STSECTOOLFUSE Driver

RELEASE NOTES

CONFIDENTIAL

1 Introduction

This document details the changes made to the STSECTOOLFUSE driver. The related API document is DVD-API-351.

Build details: 1.7.3
Driver Version: 1.7.3

Driver Version	Release Date	Description
1.00.00	12/01/2007	First release. 7109 only.
1.00.01	17/01/2007	Corrected some documentation errors.
1.00.02	18/01/2007	Corrected some documentation errors. Added appendix C.
1.00.03	26/02/2007	Added new functions to utility. Added mtp_locka bit fuses. Fixed bug when writing to bulk data.
1.00.04	09/03/2007	Fixed BRIsec00496 - Decimal printed instead of hex Fixed BRIsec00497 - Instructions for keyed part Fixed BRIsec00509 - crypt_sigchk_enable fuse issue
1.01.00	08/05/2007	Fixed BRIsec00524 - Error response for BulkWriteItem now 'bad param' ST7200 build added.
1.01.01	08/05/2007	Added STSECTOOLFUSE_ReadSysRegItem and STSECTOOLFUSE_ReadMtpItem functions.
1.01.02	10/05/2007	Added information about utility builds in utility build documents. Added more 7200 fuses.
1.01.03	24/05/2007	Added SAF locations to fuse value list.
1.01.04	27/09/2007	Compilation with toolset st40r2-3.1.1 for 7109 only.
1.01.05	27/09/2007	Fixed write error with t1f_secure_filt_bypass_enable on 7200. Compilation with toolset st40r2-4.0.2 for 7109 and 7200.
		Fixed BRIsec00704 - MTP details for STSECTOOLFUSE_TKDMA_ESTAR_CW_SECURE_OTP_ITEM and STSECTOOLFUSE_TKDMA_NDS_VGS_ENABLE_OTP_ITEM have been swapped.
1.2.0	11/02/2008	Added support for 5167
1.2.1	15/02/2008	Added STSECTOOLFUSE_ALL_OTP_ITEM item for 5167. Built against STCOMMON 2.1.3. Added OTP Application note document

Driver Version	Release Date	Description
1.2.2	25/03/2008	Fixed issue: Unable to set boot rom enable fuse on 5167
1.2.3	21/04/2008	Fixed BRIsec00899 - Added HowToExecuteUtility.txt. Renamed ST40 utilitie executables to use .out suffix.
1.2.4	13/06/2008	Fixed issue about the otp appnote not appearing in the release's zip files for 7109.
1.3.0	07/08/2008	Added support for 7105 and 7111 for OS21.
1.3.1	08/09/2008	Updated fuse list for 7105 and 7111.
1.3.2	17/11/2008	Added true 32-bit support to all OS21 builds. Added support for 7141, 7200 (cut 2) for OS21. Added library support for STLinux 2.2/2.3 on 7109, 7105, 7111, 7141, 7200 (cut 2). Deprecated support for 7200 cut 1.
1.3.3	03/12/2008	Minor update to fuse definitions.
1.3.4	05/12/2008	Added 7111 cut2 release, as distinct from 7111 cut 1 `STSECTOOLFUSE_CW_SECURE_OTP_ITEM` now has R/W access on 7111 cut 2 Renamed `STSECTOOLFUSE_CW_AV_ENABLE_OTP_ITEM` to `STSECTOOLFUSE_CW_ENABLE_OTP_ITEM`
1.3.5	05/01/2009	Fixed bug in Linux ioctl driver code regarding STSECTOOLFUSE_BulkReadItem and STSECTOOLFUSE_BulkWriteItem functions.
1.4.0	17/03/2009	Added 5197 support (read only) Ported to Stapler (version 1.1.0 and above)
1.4.1	31/03/2009	Fixed 5197 write (Note does not work over JTag)
1.4.2	14/05/2009	Updated 5197 write (auto retry write upon failure)
1.4.3	29/06/2009	Updated 7105 to support cut3.0, distinct form 7105 cut 1.0 and 2.0
1.4.4	11/08/2009	Fixed bug BRISec1638 - Set correct R/W mode for STSECTOOLFUSE_TRANS_CW_SECURE_OTP_ITEM. Fixed bug BRISec1634 - 7141 cut >=2 support added for fuse STSECTOOLFUSE_TRANS_CW_SECURE_OTP_ITEM 7109 gcc version 3.x support dropped, due to dependencies (bug BRISec1637)
1.4.5	09/09/2009	Fixed BRISec 1712 - jtag_protect has incorrect address.
1.4.6	30/09/2009	Fixed bug BRISec1732 - Bulk32 write fails.

CONFIDENTIAL

Driver Version	Release Date	Description
1.4.7	14/10/2009	Fixed bug BRISec1794 - STSECTOOLFUSE 7141 c2 utility includes 7141 c1 fuse definitions file Fixed feature request BRISec1792 - Added additional fuses to 7141 c2 fuse definitions to meet customer requirements
1.4.8	21/10/2009	Implemented request BRISec1797 - Added STSECTOOLFUSE_DIRT_DISABLE fuse item for 5197 Fixed re-opened bug BRISec1792 since some 7141 c2 fuse addresses for new fuses in 1.4.7 were incorrect
1.4.9	23/10/2009	Fix for bug BRISec1808 - Add PCI disable fuse for customer.
1.4.10	11/11/2009	Added uclibc support to Linux release
1.5.0	12/01/10	Added support for STi5206/ STi5289. Added stsectoolfuse_utility_readme.txt, describing how to examine and blow fuses using the utility. The following API functions have been deprecated - there functionality is performed internally. The functions remain to allow backwards-compatibility but will cause compilation warnings: STSECTOOLFUSE_StartOTP STSECTOOLFUSE_StopOTP STSECTOOLFUSE_PermanentWriteEnable STSECTOOLFUSE_PermanentWriteDisable STSECTOOLFUSE_Identity STSECTOOLFUSE_ReadMtpItem STSECTOOLFUSE_ReadSysRegItem Document examples and fuse list appendices updated.
1.6.0	11/03/10	Added support for 5197 cut 3 (BRIse002122)
1.6.1	15/04/10	Fixed : BRIsec002197 [5289/5206 SIgnature checking cannot be enabled] BRIsec002173[Support for 5197 cut 3.x omitted from release list] BRIsec002168 [STSECTOOLFUSE update to new build system] BRIsec002196 [7141 c.2.2 fuses not supported] BRIsec002168 [STSECTOOLFUSE update to new build system] BRIsec002155 [Minor doc errors]

CONFIDENTIAL

Driver Version	Release Date	Description
1.6.2	20/05/10	Fixed: BRIsec2273 - Updated 5197/5167 swaf timing and reset sequence BRIsec2293 - Re-introduced 5167 support BRIsec2232 - 5197 cut 3 VCC size change BRIsec2349 - Reduce Safmem programming delay
1.6.3	26/05/10	Added 5206 Linux support Fixed: BRIsec2242 - 5206 crypto_enable missing
1.7.0	23/08/10	BRIsec2502 - Added device multi-cut support Increased code maintainability index
1.7.1	29/09/10	BRIsec2573 - Added crypt_fw_version_ctrl fuse on 5206 and 7141 platforms
1.7.2	28/10/10	Fixed BRIsec2620 - Error in ioctl code forces BulkWrite operation instead of BulkRead
1.7.3	31/01/11	BRIsec2602: 5289: Add trans_cp_secure and trans_cpcw_sec_polarity BRIsec2710: [STSECTOOLFUSE] _BulkWriteItem() should return error for locked fuse

1.1 List of supported SoCs

SoC	OS20	OS21		LINUX	
		29-bit	32-bit	29-bit	32-bit
5167	X				
5197		X	X	X	X
7109 cut2.0 and above		X	X	X	X
7111 cut 2.0 and above		X	X	X	X
7105 cut 3.0 and above		X	X	X	X
7141 cut 2.0 and above		X	X	X	X

Table 1 SoC and OS support on STSECTOOLFUSE 1.7.3

CONFIDENTIAL

SoC	OS20	OS21		LINUX	
		29-bit	32-bit	29-bit	32-bit
5206		X	X	X	X

Table 1 SoC and OS support on STSECTOOLFUSE 1.7.3

1.2 Dependencies

The driver is dependent on the following libraries and has been tested with the versions specified:

- stapler - version 1.6.0

1.3 Utility

The driver is released with a pre-built fuse utility program, which can be used to read and set fuse values from the command line.

Each chip has two utility variants - one in which information is printed via JEI and one where information is printed via the serial port. For the serial port utility variants the serial port parameters are:

Baud rate: 9600bps
Data bits: 8
Parity: None
Stop Bits: 1

2 Unresolved DDTS/Bugzilla entries

3 Resolved DDTS/Bugzilla entries

BRIsec002197 [5289/5206 SIgnature checking cannot be enabled]

BRIsec002173[Support for 5197 cut 3.x omitted from release list]

BRIsec002168 [STSECTOOLFUSE update to new build system]

BRIsec002196 [7141 c.2.2 fuses not supported]

BRIsec002168 [STSECTOOLFUSE update to new build system]

BRIsec002155 [Minor doc errors]

BRIsec2273 [Updated 5197/5167 swaf timing and reset sequence]

BRIsec2293 [Re-introduced 5167 support]

BRIsec2232 [5197 cut 3 VCC size change]

BRIsec2349 [Reduce Safmem programming delay]

CONFIDENTIAL

BRIsec2355 [5206 crypto_enable fuse added]

BRIsec2502 [Device multi-cut support]

BRIsec2573 [Access to crypt_fw_version_ctrl fuse on 7141 and 5206]

4 Know problems and limitatons

There is currently no way to specify a non-default charge pump level or refresh interval value for 7109.

The fuse utility program for 5167 and 5197 hangs while attempting to set a fuse value when running via JEI. The fuse value will be set, but the utility will need to be restarted. Using the serial port utility avoids this issue.

Information furnished is believed to be accurate and reliable. However, STMicroelectronics assumes no responsibility for the consequences of use of such information nor for any infringement of patents or other rights of third parties which may result from its use. No licence is granted by implication or otherwise under any patent or patent rights of STMicroelectronics. Specifications mentioned in this publication are subject to change without notice. This publication supersedes and replaces all information previously supplied. STMicroelectronics products are not authorized for use as critical components in life support devices or systems without express written approval of STMicroelectronics.

The ST logo is a trademark of STMicroelectronics

@2009 STMicroelectronics - All Rights Reserved

STMicroelectronics GROUP OF COMPANIES

CONFIDENTIAL

CONFIDENTIAL