Please note that Cypress is an Infineon Technologies Company.
The document following this cover page is marked as “Cypress” document as this is the company that originally developed the product. Please note that Infineon will continue to offer the product to new and existing customers as part of the Infineon product portfolio.

Continuity of document content
The fact that Infineon offers the following product as part of the Infineon product portfolio does not lead to any changes to this document. Future revisions will occur when appropriate, and any changes will be set out on the document history page.

Continuity of ordering part numbers
Infineon continues to support existing part numbers. Please continue to use the ordering part numbers listed in the datasheet for ordering.

AN220123

Protection Features of the S25FL-L Family of SPI 3.0V Flash Products

Author: Bryan Hancock

Associated Parts: S25FL256L, S25FL128L, S25FL064L

AN220123 describes the protection features in Cypress SPI Flash FL-L family of devices.

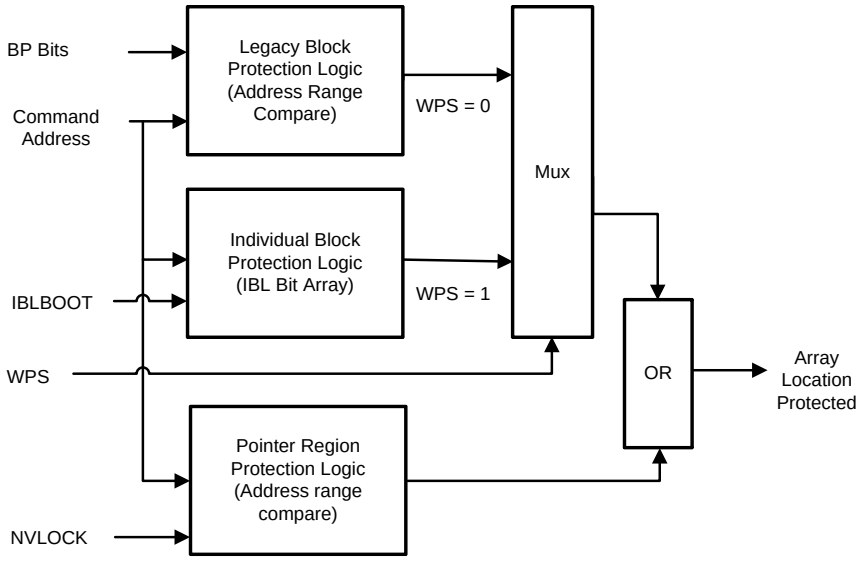
1 Introduction

Cypress S25FL-L SPI flash family of devices offers many ways to protect the data in the memory. The choices can be overwhelming to users. This document describes the protection schemes in three areas: Array Protection, Status and Configuration Register Protection, and Security Regions Protection. It describes the details of the protection, advantages and examples of use cases. It introduces different functions associated with the protection mechanisms; however, it does not go into details to explain how to implement such functions. Users may refer to the device datasheets for specific commands or registers related to these functions.

2 Array Protection

There are three types of memory array protection: Legacy Block (LBP), Individual Block Lock (IBL) and Pointer Region (PRP). The Write Protect Selection (WPS) bit is used by the user to enable one of two protection mechanisms: Legacy Block (LBP) protection (WPS = 0) or Individual Block Lock (IBL) protection (WPS = 1). Only one protection mechanism can be enabled at one time. The Legacy Block Protection is the default protection and is mutually exclusive with the IBL protection scheme. When the Pointer Region Protection is enabled, it is logically ORed with the Legacy Block Protection or Individual Block Lock protection.

Figure 1. WPS Selection of LBP or IBL and PRP Array Protection



2.1 Legacy Block Protection (LBP)

Most SPI flash devices use the same subset of core commands for backward compatibility. Within this group of legacy commands and features for data protection, Block Protection bits (BP bits), and the WP# pin are common methods of sector protection.

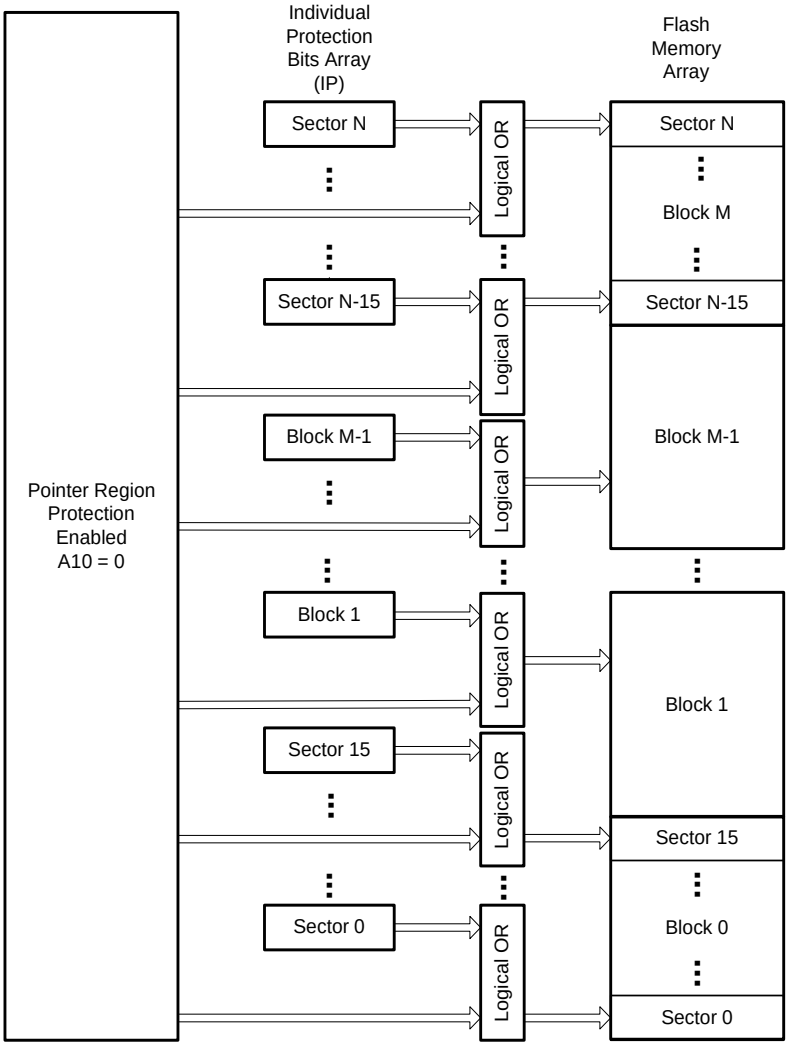
In systems where multiple flash vendors' devices are used, it may be desirable to use the commands or features that work across all devices. When it comes to protecting sectors in SPI flash, the BP bits are the common way to do it. This method allows you to protect the full array, half the array, a quarter of the array, etc. The WP# pin is also a common way to provide hardware protection.

The Cypress FL-L SPI flash family maintains this compatibility by providing the BP bits and the WP# pin.

2.2 Individual Block/Sector Lock (IBL)

Individual Block Lock (IBL) bits are volatile, with one bit for each sector / block, and each bit can be individually modified. By issuing the IBL or Global Block Lock (GBL) commands, an IBL bit is set to '0' protecting each related sector / block. By issuing IBUL or GUL commands, an IBL bit is cleared to '1' unprotecting each related sector or block. By issuing the IBLRD command, the state of each IBL bit can be read. This feature allows software to easily protect individual sectors / blocks against inadvertent changes, yet does not prevent the easy removal of protection when changes are needed. IBLs can be set or cleared as often as needed as they are volatile bits. Every main 64-KB Block and the 4-KB Sectors in bottom and top blocks has a volatile Individual Block Lock Bit (IBL) associated with it. When a sector / block IBL bit is '0', the related sector/block is protected from program and erase operations. IBL bits are volatile and protection is reset after a power on or reset occurs.

Figure 2. Individual Block Lock / Pointer Region Protection Control

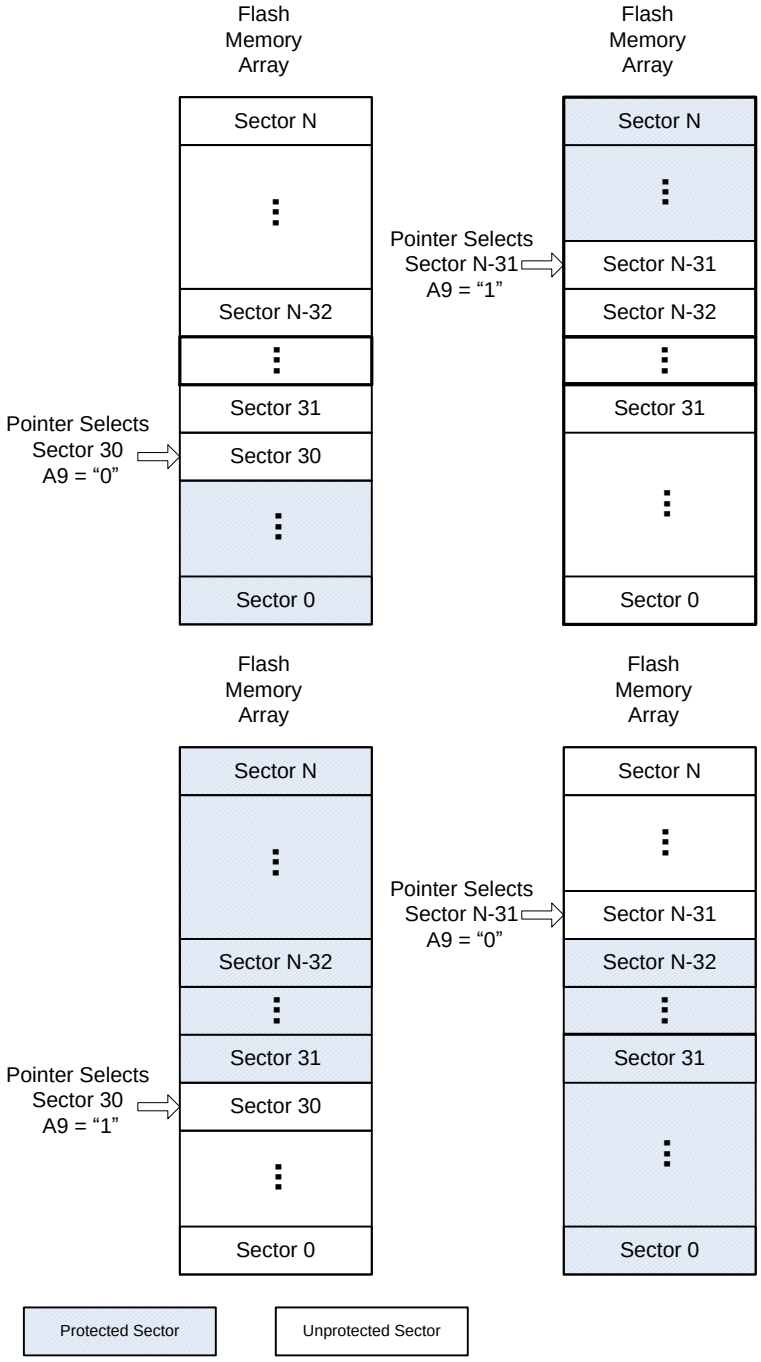


Notes;
1. The "M" is the top 64KB Block.
2. The "N is the top 4KB Sector.

2.3 Pointer Region Protection (PRP)

Pointer Region Protection is defined by a nonvolatile address pointer that selects any 4-KB sector as the boundary between protected and unprotected regions in the memory. PRP settings can also be protected from modification until the next power cycle or a password is supplied, or can be permanently locked. PRP can be used in combination with either the Legacy Block Protection or Individual Block Lock protection methods. When enabled, PRP protection is logically ORed with the protection method selected by the WPS bit (CR2V[2]). This provides a protection scheme with individual sector granularity that remains in effect across power cycles and reset operations.

Figure 3. Pointer Region Protection Examples



3 Status Register Protect (SRP)

Status Register Protect (SRP) places the device in Hardware Protected mode. In this mode, any command that change status registers or configuration registers are ignored and not accepted for execution, effectively locking the state of the Status Registers and Configuration Registers.

Status Register Protect bits (SRP1 and SRP0) are volatile bits in the configuration and status registers (CR1V[0] and SR1V[7]). The SRP bits control the method of write protection for SR1NV, SR1V, CR1NV, CR1V, CR2NV, CR2V, CR3NV, DLRNV and DLRV: software protection, hardware protection, power supply lock-down or permanent protection.

Table 1. Status Register Protection Bits

SRP1_D CR1NV[0]	SRP1 CR1V[0]	SRP0 SR1V[7]	WP#	Status Register	Description
0	0	0	X	Software Protection	WP# pin has no control. SR1NV, SR1V, CR1NV, CR1V, CR2NV, CR2V, CR3NV, DLRNV and DLRV can be written. [Factory Default]
0	0	1	0	Hardware Protected	When WP# pin is low SR1NV, SR1V, CR1NV, CR1V, CR2NV, CR2V, CR3NV, DLRNV and DLRV are locked and cannot be written.
0	0	1	1	Hardware Unprotected	When WP# pin is high SR1NV, SR1V, CR1NV, CR1V, CR2NV, CR2V, CR3NV, DLRNV and DLRV are unlocked and can be written.
0	1	X	X	Power Supply Lock-Down	SR1NV, SR1V, CR1NV, CR1V, CR2NV, CR2V, CR3NV, DLRNV and DLRV are protected and cannot be written to again until the next power-down, power-up cycle.
1	1	X	X	Permanent Protection One Time Program	SRP1_D CR1NV[0] = 1 SR1NV, SR1V, CR1NV, CR1V, CR2NV, CR2V, CR3NV, DLRNV and DLRV are permanently protected and cannot be written. When SRP1_D CR1NV[0] = '1' a power-down, power-up cycle, or hardware reset, will reload SRP1 from SRP1_D = '1' the volatile bit SRP1 is not writable, thus providing OTP protection.

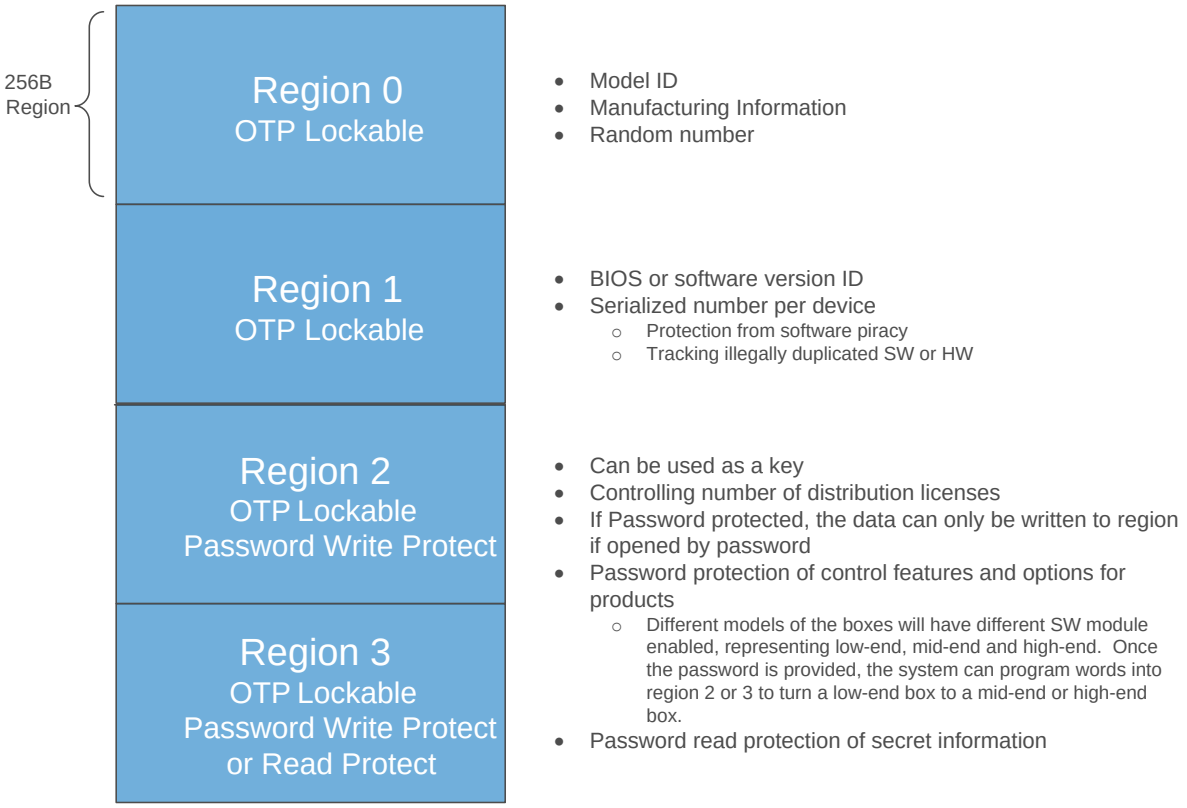
4 Security Regions Protection

The device has a 1024-byte address space that is separate from the main flash array. This area is divided into four individually lockable, 256-byte length regions. The Security Region memory space is intended for increased system security. The data values can 'mate' a flash component with the system CPU/ASIC to prevent device substitution. The Security Region address space is protected by the Security Region Lock bits or the Protection Register or Password Protection. Regions 2 and 3 also have temporary protection from program or erase by the Protection Register (PR) NVLOCK bit. The Security Region Password Protection Bit in the Individual and Region Protection (IRP) Register (IRP[2]) allows Regions 2 and 3 to be protected from Program and Erase operations until a password is provided. The Security Region Read Protection Bit in the IRP Register allows Region 3 to also be protected from Read operations until a password is provided.

4.1 Security Region Lock Bits (LB3, LB2, LB1, LB0)

The Security Region Lock Bits (LB3, LB2, LB1, LB0) are non-volatile One Time Program (OTP) bits in Configuration Register 1(CR1NV[5:2]) that provide the write protect control and status to the Security Regions. The default state of Security Regions 0 to 3 are unlocked. LB[3:0] can be set to 1 individually using the Write Status Registers or Write Any Register command. LB[3:0] are One Time Programmable (OTP), once it's set to '1', the corresponding 256 512 Byte Security Region will become read-only permanently. This enables permanent protection from programming and erasure of the corresponding Security Region. This will secure code or data from inadvertent or malicious changes.

Figure 4. Security Regions Use Cases



5 Individual and Region Protection Functions

Individual and Region Protection (IRP) is the name used for a set of independent hardware and software methods used to disable or enable programming or erase operations or password protection on Security Regions 2 and 3 and the Pointer Region Protection register. Security Regions 2 and 3 are also protected respectively by LB2 or LB3=1 (CR1NV[4:5]). The selection of the method of protection is by the Individual and Region Protection register (IRP) bits PERMLB IRP[0], PSLMLB IRP[1] and PWDMLB IRP[2].

Each method is managed the NVLOCK bit. When NVLOCK =1, the Security Regions 2 and 3 and the Pointer Region Protection Register (PRPR) may be programmed and erased. When NVLOCK =0, the Security Regions 2 and 3 and PRPR cannot be programmed or erased. An overview of all methods is shown in Figure 5.

5.1 Default Lock Protection IRP [2, 1, 0] = [1, 1, 1]

Lock protection is the default method. This method sets the NVLOCK bit to '1' during POR or Hardware Reset so that the NVLOCK-related areas and registers are unprotected by a device reset. The PRL (A6h) command clears the NVLOCK bit to '0' to protect the NVLOCK related areas and registers. There is no command in the Power Supply Lock-down method to set the NVLOCK bit to '1', therefore the NVLOCK bit will remain at '0' until the next power off or hardware reset. The Default Lock Protection method allows the boot code the option of changing Security Regions 2 and 3 or the value in PRPR, by programming or erasing these nonvolatile areas, then protecting these nonvolatile areas from further change for the remainder of normal system operation by clearing the NVLOCK bit to '0'. This is sometimes called boot-code controlled protection, because after power up, protection is controlled by the boot code.

5.2 Power Supply Lock-down Protection IRP [2, 1, 0] = [1, 0, 1]

The Power Supply Lock-down method permanently locks the device in Default Lock Protection mode. After Power Supply Lock-down Protection mode is selected by programming IRP[1] = '0', the state of all IRP bits are locked and permanently protected from further programming. This protects the device from being changed to unwanted modes of operation.

5.3 Permanent Protection IRP[2, 0] = [1, 0]

The Permanent Protection method permanently sets the SECRRP bit = '1' and clears NVLOCK to '0'. This permanently protects the Security Regions 2 and 3 and PRPR. The selection of the NVLOCK bit management method is made by programming OTP bits in the IRP Register (IRP[2 or 1 or 0] so as to permanently select the method used. This is used to permanently protect memory and Security regions 2 and 3 from malicious changes.

5.4 Password Protection IRP[6, 2] = [1 , 0]

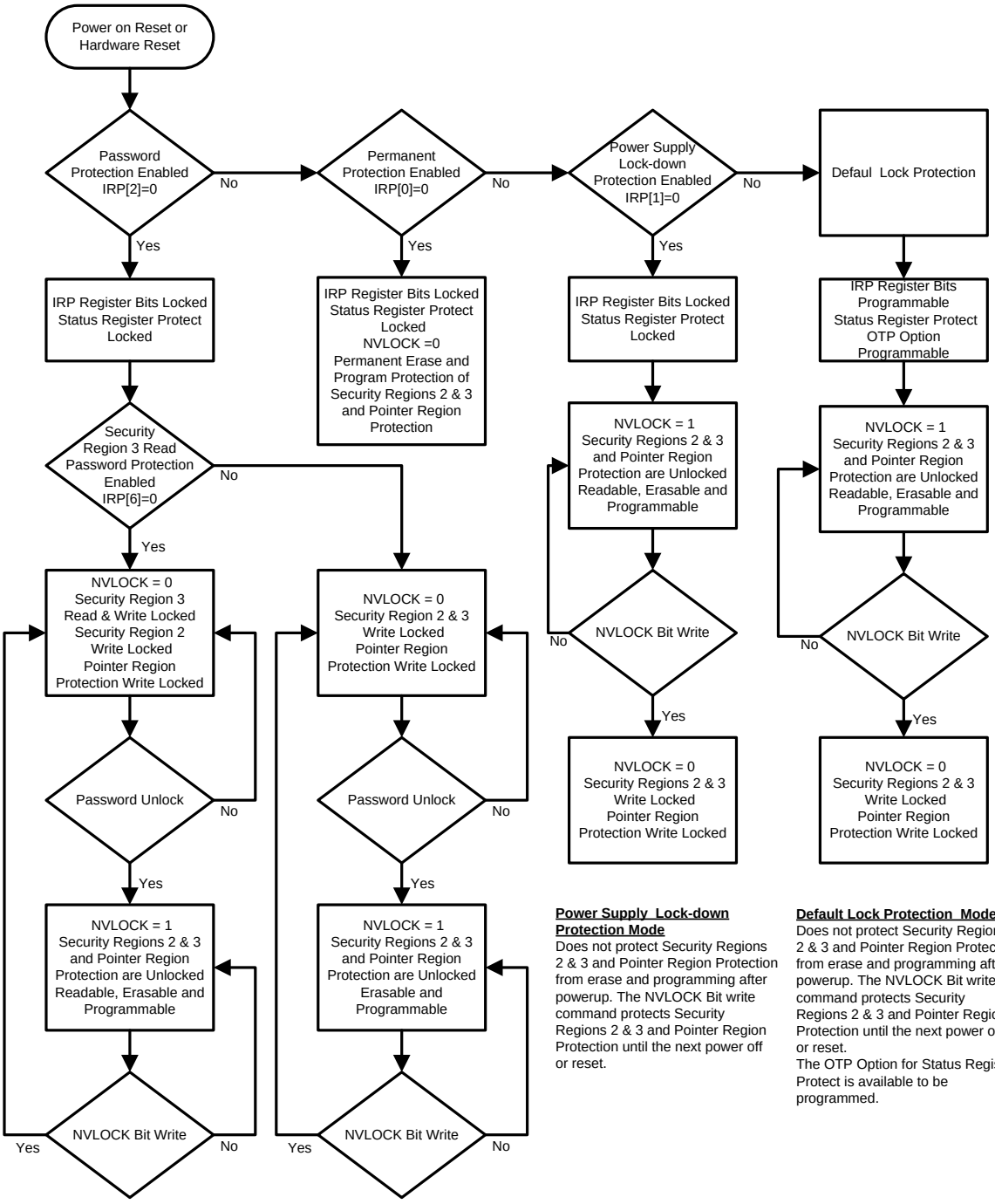
The Password Protection method allows an even higher level of security than Power Supply Lock-down protection mode, by requiring a 64-bit password for unlocking the NVLOCK bit. In addition to this password requirement, after power up or hardware reset, the NVLOCK bit is cleared to '0' to ensure protection after power-up or reset. Successful execution of the Password Unlock command by entering the entire password sets the NVLOCK bit to '1', allowing modifications for NVLOCK-related protected Pointer region and Security region 2 and 3.

- 64-bit, one-time programmable password is defined and programmed by user; once programmed, the password cannot be read or changed. The Password Program (PASSP) and Read (PASSRD) commands are used to set and verify the password. Once the Password is programmed and verified the Password mode (IRP[2] is set to '0' in order to prevent future programming or reading of the password.
- Password Unlock command (PASSU) is used to enter the password to unlock the device.
- Protection Register Lock command resets the NVLOCK bit to '0' to lock the device again.

5.5 Read Password Protection Security Region 3 IRP[6, 2] = [0 , 0]

The Security Region Read Password Protection method enables protecting Security Region 3 from read, program, and erase. Security Region Read Password Protection is an optional addition to Password Protection mode (described above).

Figure 5. Permanent, Password and Power Supply Lock-down Protection Overview



Power Supply Lock-down Protection Mode
Does not protect Security Regions 2 & 3 and Pointer Region Protection from erase and programming after powerup. The NVLOCK Bit write command protects Security Regions 2 & 3 and Pointer Region Protection until the next power off or reset.

Default Lock Protection Mode
Does not protect Security Regions 2 & 3 and Pointer Region Protection from erase and programming after powerup. The NVLOCK Bit write command protects Security Regions 2 & 3 and Pointer Region Protection until the next power off or reset.
The OTP Option for Status Register Protect is available to be programmed.

Read Password Protection Mode
Protects Security Regions 3 from Read, Erase and Programming, Security Region 2 and Pointer Region Protection from erase and programming after powerup. A password unlock Command will enable changes to Security Region 2 & 3 and Pointer Region Protection. A NVLOCK bit write command turns the protection back on.

Password Protection Mode
Protects Security Regions 2 & 3 and Pointer Region Protection from erase and programming after powerup. A password unlock Command will enable changes to Security Region 2 & 3 and Pointer Region Protection. A NVLOCK bit write command turns the protection back on.

Permanent Protection Mode
Permanently protects Security Regions 2 & 3 and Pointer Region Protection from Erase and Programming

Note
If Security Region Lock bits LB 2 & 3 are protected CR1NV[5:4]=1, this overrides the NVLOCK and the Security Regions protected by the LB bits will be permanently protected from erase and programming. If Read Password is enabled Security Region 3 can still be read password protected.

6 Summary

Cypress SPI S25FL-L family of devices offers three types of memory array protection: Legacy Block (LBP), Individual Block Lock (IBL) and Pointer Region (PRP) features that can be used to protect data in different levels. IBL protection provides an easy, quick protection to any sectors in the device. PRP protection provides a nonvolatile protection to any sectors region. Users can also use the Status Register Protect (SRP) to protect the configuration of the device from malicious changes. Security Regions can be protected by Lock Bits and Password, enabling the device to be configured for unique product use cases and protected from end-user manipulation. Password Protection, Persistent Protection, or Power Supply Lock-down modes alter the power-on behavior of the NVLOCK bit. Refer to the specific datasheet for operational details.

7 References

- Cypress S25FL256L, S25FL128L Datasheet, Publication Number 002-00124
- Cypress S25FL064L Datasheet, Publication Number 002-12878

Document History

Document Title: AN220123 – Protection Features of the S25FL-L Family of SPI 3.0V Flash Products

Document Number: 002-20123

Revision	ECN	Orig. of Change	Submission Date	Description of Change
**	5896047	BWHA	09/26/2017	Initial version

Worldwide Sales and Design Support

Cypress maintains a worldwide network of offices, solution centers, manufacturer's representatives, and distributors. To find the office closest to you, visit us at Cypress Locations.

Products

ARM® Cortex® Microcontrollers	cypress.com/arm
Automotive	cypress.com/automotive
Clocks & Buffers	cypress.com/clocks
Interface	cypress.com/interface
Internet of Things	cypress.com/iot
Memory	cypress.com/memory
Microcontrollers	cypress.com/mcu
PSoC	cypress.com/psoc
Power Management ICs	cypress.com/pmic
Touch Sensing	cypress.com/touch
USB Controllers	cypress.com/usb
Wireless Connectivity	cypress.com/wireless

PSoC® Solutions

PSoC 1 | PSoC 3 | PSoC 4 | PSoC 5LP | PSoC 6

Cypress Developer Community

Forums | WICED IOT Forums | Projects | Videos | Blogs | Training | Components

Technical Support

cypress.com/support

Cypress Semiconductor
198 Champion Court
San Jose, CA 95134-1709