 1.3 errata.

Copyright © 2026 Texas Instruments Incorporated

Table 2-2. Device Comparison (Ethernet)

Sr. No	Module	Issue Description	Silicon Version Affected			
			AM263x 1.0A (B)	AM263x 1.1(C)	AM263x 1.2 (D) (1)	AM263x 1.3(E)
1	CPSW	i2401 - Host Timestamps cause CPSW port to lock up	Present	Present	Fixed	Fixed
2	CPSW	i2402 - Ethernet to Host Checksum Offload does not work	Present	Present	Fixed	Fixed
3	CPSW	i2439 - Host to Ethernet Timestamp accuracy issue	Present	Present	Fixed	Fixed
4	CPSW	i2438 - CPSW: Host to Ethernet Checksum Generation with VLAN ADD/ Remove	Present	Present	Fixed	Fixed

(1) This silicon version is not in production

2.2.1 Host Timestamp Fix

Host timestamps caused the CPSW port to lock up (Errata i2401). When packet preamble was corrupted, timestamp requests can not be sent to CPTS, causing lockup in CPSW port FIFO.

This erratum is fixed in AM263x Rev 1.2 and AM263x Rev 1.3, allowing the timestamp option to be safely enabled.

Software Impact: Yes

CPTS Timestamp is now enabled by default in **AM26xx MCU+ SDK 26.01.00.08.LTS**.



Figure 2-1. Host Receive Timestamp Enable in Sysconfig

2.2.2 Ethernet to Host Checksum Offload

Ethernet to Host checksum enable had an issue that caused the CPSW to be sent into an unrecoverable error state (Errata i2402). Host to Ethernet checksum was not affected by the issue.

This erratum is fixed in 1.2 and 1.3, allowing Rx Checksum option to be safely enabled.

Software Impact: Yes

Host Rx Checksum offload is enabled by default in **AM26xx MCU+ SDK 26.01.00.08.LTS**.

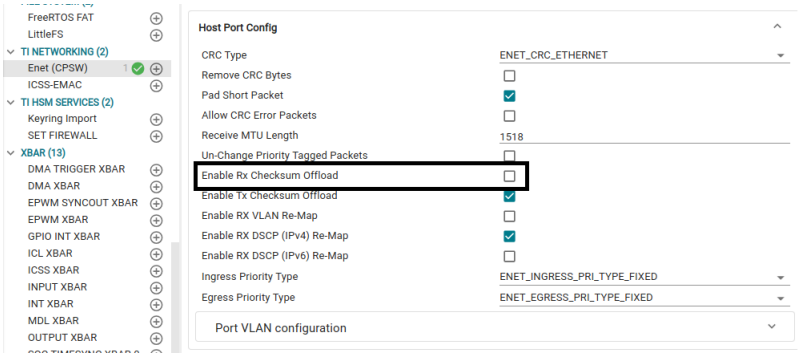


Figure 2-2. Rx Checksum Offload in Sysconfig

Copyright © 2026 Texas Instruments Incorporated

2.2.3 Host to Ethernet Timestamp Accuracy Issue

When a packet was sent from the Host to Ethernet with a timestamp to be generated on Ethernet egress, a packet length with 0xD5 in the lower eight bits resulted in a timestamp error (Errata i2439).

This erratum is fixed in AM263x Rev 1.2 and AM263x Rev 1.3

Software Impact: Yes

CPTS Timestamp is now enabled by default in **AM26xx MCU+ SDK 26.01.00.08.LTS**.



Figure 2-3. Host Receive Timestamp Enable in Sysconfig

2.3 RAM SEC Fixes

Table 2-3 provides a list of known issues in AM263x 1.0, AM263x 1.1 and fixes in AM263x 1.2, AM263x 1.3 with respect to RAM SEC module. Full details for the errata items are provided in the AM263x Sitara™ Microcontroller Silicon Revision 1.0A, 1.1 errata.

Table 2-3. Device Comparison

Sr. No.	Module	Issue Description	Silicon version affected			
			AM263x 1.0A (B)	AM263x 1.1 (C)	AM263x 1.2 (D) (1)	AM263x 1.3 (E)
1	RAM SEC	i2427- RAM SEC can cause Spurious RAM writes resulting in L2 and MBOX memory corruption	Present	Present	Present	Fixed
2	RAM SEC	i2499- Incorrect data returned to controller on single error detection during burst read	Present	Present	Present	Fixed

(1) This silicon version is not in production.

Software Impact : Yes

Copyright © 2026 Texas Instruments Incorporated

3 Software Migration Recommendations

3.1 SBL-Related Fixes

This change is transparent to software and require no code modifications.

3.2 TIFS-Related Changes

- **Root-of-Trust Switching**: With the changes to public key hash accessibility in Rev 1.3, TIFS now supports Root-of-Trust (RoT) switching service with the authentication of dual-signed certificates (with both primary and backup keys).
- **Application Decryption**: With the changes to symmetric key accessibility in Rev 1.3, TIFS can now support application decryption with the original symmetric key. Update to the latest TIFS version to leverage new capabilities for dual-signed certificates and original symmetric key access. Refer to the TIFS documentation for implementation details.

3.3 CPSW-Related Fixes

Update to the latest SDK version (AM26xx MCU+ SDK 26.01.00.08.LTS), which enables timestamp and checksum features by default. Existing applications disabling these features will continue to work without changes.

Copyright © 2026 Texas Instruments Incorporated

4 Board Changes

There are no board changes.

Copyright © 2026 Texas Instruments Incorporated

5 Silicon Version Identification

If software relies on silicon revision identification to enable or disable features, or to implement workarounds for known silicon errata, please note the following detection procedure.

The silicon version can be identified by reading bits [3:0] of TOP_CTRL: EFUSE_ROW_15, located at memory location 0x50D8 0434.

Note

The MCU+ SDK OTP Keywriter contains a PG_VER check. When switching to a new device revision, make sure the latest OTP Keywriter from the SDK is used for key programming.

Table 5-1. BIT FIELD DESCRIPTION OF TOP_CTRL:EFUSE_ROW_15

Reserved																										PG Version			
31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0

Table 5-2. IDENTIFYING PG_VERSION USING BITS[3:0] OF TOP_CTRL:EFUSE_ROW_15

PG VERSION	Device Revision	Description of Bits [3:0]
AM263 1.1	C	0011
AM263 1.2(1)	D	0100
AM263 1.3	E	0101

(1) This sample version is not in production

Copyright © 2026 Texas Instruments Incorporated

6 Summary

The transition from AM263x 1.1 to AM263x 1.3 brings significant improvements in device security and network functionality. Most fixes are transparent to software applications, requiring minimal changes for customers. We recommend updating to the latest SDK to take advantage of these improvements.

Copyright © 2026 Texas Instruments Incorporated

7 References

1. Texas Instruments, *AM263x Sitara™ Microcontroller Silicon Revision 1.0A, 1.1, 1.3*, errata

Copyright © 2026 Texas Instruments Incorporated

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATASHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES “AS IS” AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI products for your application, (2) designing, validating and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, regulatory or other requirements.

These resources are subject to change without notice. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you fully indemnify TI and its representatives against any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI’s products are provided subject to TI’s Terms of Sale, TI’s General Quality Guidelines, or other applicable terms available either on ti.com or provided in conjunction with such TI products. TI’s provision of these resources does not expand or otherwise alter TI’s applicable warranties or warranty disclaimers for TI products. Unless TI explicitly designates a product as custom or customer-specified, TI products are standard, catalog, general purpose devices.

TI objects to and rejects any additional or different terms you may propose.

Copyright © 2026, Texas Instruments Incorporated

Last updated 10/2025