MC-ISAR_AS422_TC3xx_1.30.0_Patch_4

Release Notes
Product name: MC-ISAR_AS422_TC3xx[1]
Release number: 1.30.0_Patch_4
Type of release: PATCH*
Release method: via Release Area
AUTOSAR specification: 4.2.2
Compiler support: Tasking 6.2r2p2, HighTec GNU 4.9.2.0
Processor platform: TC39xBA, TC39xBB, TC39xBC, TC38xAA, TC38xAB, TC38xAC, TC38xAD, TC37xEDAA, TC37xEDAB, TC37xAA and TC35xAA
Date: 2020-05-05
Patch Applicability: 1.30.0

* This patch has passed delta testing, but has not been subject to the full validation process for a production release. Customers must perform their own integration testing.

[1] Earlier known as MC_AURIX2G_SW_MCAL

1. Scope and purpose

This patch is to provide the fix for following issues:

Issue Id	0000053912-10661
Title	FEE internal variable not reset during cancel operation.

Issue Id	0000053912-10922
Title	Issues in word-line failure handling algorithm in certain scenario.

Issue Id	0000053912-10903
Title	Handling of Program verify error flag during QS hardening.

Issue Id	0000053912-10899
Title	Mishandling of the un-configured blocks during word-line failure scenario.

Issue Id	0000053912-10284
Title	Issue while performing Hardening check in certain scenario.

The patch is applicable to following package

Date of Release	**Package**
2019-10-24	MC-ISAR_AS42x_TC3xx_BASIC_1.30.0

2. Details of Issues Fixed

Issue Id	0000053912-10661
Title	FEE internal variable not reset during cancel operation.
Description	Due to an error in the software implementation of FEE driver, when a pending user write request is cancelled by Fee_Cancel()/ Fee_17_CancelAll() API, followed by either user write request or user read request and then followed by user write request, driver may write unintended data. API call sequences: Fee_Write() → Fee_Cancel() → Fee_Read() → Fee_Write() or Fee_Write() → Fee_Cancel() → Fee_Write()
Impact	In the scenario mentioned in the description, the data flash content may be corrupted leading to • Data loss of user blocks and/or • Trap (DAE/DSE)
Solution	Length variable used in write operation is reset to default whenever the user write request is accepted.

Issue Id	0000053912-10922
Title	Issues in word-line failure handling algorithm in certain scenario.
Description	Possibilities of Data blocks corruption leading to trap under certain scenarios while handling word-line failures during write operation.
Impact	Data flash content may be corrupted leading to data loss of user blocks and may result in a trap.
Solution	The last written block information is correctly updated in the case of word-line failure when the last written block is spanning across the word-line.

Issue Id	0000053912-10903
Title	Handling of Program verify error flag during QS hardening.
Description	Occurrence of Program verify error during QS hardening results in a word-line skip for the write operation of the block, which triggered GC.
Impact	Unintended word-line skips resulting in unusable word-lines until next GC happens.
Solution	Program verify error flag detected during QS hardening is cleared after completing QS hardening.

Issue Id	0000053912-10899
Title	Mishandling of the un-configured blocks during word-line failure scenario.

Description	Un-configured blocks management while handling word-line failures during write operation may result in out of bound array access.
Impact	During the mentioned scenario, if out of bound array happens to be in a reserved memory area, it results in a trap.
Solution	Implementation error while traversing through the un-configured blocks is corrected.

Issue Id	0000053912-10284
Title	Issue while performing Hardening check in certain scenario.
Description	As part of FEE double sector algorithm garbage collection (GC) happens. During GC, erase operation could weaken the data in QS region because of the ‘erase disturbs’. In order to secure the QS data, FEE driver performs check and hardening periodically. Due to an error in the software implementation of FEE driver, hardening check is not performed for all pages. This issue is observed only when user configures both NVM and QS data blocks
Impact	This may result in not performing the hardening operation for a page where hardening is actually required and thereby leading to data loss in the QS region
Solution	Implementation error while scanning through the pages during Hardening check is corrected.

3. Contents of 1.30.0_Patch_4

Package for Patch 1.30.0_Patch_4 (`MC-ISAR_AS422_TC3xx_1.30.0_Patch_4.zip`) contains:

1. Releasenote_MC-ISAR_AS422_TC3xx_1.30.0_Patch_4.pdf
2. Folder `MC-ISAR_AS422_TC3xx_1.30.0_Patch_4\patched_files` contains

Module	File	Purpose
Fee	Fee.c	Issues fixed and SW patch version is updated to 10.30.21
	plugin.xml	SW patch version is updated to 10.30.21
	Fee.bmd (for all supported processor platform)	SW patch version is updated to 10.30.21
	Fee.xdm	SW patch version is updated to 10.30.21
	Fee_Bswmd.arxml	SW patch version is updated to 10.30.21
	CRYPTOMANIFEST.MF	Crypto Signature files for plugins
	CRYPTOMANIFESTSIG.MF	

4. Steps to use 1.30.0_Patch_4

1. Ensure that `MC-ISAR_AS42x_TC3xx_BASIC_1.30.0` BASE package is installed.
2. Extract `MC-ISAR_AS422_TC3xx_1.30.0_Patch_4.zip`
3. Replace files present in BASE packages from the files present under `MC-ISAR_AS422_TC3xx_1.30.0_Patch_4\patched_files`.
   Please see following example for replacing files:

```
xcopy /F /E /Y <PATCH EXTRACTED PATH>\patched_files <BASE PACKAGE INSTALLED PATH>\MC-ISAR_AS42x_TC3xx_BASIC_1.30.0\
```

4. Clean and build the release package. (Refer TC3xx_SW_MCAL_UM_Basic.pdf for details)

Trademarks
All referenced product or service names and trademarks are the property of their respective owners.

Published by

Infineon Technologies AG

81726 München, Germany

Edition 2020-05-05

Do you have a question about this document?

Email: erratum@infineon.com

Document reference

IFX-sbp1571723956889

IMPORTANT NOTICE

The information given in this document shall in no event be regarded as a guarantee of conditions or characteristics (“Beschaffenheitsgarantie”) .

With respect to any examples, hints or any typical values stated herein and/or any information regarding the application of the product, Infineon Technologies hereby disclaims any and all warranties and liabilities of any kind, including without limitation warranties of non-infringement of intellectual property rights of any third party.

In addition, any information given in this document is subject to customer’s compliance with its obligations stated in this document and any applicable legal requirements, norms and standards concerning customer’s products and any use of the product of Infineon Technologies in customer’s applications.

The data contained in this document is exclusively intended for technically trained staff. It is the responsibility of customer’s technical departments to evaluate the suitability of the product for the intended application and the completeness of the product information given in this document with respect to such application.

For further information on the product, technology delivery terms and conditions and prices please contact your nearest Infineon Technologies office (**www.infineon.com**).

WARNINGS

Due to technical requirements products may contain dangerous substances. For information on the types in question please contact your nearest Infineon Technologies office.

Except as otherwise explicitly approved by Infineon Technologies in a written document signed by authorized representatives of Infineon Technologies, Infineon Technologies’ products may not be used in any applications where a failure of the product or any consequences of the use thereof can reasonably be expected to result in personal injury.