AN1361
APPLICATION NOTE

Tuning Block Protection on the M58BW016B Flash Memory

CONTENTS

INTRODUCTION

The role of a standalone Flash Memory in a standard application is to collect code commands and functional parameters used by microprocessors to control the system. The final user of the application only stores data on well defined areas of the Flash address map. During application production steps, modification of some blocks of the Flash Memory must be prevented. For example generic boot code must be not modified during a calibration setup. It is also important to prevent the final user from modifying the application's functional code. For example, this could be something minor like the melody of a mobile phone, or something more serious like the control system of a vehicle's engine .

To prevent such modifications, Flash memories are equipped with a range of block protection functions. To allow even more flexibility, the M58BW016B Flash Memory is equipped with a new concept of block protection: the Tuning Block Protection, where the application manufacturer can choose a 64 bit password to protect against program and erase operations. Standard protection features are also available on the device. A version also exists with the Tuning Block Protection disabled, M58BW016D.

ORGANIZATION

The M58BW016B is a 16Mbit non-volatile burst Flash memory that can be erased electrically at the block level and programmed in-system using a 2.7V to 3.6V V_{DD} core power supply and a V_{DDQ} supply down to 2.4V for the Input and Output buffers. An optional 12V V_{PP} supply can be used to provide fast program and erase for a limited time and number of program/erase cycles.

The device has a boot block architecture with a x32 bus. The 16 Mbit address space is divided in 8 Parameter Blocks of 64 Kbit each, and 31 Main Blocks of 512 Kbit each. The device is available with Top or Bottom Boot block's. In the "Top" version the Parameter Blocks are located starting from the higher address (0xFFFFF). In the "Bottom" version they are from the first part of the memory (0x00000). In most applications the parameter blocks are used to store the boot code, and so usually require protection from accidental program or erase operations.

BLOCK PROTECTION OPTIONS

The M58BW016B features four different levels of block protection.

- **V_{PP} -** The device features an optional 12V V_{PP} voltage supply. Program or erase operation are also possible with Vpp at V_{IH} (3V). When V_{PP} is low at V_{SS} level (V_{IL}) all blocks are protected.
- **$\overline{WP}$ -** The two upper (Top) or lower (Bottom) Parameter Blocks and all the Main Blocks can be protected using the Write Protect Pin. When $\overline{WP}$ is low, $V_{IL,}$ all the lockable parameter blocks and all the main blocks are protected. When $\overline{WP}$ is high (V_{IH}) all the lockable parameter blocks and all the main blocks are unprotected.
- **$\overline{RP}$ -** If the device is held in reset mode ($\overline{RP}$ at V_{IL}), no program or erase operations can be performed on any block.
- Tuning block protection: M58BW016B features a 64 bit password protection for program and erase operations for a fixed number of blocks (see Figure 1)(a version with no password protection is also available). After power-up or reset the device is tuning protected, any attempt to program or erase the locked blocks will fail, the data in the block will not be changed and the Status Register will output the error (see data sheet for further detail on Status Register bits). A temporary Unlock command is provided to allow program or erase operations in all the blocks.

After a device reset the first three kinds of block protection (V_{PP}, $\overline{WP}$, $\overline{RP}$) can be combined to give a flexible block protection. They do not affect the Tuning Block Protection. When all three protections are disabled, V_{PP}, $\overline{WP}$ and $\overline{RP}$ at V_{IH}, the blocks locked by the Tuning Block Protection cannot be modified. All blocks are protected during power-up.

TUNING BLOCK PROTECTION DESCRIPTION

The Tuning Block Protection is a software feature to protect certain blocks from program or erase operations. The blocks are password protected. Program or erase operations are permitted only after the user has provided the correct 64 bit password, called the Tuning Protection Code. Not all blocks are tuning protected. The tuning protected blocks are the two parameter blocks closest to the boot address (Top or Bottom Boot) and the 24 main blocks located at the opposite boundary of the address space. 6 parameter blocks and 7 main blocks are not protected by the tuning algorithm. Refer to Figure 1, Tuning Block Protection Address Map.

The tuning blocks are "locked" if the tuning protection code has not been provided, and “unlocked" once the correct code has been provided. The tuning blocks are locked after reset or power-up. The Tuning Protection status can be monitored in Status Register. Bit0 in the Status Register indicates the tuning protection status. Bit0 = ‘0’ : tuning blocks are locked, Bit0 = ‘1’ : tuning blocks are unlocked. Bit1 indicates the block protection status. If it is set to ‘1’ a program or erase operation has been attempted on a protected block. The program erase controller status bit7 can be used to monitor when a program or erase operation has terminated.

Table 1, describes the commands needed to unlock and modify the tuning protected blocks.

Figure 1. Tuning Block Protection Address Map

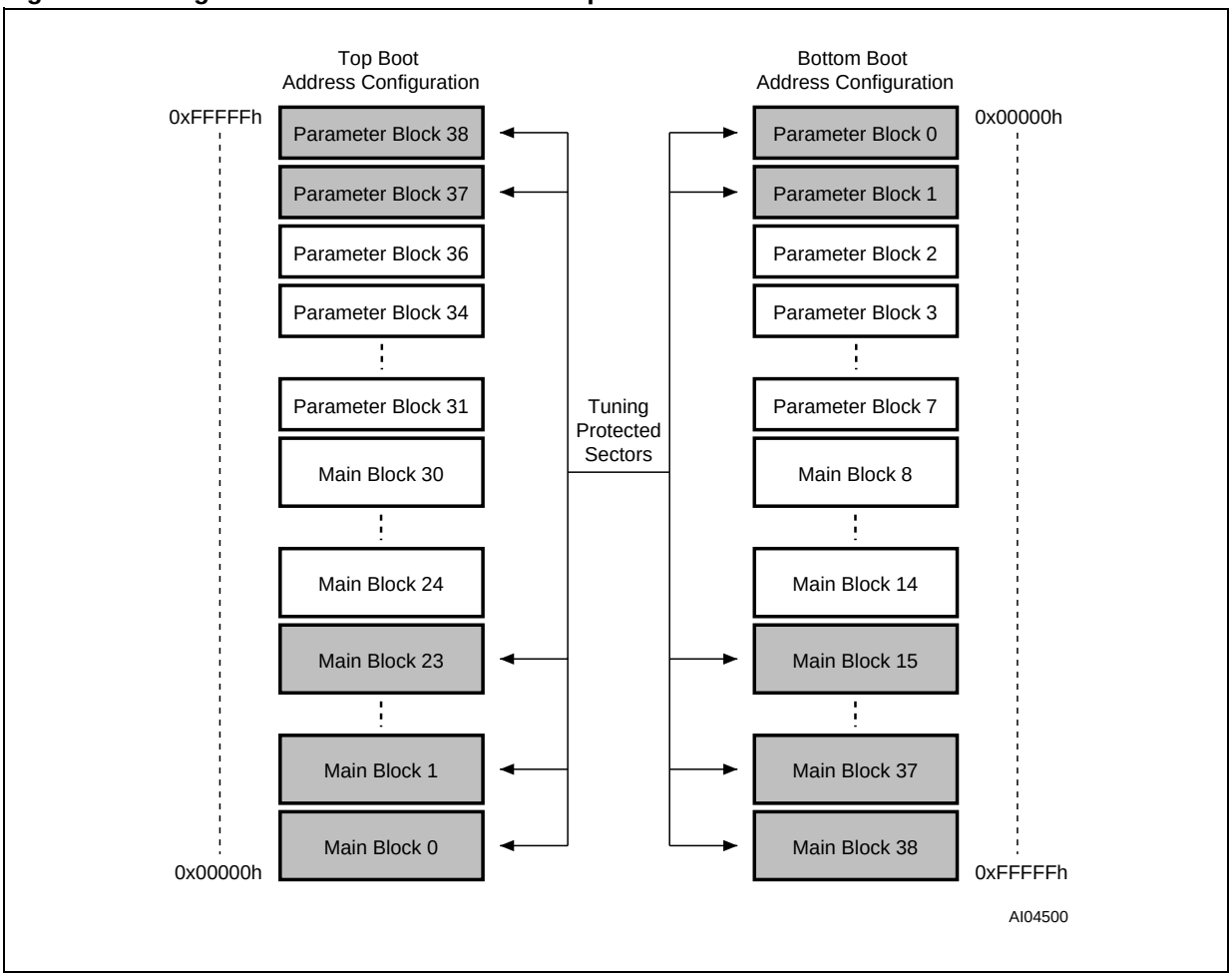


Table 1. Tuning Block Protection Commands

Command	Cycles	Bus Operations											
		1st Cycle			2nd Cycle			3rd Cycle			4th Cycle		
		Op.	Addr.	Data	Op.	Addr.	Data	Op.	Addr.	Data	Op.	Addr.	Data
Tuning Protection[2] Program	4	Write	X	48h	Write	TPAh	TPCh	Write	X	48h	Write	TPAh	TPCh
Tuning Protection Unlock[2]	4	Write	X	78h	Write	TPAh	TPCh	Write	X	78h	Write	TPAh	TPCh
Read Status Register	2	Write	X	70h	Read	X	SRDh						
Read Memory Array	≥ 2	Write	X	FFh	Read	RA	RD						
Block Erase	2	Write	X	20h	Write	BAh	D0h						
Program	2	Write	X	40h 10h	Write	PA	PD						

Note: 1. X Don't Care; TPA = Tuning Protection Address, TPC = Tuning Protection Code, SRD Status Register Data, RA Read Address, RD Read Data, PA Program Address; PD Program Data, BA Any address in the Block.
2. Cycles 1 and 2 input the first 32 bits of the code, cycles 3 and 4 the second 32 bits of the code.
3. Refer to the M58BW016B datasheet for a full description of commands.

TUNING PROTECTION UNLOCK

After a reset or power-up, the device must be unlocked to program or erase a tuning protected block. When the device is unlocked the user can protect all the blocks with V_{PP} at V_{IL}, or the first two parameters and all the main blocks with $\overline{WP}$ at V_{IL}.

The tuning protection unlock procedure is commonly used to temporary unprotect all the tuning protected blocks. It also unprotects the Tuning Protection Register where the tuning protection code is stored. Refer to Figure 2 for the operation flowchart.

The Tuning Protection Code is composed of 64 bits, but the data bus is 32 bits wide so four (2 x 2) write cycles are required to unlock the device.

- The first write cycle issues the Tuning Protection Unlock Setup command (0x78).
- The second write cycle inputs the first 32 bits of the tuning protection code on the data bus, at address 0x00000.

Bit 7 of the Status Register should now be checked to verify that the device has successfully stored the first part of the code in the internal register. If b7 = '1', the device is ready to accept the second part of the code. This does not mean that the first 32 bits match the tuning protection code, simply that it was correctly stored for the comparing. If b7 = '0', the user must wait for this bit setting (refer to write cycle AC timings).

- The third write cycle re-issues the Tuning Protection Unlock Setup command (0x78).
- The fourth write cycle inputs the second 32 bits of the code at address 0x00001.

Bit 7 of the Status Register should again be checked to verify that the device has successfully stored the second part of the code. When the device is ready (b7 = '1'), the tuning protection status can monitored on Status Register bit0. If b0 = '0' the device is locked; b0 = '1' the device is unlocked. If the device is still locked, a Read Memory Array command must be issued before any new attempt to unlock the device.

Device locked means that the 64 bit password is wrong. If the application user doesn't know the correct password, he can try again. The unlock sequence takes about 2 microseconds, therefore trying all possible combinations will take around 1,17 million years (Calculation: 264 * 2*10-6 / (3600*24*365) = 1,1698*106 years)!

Once the device is successfully unlocked, a Read Memory Array command must be issued to return the memory to read mode before any other command can be issued. The user can then program or erase all blocks, depending on $\overline{WP}$ status and V_{PP} level. At this point, it is also possible to configure a new protection code. To write a new protection code into the device tuning register, the user must perform the Tuning Protection Program sequence.

TUNING PROTECTION PROGRAM

The tuning protection code can be configured by the designer of the application. To configure the code, the user must specify the current protection code (when shipped all bits of the code are '1'), see the previous section Tuning Protection Unlock.

The tuning protection register is a non-erasable 64 Flash Memory cell array. When shipped all the bits in the register are set to '1' (that is all cells are erased). The user can program a '0' in any of the 64 positions. Once programmed it is not possible to reset a bit to '1' as the cells cannot be erased. The tuning protection register can be programmed at any moment (after providing the current code), however once all bits are set to '0' the tuning protection code can no longer be altered. Refer to Figure 2 for the operation flowchart.

The Tuning Protection Code is composed of 64 bits, but the data bus is 32 bits wide so four (2 x 2) write cycles are required to program the code.

- The first write cycle issues the Tuning Protection Program Setup command (0x48).
- The second write cycle inputs the first 32 bits of the new tuning protection code on the data bus, at address 0x00000.

Bit 7 of the Status Register should now be checked to verify that the device has successfully stored the first part of the code in the internal register. If b7 = '1', the device is ready to accept the second part of the code. If b7 = '0', the user must wait for this bit setting (refer to write cycle AC timings).

- The third write cycle re-issues the Tuning Protection Program Setup command (0x48).
- The fourth write cycle inputs the second 32 bits of the new code at address 0x00001.

Bit 7 of the Status Register should again be checked to verify that the device has successfully stored the second part of the code. When the device is ready (b7 = '1'). After completion Status Register bit 4 is set to '1' if there has been a program failure.

Programming aborts if V_{PP} drops out of the allowed range or $\overline{RP}$ goes to V_{IL}.

A Read Memory Array command must be issued to return the memory to read mode before issuing any other commands. Once the code has been changed a device reset or power-down will make the protection active with the new code.

Warning: If a Tuning Protection Program is aborted, it is not possible to re-program the device because the tuning protection register cannot be erased. The new protection code has not been correctly written and an algorithm to detect the partially written protection code is necessary.

Example,

a. Remember the positions with a logic '1', which were not to be programmed.

b. All the positions already changed to '0' in previous successful code changes cannot be modified, so they are still set to "0".

c. The positions that should have been changed from '1' to '0' can be now either '1' (program failed) or '0' (program terminated before abort event). So the user can try to guess these locations content making several unlock sequence trials.

d. If there are N undetermined bit locations, then there are 2^N possible combinations. If the user thinks that the abort occurred close to the beginning of programming, the trials should begin from the old tuning code. If the abort occurred close to the end of programming, the trials should begin from the new code.

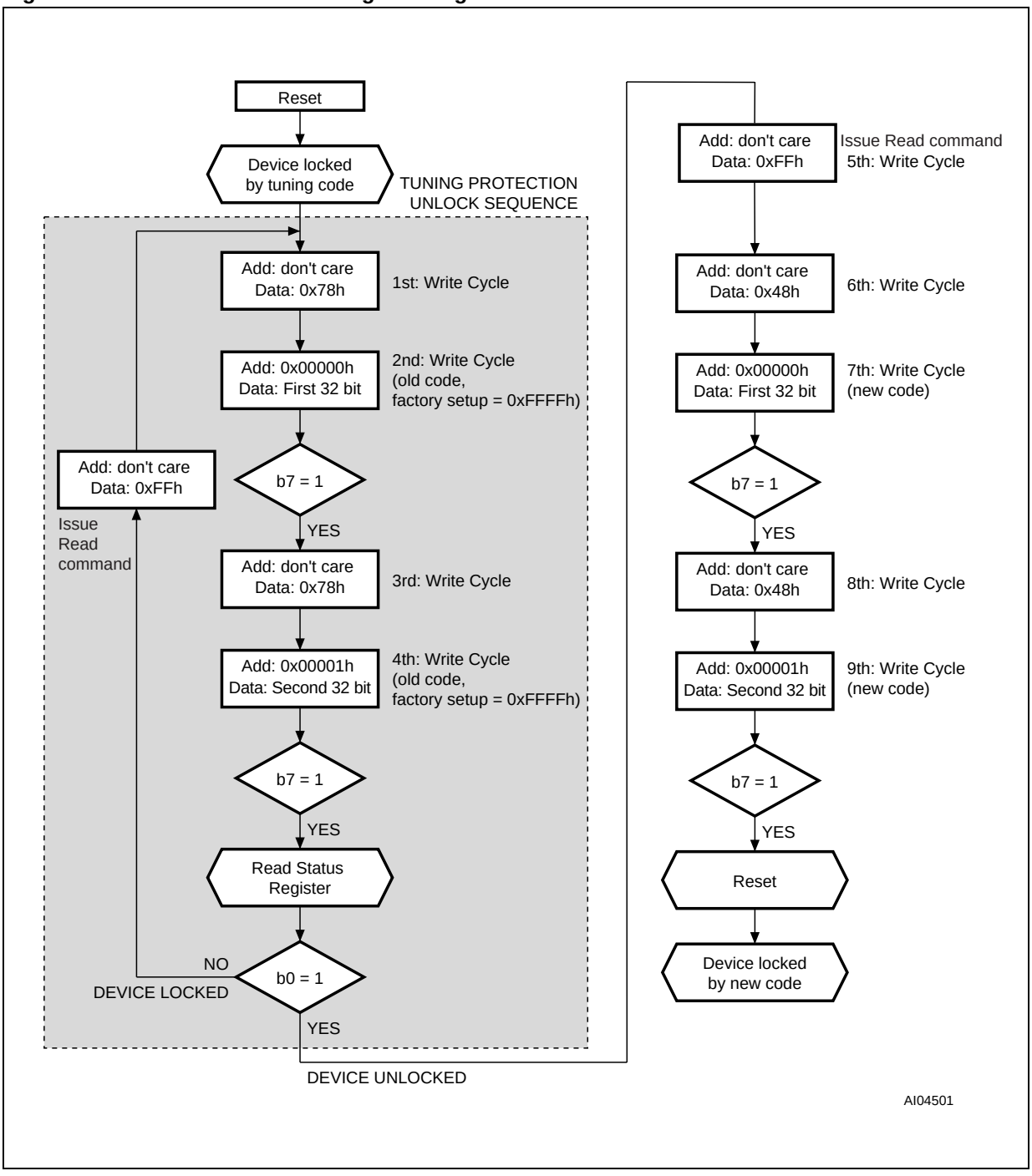
e. After the detection of the correct code, the user must re-program the desired code.

Example: Old Tuning code: 0x F0FF **F**F1F

New Tuning code: 0x F0FF **1**F1F

If a V_{PP} drop or a undesired reset occurs during the New Tuning Code Programming, the user can't be sure to have modified the code to 0x F0FF 1F1F. Looking at the new and old codes, the only positions that are undefined are the last three of the first 32 bits part (Hexadecimal digit F=1111_2 changed in 1=0001_2).

Figure 2. Unlock Device and Change Tuning Protection Code Flowchart



PROGRAM AND ERASE A TUNING PROTECTED BLOCK

The tuning protection unlock sequence is mandatory to modify a tuning protected block. After the b0 TPS bit check, the user issues the standard Erase or Program command. Any number of erase or program operations are allowed. The device is re-locked only after a reset or a power-down. V_{PP} or $\overline{WP}$ can be used to prevent the modification of all blocks, however V_{PP} and $\overline{WP}$ transitions don't affect the status of temporary tuning unprotection.

During the normal erase or program operations, other Status Register bits inform the user about the internal status (V_{PP} low, block protected, program/erase status fail). Figure 3 shows an unlock sequence to initialize a program operation. Figure 4 the same for erase.

Figure 3. Unlock Device and Program a Tuning Protected Block Flowchart

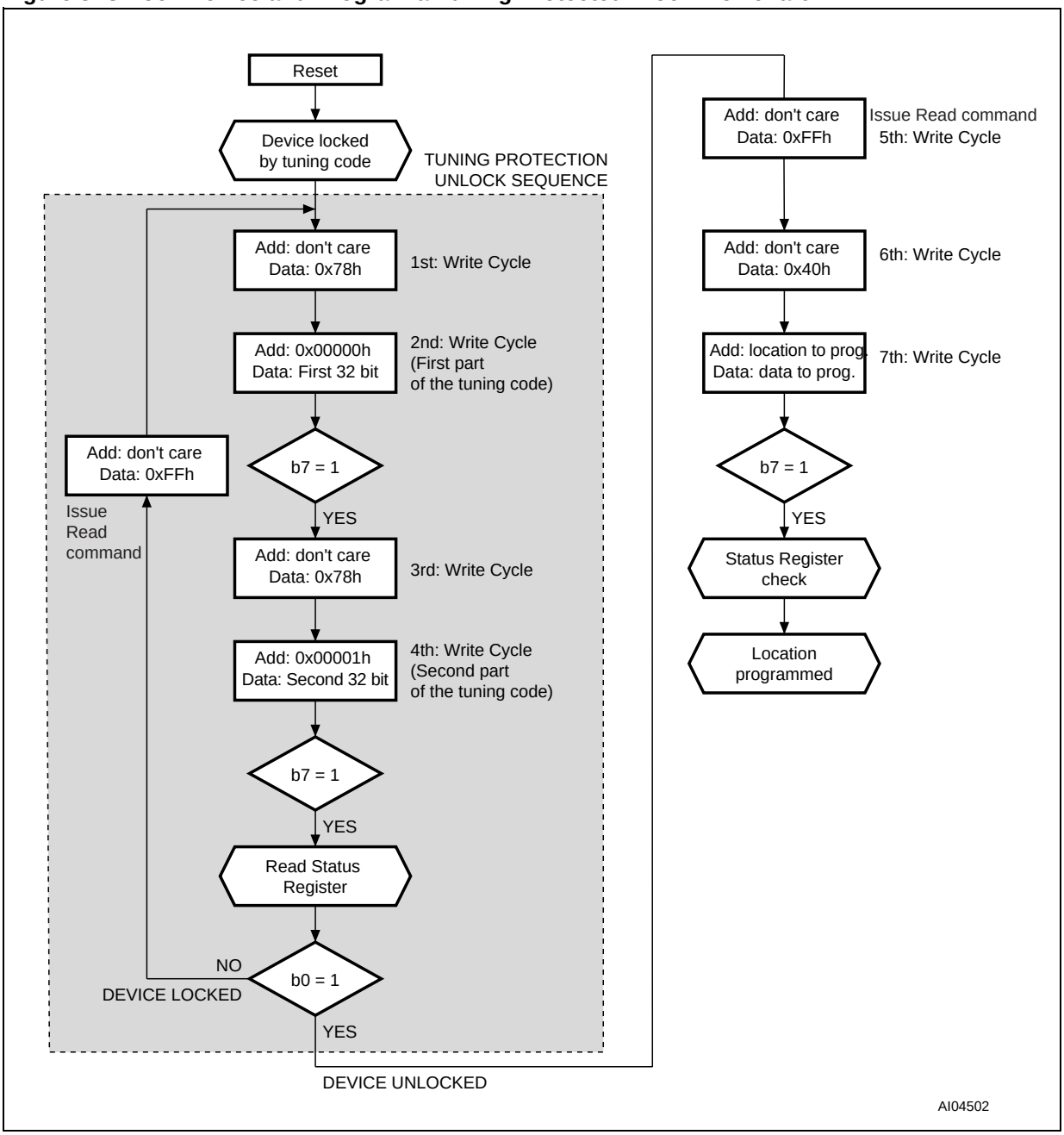
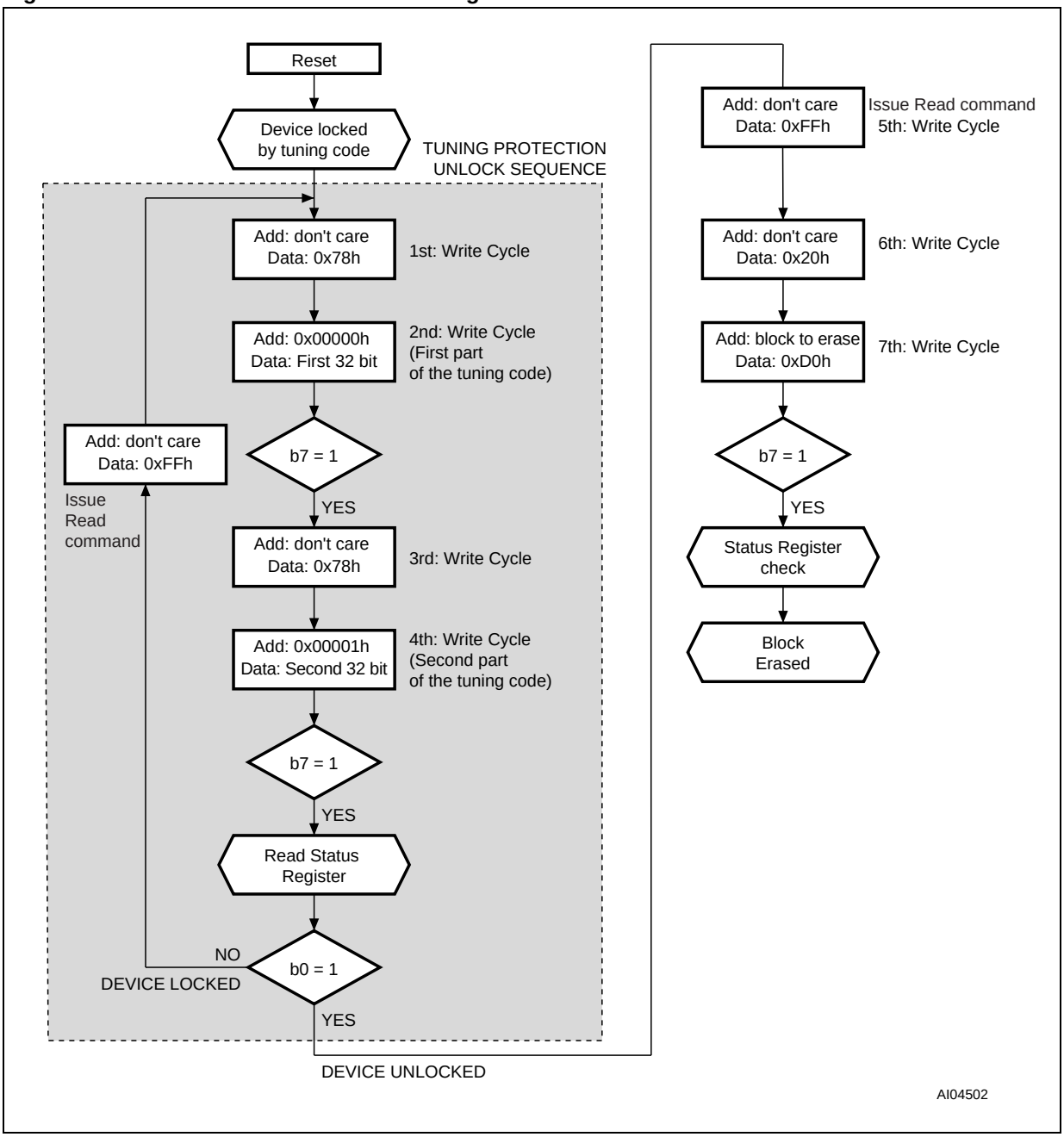


Figure 4. Unlock Device and Erase a Tuning Protected Block Flowchart



BLOCK PROTECTION COMBINATIONS

The flexible block protection of the M58BW016B allows protection for all phases of application production and usage. Table 2, shows all the possible combinations of block protection for the M58BW016B.

As previously mentioned, when the device is held in reset mode ($\overline{RP}$ at V_{IL}) no program or erase operation can be performed. With V_{PP} at V_{SS} the results are the same, but in this case the device is operational and the modify commands are recognized, but not executed (fail bits will be set in the Status Register). The 6 intermediate parameters blocks are always unprotected when V_{PP} and $\overline{RP}$ are high. For this reason this area of the device is the most suitable to make EEPROM emulation and to store final user data.

Table 2. Block Protection Combinations

Protection Options				Blocks			
$\overline{RP}$	V_{PP}	$\overline{WP}$	Tuning Protection	2 Parameters Blocks	6 Parameters Blocks	7 Main Blocks	24 Main Blocks
V_{IL}	X	X	X	Locked	Locked	Locked	Locked
V_{IH}	V_{IL}	X	X	Locked	Locked	Locked	Locked
V_{IH}	V_{IH} to 12V	V_{IL}	X	Locked	Unlocked	Locked	Locked
V_{IH}	V_{IH} to 12V	V_{IH}	On	Locked	Unlocked	Unlocked	Locked
V_{IH}	V_{IH} to 12V	V_{IH}	Off	Unlocked	Unlocked	Unlocked	Unlocked

Note: X = Don't Care.

CONCLUSIONS

The M58BW016B is a Flash memory with flexible block protection to allow data control at any time in the application lifetime. It features Tuning Block Protection, where certain blocks can be protected from program and erase operations with a 64 bit password. All the operations and algorithms related to non-volatile data protection in the final application can be derived from the protection features available in this device. The Flash Memory can be removed from the application, but no accidental or voluntary modifications can be performed on the crucial code, if it is stored in tuning protected blocks.

REVISION HISTORY

Date	Version	Revision Details
05-Jun- 2001	-01	First Issue

If you have any questions or suggestion concerning the matters raised in this document please send them to the following electronic mail address:

ask.memory@st.com (for general enquiries)

Please remember to include your name, company, location, telephone number and fax number.

littlediode
COMPONENTS FOR ALL

Littlediode supplies new, hard to find or obsolete electronic components and semiconductors all over the world.

With over two million different components listed you are sure to find the part you need.

Feel free to visit us today at our online store:

LittleDiode.com

Looking forward to providing you with the best possible service.