Data Security in SkyHigh S34ML-3 SLC NAND

Author: Zhi Feng

Associated Part Families: S34ML-3

AN219542 summarizes the data security features in SkyHigh S34ML-3 SLC NAND flash family.

1 Introduction

Compared to traditional NAND devices, SkyHigh S34ML-3 SLC NAND flash family provides additional data security features that help users achieve higher levels of security. This document summarizes these features and provides use case scenarios to help users in their system and software implementation efforts.

2 Overview of Security Features in S34ML-3 SLC NAND

NAND security features provide data protection in the flash memory array by disallowing program and erase operations in the protected blocks. Reading data from the array is not affected by the security features.

- WP# pin protection
  Just like all traditional NAND memories, S34ML-3 provides hardware protection via the WP# pin. This is an All-or-None protection. When WP# pin is asserted LOW, no program or erase operations can be done to the entire device.
- Volatile Block Protection (VBP)
  This method allows the user to protect a range of blocks during a power-on period. The protection status will be reset at the next power-on reset (POR).
- Permanent Block Protection (PBP)
  This method allows the user to permanently protect certain groups of blocks. Once a group of blocks is protected, it can no longer be unprotected.

These three features provide data protection independently. A flash memory block can be protected by one of these three methods.

The following sections introduce these security features in more details.

3 Legacy WP# Pin Protection

WP# pin can be used to protect all blocks in the device. It provides an All-or-None protection. When WP# pin is asserted LOW, no program or erase commands are accepted.

This feature is useful if the user wants to protect the entire device. When a program or an erase operation is needed, you must de-assert WP# to HIGH state (V_{IH}).

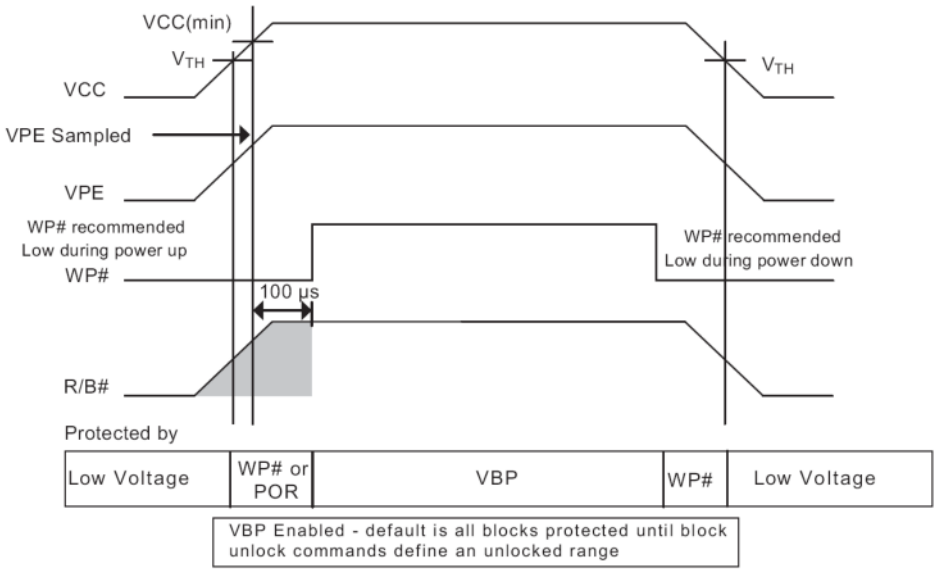
In S34ML-3 devices, WP# pin can be also used to reset VBP. If a VBP lock-down command has not been issued, and if WP# pin is asserted for at least 100 ns, the VBP feature is reset back to the power-on state, i.e., all blocks are protected.

4 Volatile Block Protection (VBP)

The VBP feature can be used to protect all or selected range of contiguous blocks.

To enable the VBP feature, the Volatile Protection Enable (VPE) hardware pin needs to be at HIGH state (V_{IH}) during the power-on period. The following figure shows the sampling point of VPE during power ON.

Figure 1. VPE HIGH at Power-Up Timing



Notes:

1. *V_{TH} = 1.8 Volts (Typ)*
2. *The VPE pin must be sampled between V_{TH} and V_{CC} (min).*
3. *During power up, VCC and VPE slopes are equal.*

When the VBP feature is enabled, after power-on, it is reset to its initial state, i.e., all blocks are protected.

There are four commands that are associated with the VBP feature:

- Unlock Lower (23h)
- Unlock Upper (24h)
- Lock-all (2Ah)
- Lock-down (2Ch)

Unlock Lower must always precede the Unlock Upper command. These two commands set up the lower and upper boundary addresses of the selected block range.

The 3-byte address cycle used in these two commands has the format listed in Table 1:

Table 1. Address Cycle Definitions of Unlock Lower/Upper Commands

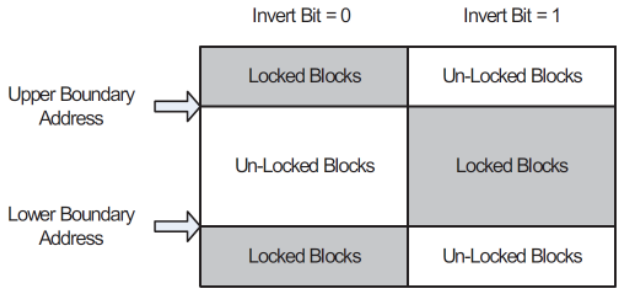
Address Cycle Mapping									
	Bus Cycle	IO[7]	IO[6]	IO[5]	IO[4]	IO[3]	IO[2]	IO[1]	IO[0]
Row Address 1	1st	BA[1]	BA[0]	L	L	L	L	L	Invert Bit (Upper cmd only)
Row Address 2	2nd	BA[9]	BA[8]	BA[7]	BA[6]	BA[5]	BA[4]	BA[3]	BA[2]
Row Address 3	3rd	L	L	L	L	L	L	BA[11]	BA[10]

Notes:

1. BA[0] controls plane selection

The Invert Bit is ignored in the Unlock Lower command. It is used in the Unlock Upper command to control the protection status of the selected range of blocks:

Figure 2. Unlock Range Option



Once the block range is set up, the VBP protection status is valid until the next power cycle. To change the range, a Lock-all (2Ah) command can be issued to reset the range first; then the Unlock Lower and Unlock Upper commands can be used to enter the new range.

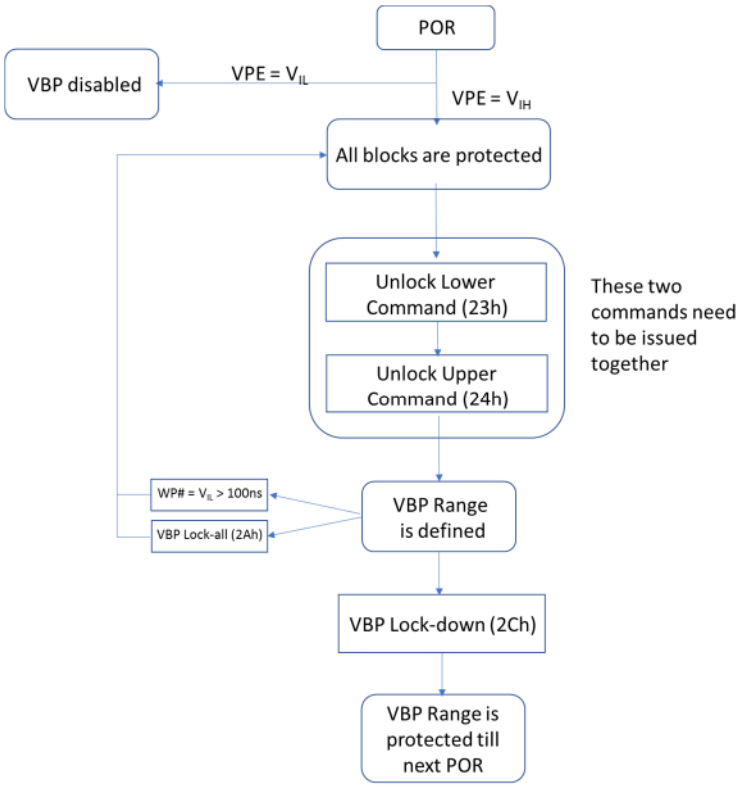
Toggling the WP# pin for at least 100 ns has the same effect as the Lock-all command. It resets the VBP feature; a new range can be entered afterwards.

If you are satisfied with the VBP protection range and do not want it to be altered until the next power cycle, you can issue a Lock-down (2Ch) command. Once the Lock-down command is entered, the current protection range will not be reset by the WP# pin or Lock-all command until the next power cycle.

Lock-all and Lock-down commands have no address cycles.

Figure 3 shows the flow of the VBP feature:

Figure 3. VBP Feature Flowchart



In dual-plane devices, due to the interleaving internal block structure, blocks are arranged in pairs. It means that if Block 1 is defined to be the lower boundary address, Block 0 will also be protected. This is the same as for the upper boundary address: if Block 8 is defined to be the upper boundary, Block 9 will also be protected. You will need to be aware of such internal relationship between blocks. For example, if the lower and upper boundaries are set up to be Block 1 to Block 4, in a single-plane device, the VBP protection range is from Block 1 to Block 4, both included. In a dual-plane device, the range is from Block 0 to Block 5, both included.

Some use case examples are as follows:

Set up VBP protection from Block 2 to Block 20

1. Power up the device with VBE HIGH to enable VBP.
2. Issue the Unlock Lower command with Block 2 address.
3. Issue the Unlock Upper command with Block 20 address and Invert Bit=1.
4. Issue the Lock-down command if such protection range is not intended to change.

Set up VBP protection for all blocks except Block 5 to Block 15

1. Power up the device with VBE HIGH to enable VBP.
2. Issue the Unlock Lower command with Block 5 address.
3. Issue the Unlock Upper command with Block 15 address and Invert Bit=0.
4. Issue the Lock-down command if such protection range is not intended to change.

Expand VBP protection from Range Block 2 - Block 20, to Range Block 2 – Block 40

1. Issue the Lock-all command.
2. Issue the Unlock Lower command with Block 2 address.
3. Issue the Unlock Upper command with Block 40 address and Invert Bit=1.

5 Permanent Block Protection (PBP)

In some use cases, certain blocks in the memory may need to be protected permanently. The PBP feature provides such capability for the first 64 blocks of the device. The first 64 blocks are arranged in sequence in 16 groups of 4 blocks each. Each group then can be protected individually by the PBP feature.

Because the PBP function is irreversible, the PBP command is constructed in a complex way to prevent inadvertent access. Table 2 summarizes the command format:

Table 2. Command Sequence of PBP Command

Entry Sequence				CMD Cycle	Address Cycles					CMD Cycle	Wait or Check Status	Exit CMD
4Ch	03h	1Dh	41h	80h	00h	00h	00h	0Yh	00h	10h	Monitor R/B# pin or use Status Read command (70h/78h)	FFh

'Y' is the group address value. Because there are total 16 groups, Y is range from 0 to Fh.

For 1-Gb devices, the 5th address cycle may be omitted. If entered, it will be ignored.

After this command sequence is entered, the corresponding group will be protected permanently. It cannot be unprotected. If another group needs to be protected, a new command sequence with different Address 'Y' can be entered again.

Note that the Exit command, FFh, is necessary to exit the command sequence. If during the busy time after the 10h command, a power OFF or Reset command occurs, the PBP function cannot be guaranteed.

If you are satisfied with the current PBP protection scheme and no longer want to change it, you can issue a PBP Lock-down (PBPLDL). Once the lock-down command is entered, the PBP command will not be accepted, i.e., no more changes to the PBP protection scheme.

Table 3 summarizes the PBPLDL command format:

Table 3. Command Sequence of PBPLDL Command

Entry Sequence				CMD Cycle	Address Cycles					CMD Cycle	Wait or Check Status	Exit CMD
4Ch	03h	1Dh	41h	80h	00h	00h	00h	1Yh	00h	10h	Monitor R/B# pin or use Status Read command (70h/78h)	FFh

The value of the 4th address cycle determines whether it is a PBPLDL command or a PBP command. Note that the PBPLDL command also protects the 'Y' group, and then permanently locks down the protection scheme. You can choose an already protected group as the 'Y' address if no additional group needs protection. It is not possible to lock down the PBP scheme without protecting any group.

Because the PBP and PBPLDL commands are irreversible, you must be extra cautious when implementing software to execute these commands.

6 Protection Status Read Command (7Ah)

S34ML-3 devices provide a Protection Status Read command, 7Ah, to read the protection status of a particular block, by reading the Block Lock Status Register.

To read the Block Lock Status Register, issue command 7Ah followed by three row address cycles with the block address. The device outputs the 1-byte Status Register value.

Table 4. Command Sequence of Protection Status Read Command

CMD Cycle	Address Cycles			Output Status
7Ah	Row Address 1	Row Address 2	Row Address 3	Bit7-0

Table 5 lists the details of the 3-byte address cycles:

Table 5. Address Cycle Definitions of Protection Status Read Command

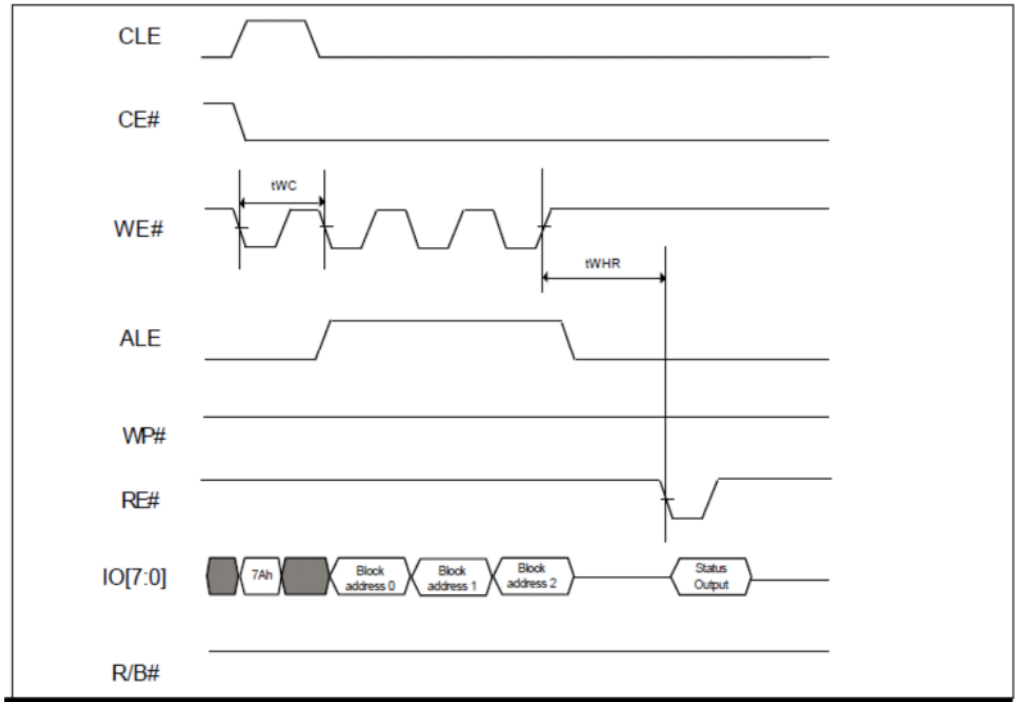
Address Cycle Mapping									
	Bus Cycle	IO[7]	IO[6]	IO[5]	IO[4]	IO[3]	IO[2]	IO[1]	IO[0]
Row Address 1	1st	BA[1]	BA[0]	L	L	L	L	L	L
Row Address 2	2nd	BA[9]	BA[8]	BA[7]	BA[6]	BA[5]	BA[4]	BA[3]	BA[2]
Row Address 3	3rd	L	L	L	L	L	L	BA[11]	BA[10]

Notes:

1. BA[0] controls plane selection

Figure 4 shows the timing information for the Protection Status Read command:

Figure 4. Protection Status Read Command Timing



The Block Lock Status Register indicates whether the block is protected or not protected by VBP or PBP, or if VBP Lock-down has been issued. Table 6 has the bit descriptions:

Table 6. Definitions of Block Lock Status Register

Bits	Field Name	Default Value	Description
7	Reserved	0	
6	Reserved	0	
5	Reserved	0	
4	PBP Lock Down Status	0	0: The PBP block range is not locked down by PBP 1: The PBP block range is locked down by PBP
3	Permanent Block Protect	1	0: The address selected block is locked by PBP 1: The address selected block is unlocked by PBP
2	VBP Block-unlock	1	0: The address selected block is locked by VBP 1: The address selected block is unlocked by VBP
1	VBP Not Locked-down	1	0: The VBP block range is locked down 1: The VBP block range is not locked down
0	VBP Locked-down	0	0: The VBP block range is not locked down 1: The VBP block range is locked down

Note that Bit[0] and Bit[1] of the register are complementary in their definitions so their value should never be the same. This is to add extra reliability in reading the register.

Also note that the Block Lock Status Register does not indicate whether the device is protected by the hardware WP# pin or not. It only indicates the status for the VBP and PBP functions.

7 Summary

SkyHigh S34ML-3 SLC NAND flash family devices provide different levels of data security functions for users to choose according to their specific application needs. The Volatile Block Protection (VBP) provides an easy, quick protection to any blocks in the device. The Permanent Block Protection (PBP) provides a non-reversible protection scheme that cannot be altered.

8 References

- SkyHigh S34ML04G3 4Gb, 3V, 2K Page Size, x8 I/O, SLC NAND Flash Memory For Embedded, Datasheet, Publication Number 002-19204
- SkyHigh S34ML04G3 4Gb, 3V, 4K Page Size, x8 I/O, SLC NAND Flash Memory For Embedded Datasheet, Publication Number 002-19822

Document History

Document Title: AN219542 - Data Security in SkyHigh S34ML-3 SLC NAND

Document Number: 002-19542

Revision	ECN	Orig. of Change	Submission Date	Description of Change
**	5777693	ZHFE	06/19/2017	New application note
*A	5968576	ZHFE	11/16/2017	Minor revision based on datasheet changes
*B		MNAD	05/02/2019	Updated to SkyHigh format