How to use the software write protection register in CMOSF9V EEPROM products

Introduction

The purpose of this technical note is to provide guidelines on the usage of the software write protection for the products listed in Table 1.

New high density of EEPROM (electrically erasable programmable read-only memory) devices are manufactured with new advanced CMOSF9V technology. They offer low power consumption, footprint optimization, configurable device address, and software write protection.

To protect the EEPROM against unwanted write operations, the EEPROM in CMOSF9V has a dual protection mechanism. One by hardware with the /WC pin and one by software using the software write protection register (SWP).

This technical note describes the software protection mechanism and how to set up the SWP register to protect partially or fully the memory.

Table 1. Applicable products

Series	RPN
Standard serial EEPROM	M24256X-F
	M24512E-F, M24512X-F
	M24M01E-F, M24M01X-F
	M24M02E-F, M24M02X-F

1 Software write protection (SWP)

1.1 SWP register description

The software write protection (SWP) register is a non-volatile 8-bit register. It allows the user to protect a specific area of memory from write access. By setting the required software write protection bits, the register can be permanently locked to prevent further changes to the device operation.

The SWP has four non-volatile bits for user configuration:

- Two bits for setting the size of the write-protected memory. These are identified as block protection bits (BP0, BP1).
- One bit that enables / disables the write protection of the desired area. This is identified as write protect activation (WPA) bit.
- One bit to permanently lock the SWP register in read-only mode. It is identified as the write protection lock (WPL) bit.

Table 2 describes the software write protection register:

Table 2. Software write protection register

bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0
x(1)	x	x	x	WPA	BP1	BP0	WPL

1. *x = Don't care. Read as 0*

1.2 SWP register management

On power-up, the device loads the last configuration of the SWP register value.

This register can be read and written using the software write-protect register instructions.

The user can update the SWP register as long as the WPL bit remains to 0.

With the WPL bit set-up to 0, the user can update the WPA, BP1, and WPL bits as required.

After the SWP set-up, the SWP register can be definitively frozen in read-only mode, by setting the WPL bit to 1.

As soon as WPL bit is set to 1, the SWP update is no more possible. It becomes permanently frozen.

1.3 Write protection block

The EEPROM array is not write-protected if the WPA bit is set to 0. See Table 3.

The EEPROM array is write-protected in accordance with the BP1, BP0 bits values if the WPA bit is set to 1.

As shown in Table 3, the combination of BP1, BP0 bits provides four different protection schemes for the device.

Table 3. Write protection block scheme

Protection block	WPA	BP1	BP0
Upper quarter	1	0	0
Upper half	1	0	1
Upper ¾	1	1	0
Whole memory	1	1	1
None	0	x	x

Note: x = Don't care

2 Protected address range

The user sets the SWP register bits to obtain four different write protection schemes as described in Table 3.

The protected address range depends on the memory array size and the block protection scheme set by the user. See Table 4.

Table 4. Protected address range versus densities

Protections scheme	Protected address range by density (in hex)			
	256 Kbit	512 Kbit	1 Mbit	2 Mbit
Upper quarter	6000h-07FFh	C000h-FFFFh	18000h-1FFFFh	30000h-3FFFFh
Upper half	4000h-07FFh	8000h-FFFFh	10000h-1FFFFh	20000h-3FFFFh
Upper ¾	2000h-07FFh	4000h-FFFFh	8000h-1FFFFh	10000h-3FFFFh
Whole memory	0000h-07FFh	0000h-FFFFh	0000h-1FFFFh	0000h-3FFFFh

3 Conclusion

The software protection mechanism allows the user to set-up the software write protection register at any time and via software.

Four locked protection zones can be configured within the memory array.

A flexibility is also given to the user to lock/unlock the zone and lock permanently the software register.

With such solution, the users can easily protect sensitive data or one-time programmable parameters during the application lifetime and protect data against unwanted changes.

Revision history

Table 5. **Document revision history**

Date	Version	Changes
07-Feb-2024	1	Initial release.

Contents

List of tables