AN4254

在 24CS 系列串行 EEPROM 中使用增强软件写保护功能

作者： *Erik Fasnacht*
Microchip Technology Inc.

简介

传统的 I^2C 串行 EEPROM 采用基于硬件的写保护，只允许通过外部引脚锁定或解锁整个存储器阵列，从而严重限制了可实现的数据保护方式。为解决这一限制问题，24CS 系列器件新增了 16 位配置寄存器，该寄存器允许将写保护特性配置为传统的硬件写保护或增强的软件写保护。

传统的硬件写保护采用写保护（Write Protection，WP）引脚，在 WP 引脚为 “1” 时，对整个存储器阵列进行写保护。顾名思义，传统的写保护模式作用与标准的 I^2C 串行 EEPROM 相同。然而，当今的许多应用都可以从更灵活的数据保护管理中受益。对于这些应用， 24CS 提供了利用增强软件写保护的选项，可将存储器阵列分为八个区，每个区都可以单独设置为写保护。这种新增的灵活性允许 24CS 系列器件根据应用需要提供更细粒度的数据保护。

所需的写保护设置可通过配置寄存器进行设置，而配置寄存器可通过向特定器件地址和字地址发送命令的方式访问。如果需要，可锁定配置寄存器，这样可以将其设置为只读，且不能再进行修改，从而使当前的数据保护方案永久生效。本应用笔记用于演示如何在应用中利用 16 位配置寄存器设置数据保护。

配置寄存器字节 0

配置寄存器格式和最高有效字节（Most Significant Byte， MSB）的位定义请参见寄存器 1。该字节包含状态信息以及用于设置当前写保护特性和锁定配置寄存器的位。

寄存器 1： 配置寄存器 —— 字节 0

R-0	U-0	U-0	U-0	U-0	U-0	R/W	R/W
ECS	—	—	—	—	—	EWPM	LOCK
bit 15							bit 8

图注：			
R = 可读位	W = 可写位	U = 未实现位，读为 0	
-n = POR 时的值	1 = 置 1	0 = 清零	x = 未知

bit 15 **ECS**：错误校正状态位
1 = 之前已执行的读操作确实需要使用纠错码 （Error Correction Code， ECC）方案
0 = 之前已执行的读操作不需要使用纠错码 （ECC）方案

bit 14-10 **未实现**：读为 0

bit 9 **EWPM**：增强软件写保护模式位
1 = 增强保护：WP 引脚将被视为“无关项”，而存储器阵列则按照寄存器 2 中定义的 SWP 位进行保护
0 = 传统的保护功能 （出厂默认设置）：整个存储器阵列和安全寄存器内容通过 WP 引脚进行保护

bit 8 **LOCK**：锁定配置寄存器位
1 = 配置寄存器设置为只读 （永久）
0 = 可对配置寄存器进行写操作 （出厂默认设置）

错误校正状态（ERROR CORRECTION STATE，ECS）位

当用户需要确定是否调用了片上纠错码（ECC）逻辑方案时，使用此位。 ECS 位将置为逻辑 “0”，除非之前已执行的读操作需要使用 ECC 逻辑方案。出现这种情况时，ECS 位将置为逻辑 “1”。ECS 位将继续读取逻辑 “1”，直至发出了另一个读操作，且不需要使用 ECC 逻辑方案或发生上电复位 （Power-On Reset， POR）事件。

增强软件写保护模式（ENHANCED SOFTWARE WRITE PROTECTION MODE， EWPM）位

此位用于在传统的硬件写保护模式 （逻辑 “0” ）和增强的软件写保护模式 （逻辑 “1” ）之间切换选择。传统的硬件写保护模式支持通过 WP 引脚对整个存储器阵列进行写保护。

增强的软件写保护模式为软件写保护功能，在此模式下，存储器阵列被分为八个单独区域。每个区都是独立的，并使用 SWP[7:0] 位进行配置 （寄存器 2）。

传统的写保护模式

当 EWPM 位置为逻辑 “0” 时， 24CS 系列采用传统的硬件数据保护方案，该方案允许用户在 WP 引脚置为有效（高）时对整个存储器内容进行写保护。如果 WP 引脚置为无效 （低），则不会设置写保护。

表 1： 传统的硬件写保护特性

WP 引脚	受保护地址范围
1 （高）	整个阵列
0 （低）	无

增强软件写保护模式

当 EWPM 位置为逻辑 “1” 时，通过将 EEPROM 阵列划分为八个独立区域，从而将 24CS 系列配置为多功能软件写保护方案。通过编程配置寄存器中的相应位（见寄存器 2），可对这八个区域的每个区域进行写保护。通过锁定配置寄存器，可将保护方案设置为永久。

锁定配置寄存器 （LOCK CONFIGURATION REGISTER， LOCK）位

此位允许用户通过将配置寄存器设置为只读，从而锁定配置寄存器，这样就不能再对其进行修改。当 LOCK 位置为逻辑 “1” 时， 当前数据保护方案则为永久。

配置寄存器字节 1

配置寄存器格式和最低有效字节 （Least Significant Byte，LSB）的位定义请参见寄存器 2。此字节包含八个独立的软件写保护存储区 （SWP[7:0]）位。

寄存器 2： 配置寄存器 —— 字节 1

R/W	R/W	R/W	R/W	R/W	R/W	R/W	R/W
SWP7	SWP6	SWP5	SWP4	SWP3	SWP2	SWP1	SWP0
bit 7							bit 0

图注：			
R = 可读位	W = 可写位	U = 未实现位，读为 0	
-n = POR 时的值	1 = 置 1	0 = 清零	x = 未知

如果 EWPM = 1：

bit 7 **SWP7：** 软件写保护存储区 7 位
1 = 对存储区 7 进行写保护
0 = 未对存储区 7 进行写保护

bit 6 **SWP6：** 软件写保护存储区 6 位
1 = 对存储区 6 进行写保护
0 = 未对存储区 6 进行写保护

bit 5 **SWP5：** 软件写保护存储区 5 位
1 = 对存储区 5 进行写保护
0 = 未对存储区 5 进行写保护

bit 4 **SWP4：** 软件写保护存储区 4 位
1 = 对存储区 4 进行写保护
0 = 未对存储区 4 进行写保护

bit 3 **SWP3：** 软件写保护存储区 3 位
1 = 对存储区 3 进行写保护
0 = 未对存储区 3 进行写保护

bit 2 **SWP2：** 软件写保护存储区 2 位
1 = 对存储区 2 进行写保护
0 = 未对存储区 2 进行写保护

bit 1 **SWP1：** 软件写保护存储区 1 位
1 = 对存储区 1 进行写保护
0 = 未对存储区 1 进行写保护

bit 0 **SWP0：** 软件写保护存储区 0 位
1 = 对存储区 0 进行写保护
0 = 未对存储区 0 进行写保护

如果 EWPM = 0：

bit 7-0 未使用

软件写保护存储区 （SWP[7:0]）位

这些位将存储器阵列分为八个单独区域。每个区可独立于其他保护区进行单独设置。要对某个区进行写保护，就必须将相应 SWP 位置为逻辑 “1”。

注： 在传统的硬件写保护模式下（EWPM = “0”），SWP[7:0] 位将被忽略。但是，在写操作序列期间仍必须发送一个虚拟值，以启动内部写操作。

访问寄存器

配置寄存器的值可通过对特定字地址执行随机读操作序列来确定。更改配置寄存器的值可通过字节写操作序列完成，同时将特定数据发送至器件。

器件地址要求

访问此寄存器需要将“1011b”（Bh）用作器件地址中的器件类型标识符（见表 2）。器件类型标识符后面是硬件客户端地址位，其值由器件地址输入引脚 A2、A1 和 A0 决定。最后，位 0 为读 / 写选择（R/W）位，其中逻辑“1”用于读取，而逻辑“0”用于写入。

表 2： 配置寄存器器件地址字节

存储区	器件类型标识符				硬件地址位 (1)			读取 / 写入
	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
配置寄存器	1	0	1	1	A2	A1	A0	R/$\overline{W}$

注 1：使用 SOT-23 封装时，硬件客户端地址位必须置为逻辑“0”。

字地址要求

访问配置寄存器时，必须向器件发送一个 16 位字地址。除了位 A15、A11 和 A10，字地址中的所有位都将被忽略。位 A15 和 A11 必须置为逻辑“1”，而位 A10 则必须置为逻辑“0”。有关更多信息，请参见表 3 和表 4。

表 3： 配置寄存器字地址字节 0

字地址	A15	A14	A13	A12	A11	A10	A9	A8
字地址字节 0	1	x	x	x	1	0	x	x

表 4： 配置寄存器字地址字节 1

字地址	A7	A6	A5	A4	A3	A2	A1	A0
字地址字节 1	x	x	x	x	x	x	x	x

写操作

写入配置寄存器时，必须将包含数据字节 （字节 0 和字节 1）以及有效确认字节的写操作序列发送至器件。图 1 给出了配置寄存器写操作序列的示例。

确认字节

为了启动内部写入过程，必须将数据字节（字节 0 和字节 1）以及确认字节发送至器件。发送这三个字节之外的任何内容都会中止写周期，并且不会更改配置寄存器的内容。

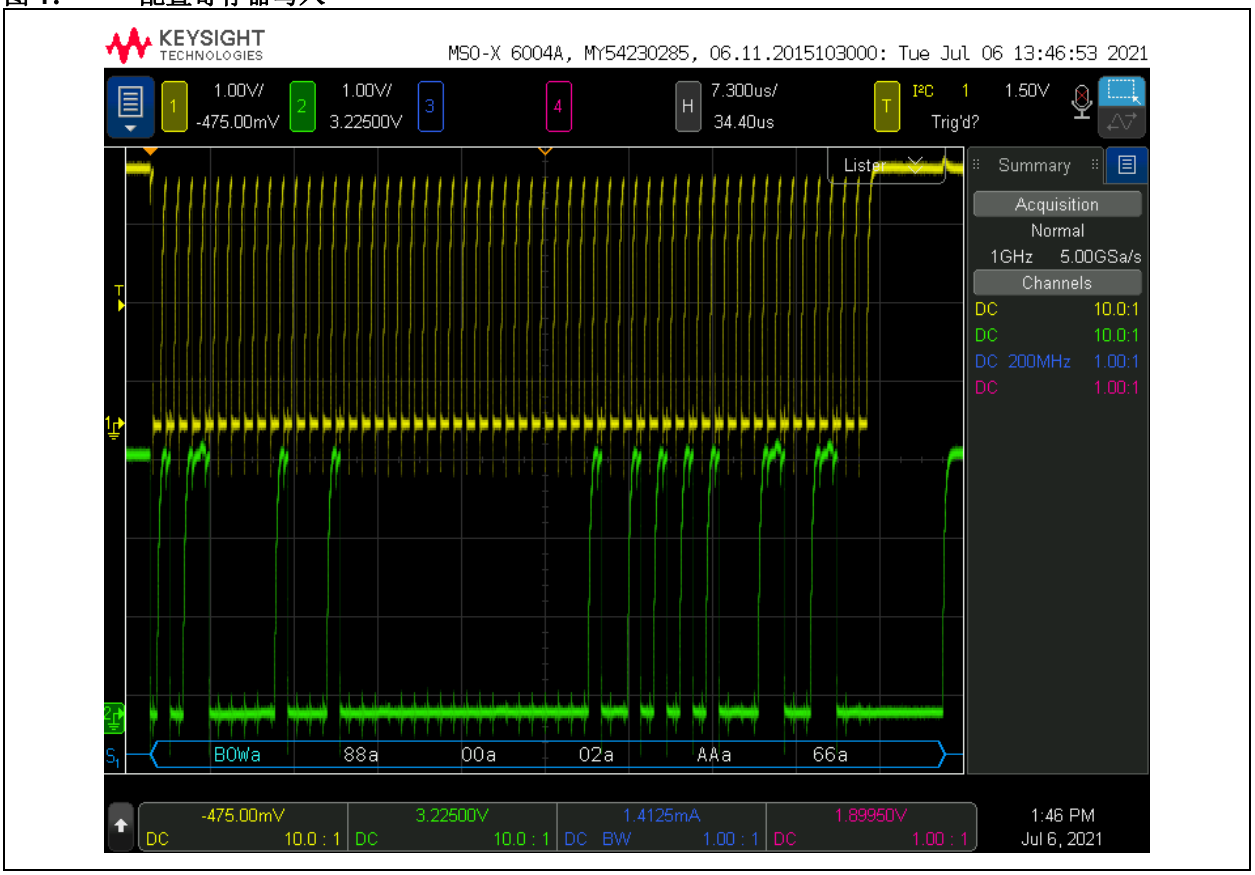
确认字节的数据取决于写入 LOCK 位的值。如果用户想要锁定配置寄存器（LOCK = “1”），则确认字节必须为 99h。如果用户想要配置寄存器处于未锁定状态（LOCK = “0”），则确认字节必须为 66h。表 5 给出了确认字节的有效数据值。

注： 配置寄存器一旦被锁定就无法将其解锁。

表 5： 配置寄存器确认字节

新的 LOCK 位值	D7	D6	D5	D4	D3	D2	D1	D0
1 （锁定）	1	0	0	1	1	0	0	1
0 （未锁定）	0	1	1	0	0	1	1	0

图 1： 配置寄存器写入



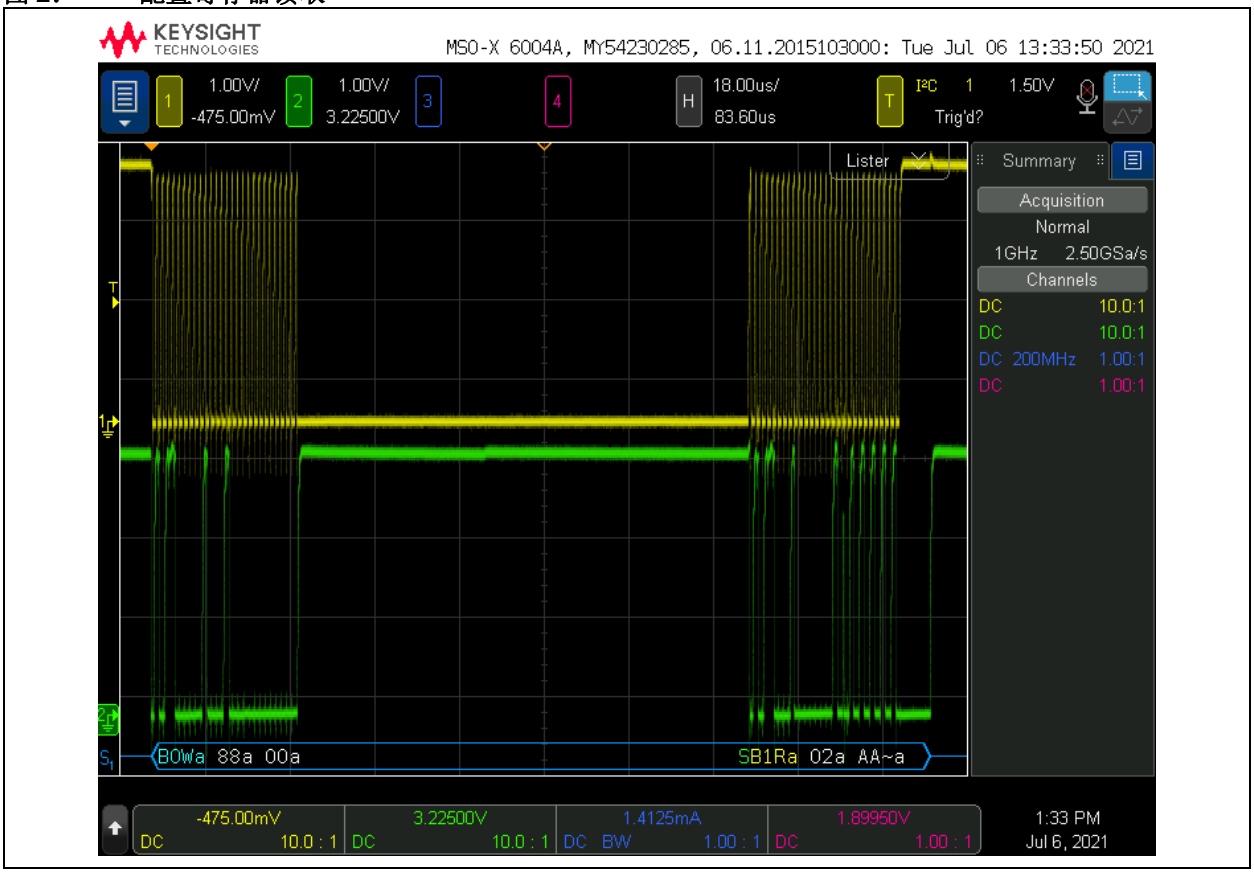
读操作

读取配置寄存器时，必须向器件发送一个随机读操作序列。

图 2 给出了配置寄存器读操作序列的示例。在当前地址读操作序列期间，无法读取配置寄存器的内容，因为必须将正确的字地址字节发送至器件。

注： 如果主机在读操作期间继续确认数据字节，24CS 系列将自动从第二个配置寄存器数据字节计满返回至第一个数据字节。

图 2：　配置寄存器读取



结论

本应用笔记详细介绍了 I^2C 配置寄存器提供的灵活写保护功能。欲了解有关 I^2C 配置寄存器和器件操作的详细信息，请参见 www.microchip.com 上相应器件的数据手册。

附录 A： 版本历史

版本 A （2021 年 10 月）

本文档的初始版本。

请注意以下有关 Microchip 产品代码保护功能的要点：

- Microchip 的产品均达到 Microchip 数据手册中所述的技术规范。
- Microchip 确信：在正常使用且符合工作规范的情况下， Microchip 系列产品非常安全。
- Microchip 注重并积极保护其知识产权。严禁任何试图破坏 Microchip 产品代码保护功能的行为，这种行为可能会违反《数字千年版权法案》（Digital Millennium Copyright Act）。
- Microchip 或任何其他半导体厂商均无法保证其代码的安全性。代码保护并不意味着我们保证产品是“牢不可破”的。代码保护功能处于持续发展中。 Microchip 承诺将不断改进产品的代码保护功能。

ISBN：978-1-6683-4760-7

全球销售及服务网点

美洲

公司总部 Corporate Office
2355 West Chandler Blvd.
Chandler, AZ 85224-6199
Tel: 1-480-792-7200
Fax: 1-480-792-7277
技术支持：
http://www.microchip.com/support
网址：www.microchip.com

亚特兰大 Atlanta
Duluth, GA
Tel: 1-678-957-9614
Fax: 1-678-957-1455

奥斯汀 Austin, TX
Tel: 1-512-257-3370

波士顿 Boston
Westborough, MA
Tel: 1-774-760-0087
Fax: 1-774-760-0088

芝加哥 Chicago
Itasca, IL
Tel: 1-630-285-0071
Fax: 1-630-285-0075

达拉斯 Dallas
Addison, TX
Tel: 1-972-818-7423
Fax: 1-972-818-2924

底特律 Detroit
Novi, MI
Tel: 1-248-848-4000

休斯敦 Houston, TX
Tel: 1-281-894-5983

印第安纳波利斯 Indianapolis
Noblesville, IN
Tel: 1-317-773-8323
Fax: 1-317-773-5453
Tel: 1-317-536-2380

洛杉矶 Los Angeles
Mission Viejo, CA
Tel: 1-949-462-9523
Fax: 1-949-462-9608
Tel: 1-951-273-7800

罗利 Raleigh, NC
Tel: 1-919-844-7510

纽约 New York, NY
Tel: 1-631-435-6000

圣何塞 San Jose, CA
Tel: 1-408-735-9110
Tel: 1-408-436-4270

加拿大多伦多 Toronto
Tel: 1-905-695-1980
Fax: 1-905-695-2078

亚太地区

中国 - 北京
Tel: 86-10-8569-7000

中国 - 成都
Tel: 86-28-8665-5511

中国 - 重庆
Tel: 86-23-8980-9588

中国 - 东莞
Tel: 86-769-8702-9880

中国 - 广州
Tel: 86-20-8755-8029

中国 - 杭州
Tel: 86-571-8792-8115

中国 - 南京
Tel: 86-25-8473-2460

中国 - 青岛
Tel: 86-532-8502-7355

中国 - 上海
Tel: 86-21-3326-8000

中国 - 沈阳
Tel: 86-24-2334-2829

中国 - 深圳
Tel: 86-755-8864-2200

中国 - 苏州
Tel: 86-186-6233-1526

中国 - 武汉
Tel: 86-27-5980-5300

中国 - 西安
Tel: 86-29-8833-7252

中国 - 厦门
Tel: 86-592-238-8138

中国 - 香港特别行政区
Tel: 852-2943-5100

中国 - 珠海
Tel: 86-756-321-0040

台湾地区 - 高雄
Tel: 886-7-213-7830

台湾地区 - 台北
Tel: 886-2-2508-8600

台湾地区 - 新竹
Tel: 886-3-577-8366

亚太地区

澳大利亚 Australia - Sydney
Tel: 61-2-9868-6733

印度 India - Bangalore
Tel: 91-80-3090-4444

印度 India - New Delhi
Tel: 91-11-4160-8631

印度 India - Pune
Tel: 91-20-4121-0141

日本 Japan - Osaka
Tel: 81-6-6152-7160

日本 Japan - Tokyo
Tel: 81-3-6880-3770

韩国 Korea - Daegu
Tel: 82-53-744-4301

韩国 Korea - Seoul
Tel: 82-2-554-7200

马来西亚 Malaysia - Kuala Lumpur
Tel: 60-3-7651-7906

马来西亚 Malaysia - Penang
Tel: 60-4-227-8870

菲律宾 Philippines - Manila
Tel: 63-2-634-9065

新加坡 Singapore
Tel: 65-6334-8870

泰国 Thailand - Bangkok
Tel: 66-2-694-1351

越南 Vietnam - Ho Chi Minh
Tel: 84-28-5448-2100

欧洲

奥地利 Austria - Wels
Tel: 43-7242-2244-39
Fax: 43-7242-2244-393

丹麦 Denmark - Copenhagen
Tel: 45-4485-5910
Fax: 45-4485-2829

芬兰 Finland - Espoo
Tel: 358-9-4520-820

法国 France - Paris
Tel: 33-1-69-53-63-20
Fax: 33-1-69-30-90-79

德国 Germany - Garching
Tel: 49-8931-9700

德国 Germany - Haan
Tel: 49-2129-3766400

德国 Germany - Heilbronn
Tel: 49-7131-72400

德国 Germany - Karlsruhe
Tel: 49-721-625370

德国 Germany - Munich
Tel: 49-89-627-144-0
Fax: 49-89-627-144-44

德国 Germany - Rosenheim
Tel: 49-8031-354-560

以色列 Israel - Hod Hasharon
Tel: 972-9-775-5100

意大利 Italy - Milan
Tel: 39-0331-742611
Fax: 39-0331-466781

意大利 Italy - Padova
Tel: 39-049-7625286

荷兰 Netherlands - Drunen
Tel: 31-416-690399
Fax: 31-416-690340

挪威 Norway - Trondheim
Tel: 47-7288-4388

波兰 Poland - Warsaw
Tel: 48-22-3325737

罗马尼亚 Romania - Bucharest
Tel: 40-21-407-87-50

西班牙 Spain - Madrid
Tel: 34-91-708-08-90
Fax: 34-91-708-08-91

瑞典 Sweden - Gothenberg
Tel: 46-31-704-60-40

瑞典 Sweden - Stockholm
Tel: 46-8-5090-4654

英国 UK - Wokingham
Tel: 44-118-921-5800
Fax: 44-118-921-5820