Automotive Product Group
Automotive Infotainment Division

SQI flash protection application note

1 Introduction

This document provides an overview of the SQI flash protection feature of all part numbers supported by STA8088 and STA8089/90.

All the SQI memories devices supported by TeseoII STA8088xx and TeseoIII STA8089/90 families have different ways to implement the flash protection feature. However all of them support the SPM (Software Protection Mode) that is discussed in this document.

1.1 Index

LIST OF FIGURES

2 Document Management

2.1 Revision History

Release	Date	Author	Status/Comment
1.0	Jul 9th 2014	G. De Angelis	First Release
1.1	Dec 12th 2014	A. Furno	General review
1.2	Feb 22nd 2016	G. De Angelis	Added comment for Spansion memory
1.3	June 3rd 2016	G. De Angelis	Added more detailed tables
1.4	June 16th 2016	G. De Angelis	Added Macronix R series table

2.2 Acronyms

Keywords	Definition
SPM	Software Protection Mode

2.3 Reference documents

[1] STA8088 Datasheet
[2] STA8088 Firmware Configuration
[3] STA8089-90 Firmware Configuration
[4] Macronix MX25U1635E Datasheet Rev. 2.0
[5] Macronix MX25U1635F Datasheet Rev. 1.5
[6] Winbond W25Q16DW Datasheet Rev. J
[7] Winbond W25Q16DV Datasheet Rev. F
[8] Winbond W25Q32FV Datasheet Rev. I
[9] Winbond W25Q256FV Datasheet Rev. H
[10] Winbond W25Q32BV Datasheet Rev. I
[11] Micron N25Q032A Datasheet Rev. J 2/15 EN
[12] Micron N25Q064A Datasheet Rev. N 10/14 EN
[13] Spansion S25FL1xxK Datasheet Rev. D
[14] Macronix MX25R3235F Datasheet Rev. 1.3

2.4 Contact info

Keyword	Definition
Giovanni De Angelis	giovanni.de-angelis@st.com

3 Power Cycles on Flashes

Power On/off cycles are critical in Flash management and particular attention is required to avoid accesses during these phases.

- Power – on

During Power on cycles, Flash has internal circuit that prevent accesses avoiding command execution in this condition. Furthermore during power on cycles, TeseoII and TeseoIII have internal startup timing that assure the necessary time for the flash to be ready to accept any command. During Power on cycles no access to the flash is executed.

- Power – off

Power off cycles are more critical, because in this phase there may be conditions where accesses to the Flash are possible. If Power off sequence is SW controlled, this may avoid undesired access to the flash while power is going down. If Power off is not controlled, conditions when the Flash is still responding to command with Voltage that is below the nominal value are possible. The flash embedded a Low Voltage Detection logic that, when Voltage level is below a specific value, keeps internal logic under Reset with no response to any command. This voltage level is reported as VWI in flash manual and thresholds is different between 1.8V and 3.3V flashes.

Hereafter are reported as examples snapshots from 1.8 and 3.3 Flash Datasheet. The behaviour of the Flash is common at Startup (self-protected) and required attention during power off.

MXIC

MACRONIX INTERNATIONAL CO., LTD.

MX25U1635E
MX25U3235E

POWER-ON STATE

The device is at below states when power-up:
- Standby mode (please note it is not deep power-down mode)
- Write Enable Latch (WEL) bit is reset

The device must not be selected during power-up and power-down stage unless the VCC achieves below correct level:
- VCC minimum at power-up stage and then after a delay of tVSL
- GND at power-down

Please note that a pull-up resistor on CS# may ensure a safe and proper power-up/down level.

An internal power-on reset (POR) circuit may protect the device from data corruption and inadvertent data change during power up state. When VCC is lower than VWI (POR threshold voltage value), the internal logic is reset and the flash device has no response to any command.

For further protection on the device, after VCC reaching the VWI level, a tPUW time delay is required before the device is fully accessible for commands like write enable (WREN), page program (PP), quad page program (4PP), sector erase (SE), block erase 32KB (BE32K), block erase (BE), chip erase (CE), WRSCUR and write status register (WRSR). If the VCC does not reach the VCC minimum level, the correct operation is not guaranteed. The write, erase, and program command should be sent after the below time delay:
- tPUW after VCC reached VWI level
- tVSL after VCC reached VCC minimum level

The device can accept read command after VCC reached VCC minimum and a time delay of tVSL, even time of tPUW has not passed.
Please refer to the figure of "power-up timing".

Note:
- To stabilize the VCC level, the VCC rail decoupled by a suitable capacitor close to package pins is recommended. (generally around 0.1uF)
- At power-down stage, the VCC drops below VWI level, all operations are disable and device has no response to any command. The data corruption might occur during the stage while a write, program, erase cycle is in progress.

8.3 Power-up Timing and Write Inhibit Threshold

PARAMETER	SYMBOL	SPEC		UNIT
		MIN	MAX	
VCC (min) to /CS Low	t_{VSL}[1]	20		µs
Time Delay Before Write Instruction	t_{PUW}[1]	5	10	ms
Write Inhibit Threshold Voltage	V_{WI}[1]	1.0	2.0	V

Note:
1. These parameters are characterized only.

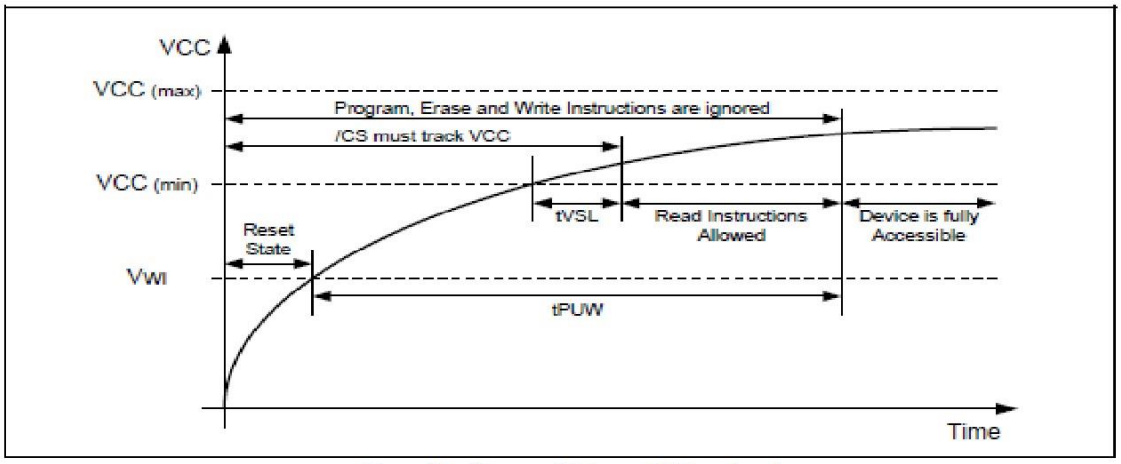

Figure 41a. Power-up Timing and Voltage Levels

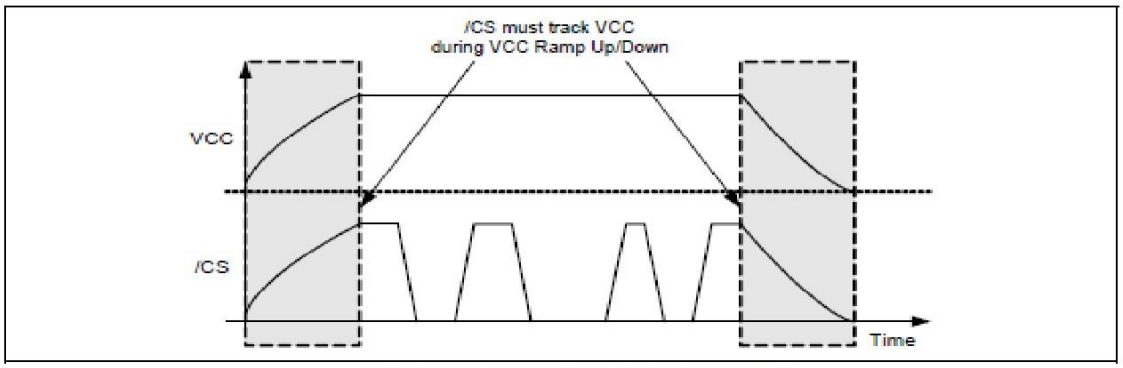

Figure 41b. Power-up, Power-Down Requirement

From Flash specification, the Vcc (min) voltage supply is specified as:

- 3.3V Flashes = 2.7V
- 1.8V Flashes = 1.62 V

The VWI voltage level (the one below which Flash LVD operates) is reported as:

- 3.3V Flashes = 1V min, 2V max
- 1.8V Flashes = 1V min, 1.4V max.

As example, during power down cycle in case of the 3.3 devices, there is a condition from 2.7V (Vcc – min) down to 2 V (VWI – max) where accesses to the Flash may not be properly executed.

There may generate false system level signals which result in unexpected erasure or programming condition.
The execution of these sequences in not guaranteed, and final flash status may be not correct.

To avoid such a condition and when it's not possible to assure a SW controlled shutdown, Flashes may be SW protected: this SW Protected Mode allows part or all the memory to be protected and respond as read only.

These settings allow portions (blocks) of Flash to be configured in the way to avoid undesired action of Program or Erase.

These Block Protect bits are non volatile RD/WR bits resident in the Flash Status Register.

SW has control of the different area of the Flash with these Protection Bits: once set, in the way to access in Programming or Erasing the protected area, the related bits have to be temporary cleared (to a 0 state indicating that the device is ready for required operations).

4 Description

ST GNSS devices supports different types of SQI flash memories. Each one has its own implementation of flash protection feature.

SPM is a configurable and easy to use way to protect SQI flash memory; the feature is supported by all the SQI flash part numbers listed in this document. SPM flash protection could not work with any other SQI flash part number not present in this document.

Even if SPM configuration is different among SQI flash model, all of them are associated with the same mechanism. These characteristics are common to all flash types:

- SPM can be fully configured and enabled by software;
- the configuration is stored in a non-volatile register, when enabled its status does not change after power cycle;
- the configuration can be modified at runtime by writing in a status register;
- protection feature is designed to be used on the flash program area, which typically is the lower 1MB of the SQI flash (0x00000000-0x000FFFFF). The area where GNSS data are stored (called NVM) must **NOT** be protected for any reason.

To support SPM feature, two new IDs have been added to the Configuration Data Block; they are CDB IDs 249 called “SPM” and 250 called “SPM_CONFIGURATION”.

See “STA8088_Firmware_Configuration.pdf” and “STA8089-90_Firmware_Configuration.pdf” documents for details.

Figure 1 is a flowchart to describe how SPM works in the official STA8088 Binary Image firmware; the behavior for STA8089-90 is the same.

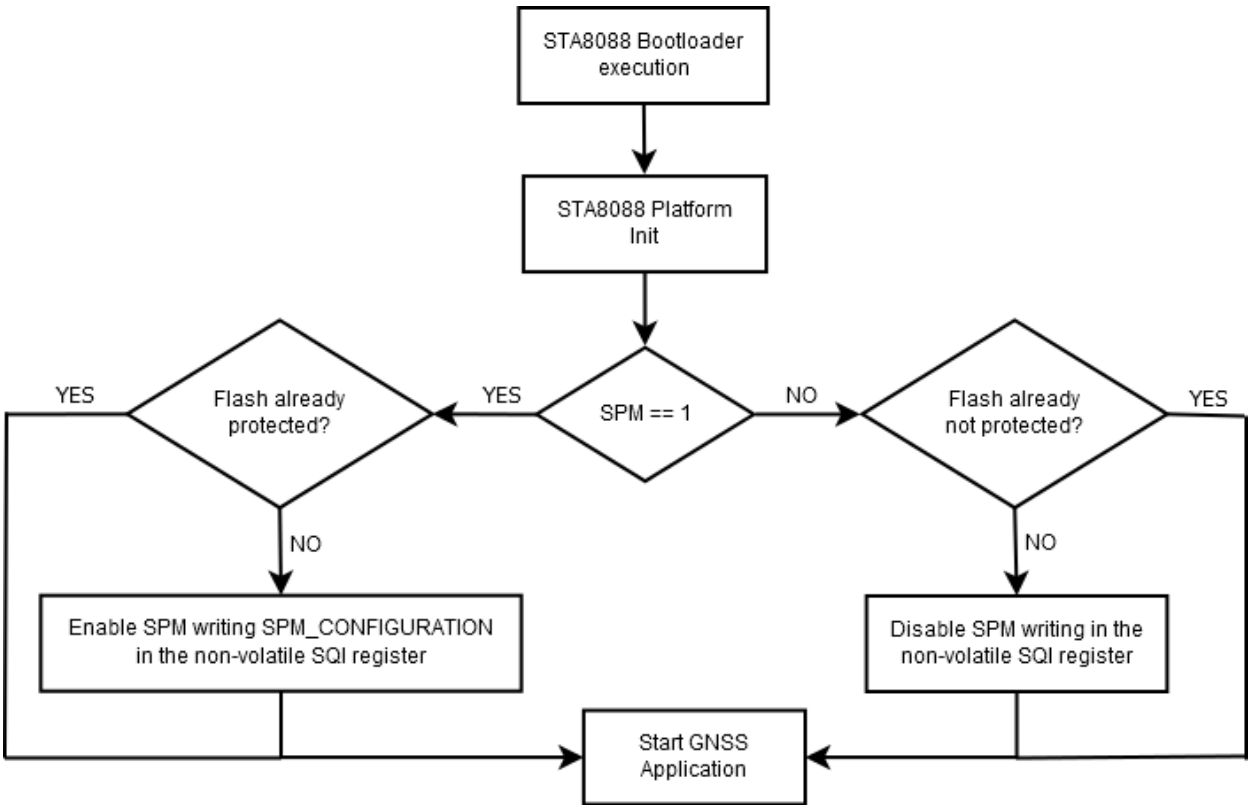

Figure 1: Software Protection Mode flowchart

The STA80xx Bootcode never enables protection in the SQI flash memory; it's STA80xx Binary Image firmware that configures SPM using the configuration provided by the user. SPM feature is supported on TeseoII from STA8088 Binary Image 3.1.15 and 3.3.5 DRAW; on TeseoIII from STA8089-90 Binary Image 4.5.3 and 4.7.4 DRAW.

Each SQI flash device has its proprietary configuration scheme; below there's the configuration list for all TeseoII and TeseoIII part numbers with embedded SQI:

Embedded SQI	**CDB-ID 250** SPM_CONFIGURATION	**Memory part number**
STA8088Fxx STA8088CFxx	**0x0A**	Macronix MX25U1635E
STA8089Fxx	**0x0A**	
STA8090Fxx	**0x0A**	Macronix MX25U1635F
STA8090F4xx	**0x15**	Macronix MX25R3235F

When an external SQI flash is used, the SPM configuration depends on the specific SQI flash part number. This is the configuration list of all SQI part numbers supported by TeseoII and TeseoIII:

External SQI		**CDB-ID 250** SPM_CONFIGURATION	Comments
Vendor	p/n		
Macronix	MX25U1635E MX25U1635F	**0x0A**	Supported by TeseoII and TeseoIII
Winbond	W25QxxxFV/DW/DV Where xxx<256	**0x0D**	Supported by TeseoII and TeseoIII
Winbond	W25QxxxBV Where xxx<256	**0x0D**	Supported by TeseoIII only
Winbond	W25Q256FV	**0x15**	Supported by TeseoII and TeseoIII
Micron	N25Q032A	**0x0D**	Supported by TeseoII and TeseoIII
Micron	N25Q064A	**0x0D**	Supported by TeseoII and TeseoIII
Spansion	S25FL116K S25FL132K	**0x0D**	Supported by TeseoIII only
Spansion	S25FL164K	**0x0C**	Supported by TeseoIII only
Macronix	MX25R3235F	**0x15**	Supported by TeseoIII only

4.1 Macronix MX25U1635E/F

This SQI flash is supported by both TeseoII and Teseo III platforms.

The parameter “SPM_CONFIGURATION” passed with CDB ID 250 is an 8-bit data and it’s written in the SQI SPM register without any modification. Below the bit encoding of this parameter:

CDB-ID 250 =	0	0	0	0	BP3	BP2	BP1	BP0

Figure 2 shows the SQI protection configurations valid for Macronix MX25U1635E/F flash devices:

Status bit				Protect Level
BP3	BP2	BP1	BP0	16Mb
0	0	0	0	0 (none)
0	0	0	1	1 (1block, protected block 31st)
0	0	1	0	2 (2blocks, protected block 30th~31st)
0	0	1	1	3 (4blocks, protected block 28th~31st)
0	1	0	0	4 (8blocks, protected block 24th~31st)
0	1	0	1	5 (16blocks, protected block 16th~31st)
0	1	1	0	6 (32blocks, protected all)
0	1	1	1	7 (32blocks, protected all)
1	0	0	0	8 (32blocks, protected all)
1	0	0	1	9 (32blocks, protected all)
1	0	1	0	10 (16blocks, protected block 0th~15th)
1	0	1	1	11 (24blocks, protected block 0th~23rd)
1	1	0	0	12 (28blocks, protected block 0th~27th)
1	1	0	1	13 (30blocks, protected block 0th~29th)
1	1	1	0	14 (31blocks, protected block 0th~30th)
1	1	1	1	15 (32blocks, protected all)

Figure 2: SPM table for Macronix MX25U1635E/F

SPM configuration value must match the content of BPx bits in order to properly configure SQI flash protection. For example, if user wants to enable flash protection for lower 1MB he must use the configuration:

- `BP3 = 1;`
- `BP2 = 0;`
- `BP1 = 1;`
- `BP0 = 0;`

SPM configuration value must be equal to: **0x0A**.

4.2 Winbond W25QxxxDW/DV/FV/BV

This SQI flash is supported by both TeseoII and TeseoIII platforms.

The parameter “SPM_CONFIGURATION” passed with CDB ID 250 is an 8-bit data and it’s written in the SQI SPM register without any modification. This flash type uses a different meaning for the internal register where the SPM information are stored depending on flash size. Below the bit encoding of CDB ID 250 parameter valid for all the flash up to 128Mb (16 MB):

CDB-ID 250 =	0	0	0	SEC	TB	BP2	BP1	BP0

Figure 3 shows the SQI protection configurations valid for Winbond W25Q32FV flash device. This table is valid for other part numbers DW/DV/BV with a size up to 128Mb (16 MB).

STATUS REGISTER[1]					W25Q32FV (32M-BIT) MEMORY PROTECTION[3]			
SEC	TB	BP2	BP1	BP0	PROTECTED BLOCK(S)	PROTECTED ADDRESSES	PROTECTED DENSITY	PROTECTED PORTION[2]
X	X	0	0	0	NONE	NONE	NONE	NONE
0	0	0	0	1	63	3F0000h – 3FFFFFh	64KB	Upper 1/64
0	0	0	1	0	62 and 63	3E0000h – 3FFFFFh	128KB	Upper 1/32
0	0	0	1	1	60 thru 63	3C0000h – 3FFFFFh	256KB	Upper 1/16
0	0	1	0	0	56 thru 63	380000h – 3FFFFFh	512KB	Upper 1/8
0	0	1	0	1	48 thru 63	300000h – 3FFFFFh	1MB	Upper 1/4
0	0	1	1	0	32 thru 63	200000h – 3FFFFFh	2MB	Upper 1/2
0	1	0	0	1	0	000000h – 00FFFFh	64KB	Lower 1/64
0	1	0	1	0	0 and 1	000000h – 01FFFFh	128KB	Lower 1/32
0	1	0	1	1	0 thru 3	000000h – 03FFFFh	256KB	Lower 1/16
0	1	1	0	0	0 thru 7	000000h – 07FFFFh	512KB	Lower 1/8
0	1	1	0	1	0 thru 15	000000h – 0FFFFFh	1MB	Lower 1/4
0	1	1	1	0	0 thru 31	000000h – 1FFFFFh	2MB	Lower 1/2
X	X	1	1	1	0 thru 63	000000h – 3FFFFFh	4MB	ALL
1	0	0	0	1	63	3FF000h – 3FFFFFh	4KB	U - 1/1024
1	0	0	1	0	63	3FE000h – 3FFFFFh	8KB	U - 1/512
1	0	0	1	1	63	3FC000h – 3FFFFFh	16KB	U - 1/256
1	0	1	0	X	63	3F8000h – 3FFFFFh	32KB	U - 1/128
1	1	0	0	1	0	000000h – 000FFFh	4KB	L - 1/1024
1	1	0	1	0	0	000000h – 001FFFh	8KB	L - 1/512
1	1	0	1	1	0	000000h – 003FFFh	16KB	L - 1/256
1	1	1	0	X	0	000000h – 007FFFh	32KB	L - 1/128

Figure 3: SPM table for Winbond W25Q32FV

SPM configuration value must match the content of SEC, TB and BPx bits in order to properly configure SQI flash protection. . For example, if user wants to enable flash protection for lower 1MB he must use the configuration:

- SEC = 0;
- TB = 1;
- BP2 = 1;
- BP1 = 0;
- BP0 = 1;

SPM configuration value must be equal to: **0x0D**.

Below the bit encoding of CDB ID 250 parameter valid for all the flash starting from 256Mb (32 MB):

CDB-ID 250 =	0	0	0	TB	BP3	BP2	BP1	BP0

Figure 4 shows the SQI protection configurations valid for Winbond W25Q256FV flash device:

STATUS REGISTER(1)					W25Q256FV (256M-BIT / 32M-BYTE) MEMORY PROTECTION(2)			
TB	BP3	BP2	BP1	BP0	PROTECTED BLOCK(S)	PROTECTED ADDRESSES	PROTECTED DENSITY	PROTECTED PORTION
X	0	0	0	0	NONE	NONE	NONE	NONE
0	0	0	0	1	511	01FF0000h - 01FFFFFFh	64KB	Upper 1/512
0	0	0	1	0	510 thru 511	01FE0000h - 01FFFFFFh	128KB	Upper 1/256
0	0	0	1	1	508 thru 511	01FC0000h - 01FFFFFFh	256KB	Upper 1/128
0	0	1	0	0	504 thru 511	01F80000h - 01FFFFFFh	512KB	Upper 1/64
0	0	1	0	1	496 thru 511	01F00000h - 01FFFFFFh	1MB	Upper 1/32
0	0	1	1	0	480 thru 511	01E00000h - 01FFFFFFh	2MB	Upper 1/16
0	0	1	1	1	448 thru 511	01C00000h - 01FFFFFFh	4MB	Upper 1/8
0	1	0	0	0	384 thru 511	01800000h - 01FFFFFFh	8MB	Upper 1/4
0	1	0	0	1	256 thru 511	01000000h - 01FFFFFFh	16MB	Upper 1/2
1	0	0	0	1	0	00000000h - 0000FFFFh	64KB	Lower 1/512
1	0	0	1	0	0 thru 1	00000000h - 0001FFFFh	128KB	Lower 1/256
1	0	0	1	1	0 thru 3	00000000h - 0003FFFFh	256KB	Lower 1/128
1	0	1	0	0	0 thru 7	00000000h - 0007FFFFh	512KB	Lower 1/64
1	0	1	0	1	0 thru 15	00000000h - 000FFFFFh	1MB	Lower 1/32
1	0	1	1	0	0 thru 31	00000000h - 001FFFFFh	2MB	Lower 1/16
1	0	1	1	1	0 thru 63	00000000h - 003FFFFFh	4MB	Lower 1/8
1	1	0	0	0	0 thru 127	00000000h - 007FFFFFh	8MB	Lower 1/4
1	1	0	0	1	0 thru 255	00000000h - 00FFFFFFh	16MB	Lower 1/2
X	1	1	0	X	0 thru 511	00000000h - 01FFFFFFh	32MB	ALL
X	1	X	1	X	0 thru 511	00000000h - 01FFFFFFh	32MB	ALL

Figure 4: SPM table for Winbond W25Q256FV

SPM configuration value must match the content of TB and BPx bits in order to properly configure SQI flash protection. . For example, if user wants to enable flash protection for lower 1MB he must use the configuration:

- `TB  = 1;`
- `BP3 = 0;`
- `BP2 = 1;`
- `BP1 = 0;`
- `BP0 = 1;`

SPM configuration value must be equal to: **0x15**.

4.3 Micron N25QxxxA

This SQI flash is supported by both TeseoII and TeseoIII platforms.

The parameter “SPM_CONFIGURATION” passed with CDB ID 250 is an 8-bit data and it’s written in the SQI SPM register without any modification. This flash type uses a different meaning for the internal register where the SPM information are stored depending on flash size. Below the bit encoding of CDB ID 250 parameter valid for all the flash up to 32Mb (4 MB):

CDB-ID 250 =	0	0	0	0	TB	BP2	BP1	BP0

Figure 5 shows the SQI protection configurations valid for Micron N25Q032A flash device:

Status Register Content				Memory Content	
Top/ Bottom Bit	BP2	BP1	BP0	Protected Area	Unprotected Area
0	0	0	0	None	All sectors
0	0	0	1	Upper 64th	Sectors (0 to 62)
0	0	1	0	Upper 32th	Sectors (0 to 61)
0	0	1	1	Upper 16th	Sectors (0 to 59)
0	1	0	0	Upper 8th	Sectors (0 to 55)
0	1	0	1	Upper 4th	Sectors (0 to 47)
0	1	1	0	Upper half	Sectors (0 to 31)
0	1	1	1	All sectors	None
1	0	0	0	None	All sectors
1	0	0	1	Lower 64th	Sectors (1 to 63)
1	0	1	0	Lower 32th	Sectors (2 to 63)
1	0	1	1	Lower 16th	Sectors (4 to 63)
1	1	0	0	Lower 8th	Sectors (8 to 63)
1	1	0	1	Lower 4th	Sectors (16 to 63)
1	1	1	0	Lower half	Sectors (32 to 63)
1	1	1	1	All sectors	None

Figure 5: SPM table for Micron N25Q032A

SPM configuration value must match the content of TB and BPx bits in order to properly configure SQI flash protection. For example, if user wants to enable flash protection for lower 1MB he must use the configuration:

- `TB  = 1;`
- `BP2 = 1;`
- `BP1 = 0;`
- `BP0 = 1;`

SPM configuration value must be equal to: **0x0D**.

Below the bit encoding of CDB ID 250 parameter valid for all the flash starting from 64Mb (8 MB):

CDB-ID 250 =	0	0	0	BP3	TB	BP2	BP1	BP0

Figure 6 shows the SQI protection configurations valid for Micron N25Q064A flash device:

Status Register Content					Memory Content	
Top/ Bottom Bit	BP3	BP2	BP1	BP0	Protected Area	Unprotected Area
0	0	0	0	0	None	All sectors
0	0	0	0	1	Upper 128th	Sectors (0 to 126)
0	0	0	1	0	Upper 64th	Sectors (0 to 125)
0	0	0	1	1	Upper 32nd	Sectors (0 to 123)
0	0	1	0	0	Upper 16th	Sectors (0 to119)
0	0	1	0	1	Upper 8th	Sectors (0 to 111)
0	0	1	1	0	Upper quarter	Sectors (0 to 95)
0	0	1	1	1	Upper half	Sectors (0 to 63)
0	1	0	0	0	All sectors	None
0	1	0	0	1	All sectors	None
0	1	0	1	0	All sectors	None
0	1	0	1	1	All sectors	None
0	1	1	0	0	All sectors	None
0	1	1	0	1	All sectors	None
0	1	1	1	0	All sectors	None
0	1	1	1	1	All sectors	None
1	0	0	0	0	None	All sectors
1	0	0	0	1	Lower 128th	Sectors (1 to 127)
1	0	0	1	0	Lower 64th	Sectors (2 to 127)
1	0	0	1	1	Lower 32nd	Sectors (4 to 127)
1	0	1	0	0	Lower 16th	Sectors (8 to 127)
1	0	1	0	1	Lower 8th	Sectors (16 to 127)
1	0	1	1	0	Lower quarter	Sectors (32 to 127)
1	0	1	1	1	Lower half	Sectors (64 to 127)
1	1	0	0	0	All sectors	None
1	1	0	0	1	All sectors	None
1	1	0	1	0	All sectors	None
1	1	0	1	1	All sectors	None
1	1	1	0	0	All sectors	None
1	1	1	0	1	All sectors	None
1	1	1	1	0	All sectors	None
1	1	1	1	1	All sectors	None

Figure 6: SPM table for Micron N25Q064A

SPM configuration value must match the content of TB and BPx bits in order to properly configure SQI flash protection. . For example, if user wants to enable flash protection for lower 1MB he must use the configuration:

- `BP3 = 0;`
- `TB  = 1;`
- `BP2 = 1;`
- `BP1 = 0;`
- `BP0 = 1;`

SPM configuration value must be equal to: **0x0D**.

4.4 Spansion S25FL1xxK

This SQI flash is supported by TeseoIII platform.

The parameter “SPM_CONFIGURATION” passed with CDB ID 250 is an 8-bit data and it’s written in the SQI SPM register without any modification. Below the bit encoding of this parameter:

CDB-ID 250 =	0	0	0	SEC	TB	BP2	BP1	BP0

Figure 7 shows the SQI protection configurations valid for Spansion S25FL116K flash device:

Status Register (1)					S25FL1-K (16 Mbit) Block Protection (CMP=0) (2)			
SEC	TB	BP2	BP1	BP0	Protected Block(s)	Protected Addresses	Protected Density	Protected Portion
X	X	0	0	0	None	None	None	None
0	0	0	0	1	31	1F0000h – 1FFFFFh	64 kB	Upper 1/32
0	0	0	1	0	30 and 31	1E0000h – 1FFFFFh	128 kB	Upper 1/16
0	0	0	1	1	28 thru 31	1C0000h – 1FFFFFh	256 kB	Upper 1/8
0	0	1	0	0	24 thru 31	180000h – 1FFFFFh	512 kB	Upper 1/4
0	0	1	0	1	16 thru 31	100000h – 1FFFFFh	1 MB	Upper 1/2
0	1	0	0	1	0	000000h – 00FFFFh	64 kB	Lower 1/32
0	1	0	1	0	0 and 1	000000h – 01FFFFh	128 kB	Lower 1/16
0	1	0	1	1	0 thru 3	000000h – 03FFFFh	256 kB	Lower 1/8
0	1	1	0	0	0 thru 7	000000h – 07FFFFh	512 kB	Lower 1/4
0	1	1	0	1	0 thru 15	000000h – 0FFFFFh	1 MB	Lower 1/2
X	X	1	1	X	0 thru 31	000000h – 1FFFFFh	2 MB	All
1	0	0	0	1	31	1FF000h – 1FFFFFh	4 kB	Upper 1/512
1	0	0	1	0	31	1FE000h – 1FFFFFh	8 kB	Upper 1/256
1	0	0	1	1	31	1FC000h – 1FFFFFh	16 kB	Upper 1/128
1	0	1	0	X	31	1F8000h – 1FFFFFh	32 kB	Upper 1/64
1	1	0	0	1	0	000000h – 000FFFh	4 kB	Lower 1/512
1	1	0	1	0	0	000000h – 001FFFh	8 kB	Lower 1/256
1	1	0	1	1	0	000000h – 003FFFh	16 kB	Lower 1/128
1	1	1	0	X	0	000000h – 007FFFh	32 kB	Lower 1/64

Figure 7: SPM table for Spansion S25FL116K

Figure 8 shows the SQI protection configurations valid for Spansion S25FL132K flash device:

Status Register (1)					S25FL132K (32-Mbit) Block Protection (CMP=0) ()			
SEC	TB	BP2	BP1	BP0	Protected Block(s)	Protected Addresses	Protected Density	Protected Portion
X	X	0	0	0	None	None	None	None
0	0	0	0	1	63	3F0000h – 3FFFFFh	64 kB	Upper 1/64
0	0	0	1	0	62 and 63	3E0000h – 3FFFFFh	128 kB	Upper 1/32
0	0	0	1	1	60 thru 63	3C0000h – 3FFFFFh	256 kB	Upper 1/16
0	0	1	0	0	56 thru 63	380000h – 3FFFFFh	512 kB	Upper 1/8
0	0	1	0	1	48 thru 63	300000h – 3FFFFFh	1 MB	Upper 1/4
0	0	1	1	0	32 thru 63	200000h – 3FFFFFh	2 MB	Upper 1/2
0	1	0	0	1	0	000000h – 00FFFFh	64 kB	Lower 1/64
0	1	0	1	0	0 and 1	000000h – 01FFFFh	128 kB	Lower 1/32
0	1	0	1	1	0 thru 3	000000h – 03FFFFh	256 kB	Lower 1/16
0	1	1	0	0	0 thru 7	000000h – 07FFFFh	512 kB	Lower 1/8
0	1	1	0	1	0 thru 15	000000h – 0FFFFFh	1 MB	Lower 1/4
0	1	1	1	0	0 thru 31	000000h – 1FFFFFh	2 MB	Lower 1/2
X	X	1	1	1	0 thru 63	000000h – 3FFFFFh	4 MB	All
1	0	0	0	1	63	3FF000h – 3FFFFFh	4 kB	Upper 1/1024
1	0	0	1	0	63	3FE000h – 3FFFFFh	8 kB	Upper 1/512
1	0	0	1	1	63	3FC000h – 3FFFFFh	16 kB	Upper 1/256
1	0	1	0	X	63	3F8000h – 3FFFFFh	32 kB	Upper 1/128
1	1	0	0	1	0	000000h – 000FFFh	4 kB	Lower 1/1024
1	1	0	1	0	0	000000h – 001FFFh	8 kB	Lower 1/512
1	1	0	1	1	0	000000h – 003FFFh	16 kB	Lower 1/256
1	1	1	0	X	0	000000h – 007FFFh	32 kB	Lower 1/128

Figure 8: SPM table for Spansion S25FL132K

SPM configuration value must match the content of SEC, TB and BPx bits in order to properly configure SQI flash protection. For example, if user wants to enable flash protection for lower 1MB he must use the configuration:

- `SEC = 0;`
- `TB  = 1;`
- `BP2 = 1;`
- `BP1 = 0;`
- `BP0 = 1;`

SPM configuration value must be equal to: **0x0D**.

Figure 9 shows the SQI protection configurations valid for Spansion S25FL164K flash device:

Status Register (1)					S25FL164K (64-Mbit) Block Protection (CMP=0) (2)			
SEC	TB	BP2	BP1	BP0	Protected Block(s)	Protected Addresses	Protected Density	Protected Portion
X	X	0	0	0	None	None	None	None
0	0	0	0	1	126 and 127	7E0000h – 7FFFFFh	128 kB	Upper 1/64
0	0	0	1	0	124 thru 127	7C0000h – 7FFFFFh	256 kB	Upper 1/32
0	0	0	1	1	120 thru 127	780000h – 7FFFFFh	512 kB	Upper 1/16
0	0	1	0	0	112 thru 127	700000h – 7FFFFFh	1 MB	Upper 1/8
0	0	1	0	1	96 thru 127	600000h – 7FFFFFh	2 MB	Upper 1/4
0	0	1	1	0	64 thru 127	400000h – 7FFFFFh	4 MB	Upper 1/2
0	1	0	0	1	0 and 1	000000h – 01FFFFh	128 kB	Lower 1/64
0	1	0	1	0	0 thru 3	000000h – 03FFFFh	256 kB	Lower 1/32
0	1	0	1	1	0 thru 7	000000h – 07FFFFh	512 kB	Lower 1/16
0	1	1	0	0	0 thru 15	000000h – 0FFFFFh	1 MB	Lower 1/8
0	1	1	0	1	0 thru 31	000000h – 1FFFFFh	2 MB	Lower 1/4
0	1	1	1	0	0 thru 63	000000h – 3FFFFFh	4 MB	Lower 1/2
X	X	1	1	1	0 thru 127	000000h – 7FFFFFh	8 MB	ALL
1	0	0	0	1	127	7FF000h – 7FFFFFh	4 kB	Upper 1/2048
1	0	0	1	0	127	7FE000h – 7FFFFFh	8 kB	Upper 1/1024
1	0	0	1	1	127	7FC000h – 7FFFFFh	16 kB	Upper 1/512
1	0	1	0	X	127	7F8000h – 7FFFFFh	32 kB	Upper 1/256
1	1	0	0	1	0	000000h – 000FFFh	4 kB	Lower1/2048
1	1	0	1	0	0	000000h – 001FFFh	8 kB	Lower 1/1024
1	1	0	1	1	0	000000h – 003FFFh	16 kB	Lower 1/512
1	1	1	0	X	0	000000h – 007FFFh	32 kB	Lower 1/256

Figure 9: SPM table for Spansion S25FL164K

SPM configuration value must match the content of SEC, TB and BPx bits in order to properly configure SQI flash protection. For example, if user wants to enable flash protection for lower 1MB he must use the configuration:

- `SEC = 0;`
- `TB  = 1;`
- `BP2 = 1;`
- `BP1 = 0;`
- `BP0 = 0;`

SPM configuration value must be equal to: **0x0C**.

4.5 Macronix MX25R3235F

This SQI flash is supported by TeseoIII platform.

The parameter “SPM_CONFIGURATION” passed with CDB ID 250 is an 8-bit data and it’s written in the SQI SPM register without any modification. Below the bit encoding of this parameter:

CDB-ID 250 =	0	0	0	TB	BP3	BP2	BP1	BP0

Figure 10 shows the SQI protection configurations valid for Macronix MX25R3235F flash device:

Protected Area Sizes (TB bit = 0)

Status bit				Protect Level
BP3	BP2	BP1	BP0	32Mb
0	0	0	0	0 (none)
0	0	0	1	1 (1block, block 63th)
0	0	1	0	2 (2blocks, block 62nd-63rd)
0	0	1	1	3 (4blocks, block 60th-63rd)
0	1	0	0	4 (8blocks, block 56th-63rd)
0	1	0	1	5 (16blocks, block 48th-63rd)
0	1	1	0	6 (32blocks, block 32nd-63rd)
0	1	1	1	7 (64blocks, protect all)
1	0	0	0	8 (64blocks, protect all)
1	0	0	1	9 (64blocks, protect all)
1	0	1	0	10 (64blocks, protect all)
1	0	1	1	11 (64blocks, protect all)
1	1	0	0	12 (64blocks, protect all)
1	1	0	1	13 (64blocks, protect all)
1	1	1	0	14 (64blocks, protect all)
1	1	1	1	15 (64blocks, protect all)

Protected Area Sizes (TB bit = 1)

Status bit				Protect Level
BP3	BP2	BP1	BP0	32Mb
0	0	0	0	0 (none)
0	0	0	1	1 (1block, block 0th)
0	0	1	0	2 (2blocks, block 0th-1st)
0	0	1	1	3 (4blocks, block 0th-3rd)
0	1	0	0	4 (8blocks, block 0th-7th)
0	1	0	1	5 (16blocks, block 0th-15th)
0	1	1	0	6 (32blocks, block 0th-31st)
0	1	1	1	7 (64blocks, protect all)
1	0	0	0	8 (64blocks, protect all)
1	0	0	1	9 (64blocks, protect all)
1	0	1	0	10 (64blocks, protect all)
1	0	1	1	11 (64blocks, protect all)
1	1	0	0	12 (64blocks, protect all)
1	1	0	1	13 (64blocks, protect all)
1	1	1	0	14 (64blocks, protect all)
1	1	1	1	15 (64blocks, protect all)

Figure 10: SPM table for Macronix MX25R3235F

SPM configuration value must match the content of TB and BPx bits in order to properly configure SQI flash protection. . For example, if user wants to enable flash protection for lower 1MB he must use the configuration:

- TB = 1;
- BP3 = 0;
- BP2 = 1;
- BP1 = 0;
- BP0 = 1;

SPM configuration value must be equal to: **0x15**.

5 Flash protection and XLoader

SPM feature is supported from XLoader 1.17 for TeseoII and XLoader 1.12 for TeseoIII or newer.

6 Flash protection and firmware upgrade

To start firmware upgrade process, an NMEA command called “$PSTMFWUPGRADE” must be sent to STA80xx. When this command is received by Teseo, the GNSS firmware checks if the SQI flash memory is protected. If the SQI is protected, automatically without any further command from host, Teseo sends a command to disable the protection, then the FWupgrade process continues as any other old Binary Image version. FWUpgrade procedure doesn’t change on host side.

6.1 Recovery mode support

Recovery mode is a particular feature used by TeseoII and TeseoIII Bootcodes to update the firmware without using NMEA command. A typical use case is when Teseo has been configured with a wrong NMEA baud rate and host is not able to change it according with the device. In this situation STA80xx firmware can be updated only with recovery mode.

When SQI flash protection is enabled, the Bootcode disables the protection in order to allow SQI flash upgrade. SQI flash protection is supported from Bootcode v2.8 (Included in binary 3.1.5) for TeseoII and from Bootcode v2.0.0 (included in 4.5.3 binary) for TeseoIII,

WARNING:

The bootcodes embedded in older binaries are not able to disable the flash protection then if user wants to preserve Recovery mode capability, bootcode must be updated to Bootcode v2.0.0.