

# 揭开非易失性存储器知识产权的神秘面纱

为无线、模拟、微机电系统和安全应用的 SoC 设计选择最佳的非易失性存储器知识产权解决方案

2011 年 4 月



作者

Craig Zajac

新思科技有限公司高级产品营销经理

## 概述

随着非易失性存储器 (NVM) 知识产权 (IP) — 尤其是可编程 NVM IP — 的使用从微控制器等传统的嵌入式 flash 应用扩展至无线、模拟、微机电系统 (MEMS) 和安全应用, 一个全新的设计师群体正在集成 NVM。对于这些新的用户而言, 目前有多种 NVM IP 使用模式和解决方案, 而且它们经过优化, 可以满足各类应用的要求。为了选择最佳的 NVM IP 解决方案, 设计人员必须考虑各种 NVM IP 规格以及它们的微妙含义和对片上系统 (SoC) 设计的总体影响。

诸如工作温度、电源电流、电源电压、基本时序等很多 NVM IP 规格对于一系列广泛的半导体产品而言是通用的, 而且很容易被理解。但是, 我们应正确评估更多独有规格, 以防止出现针对具体应用要求的设计过度或不足, 从而增加系统的成本和风险。

本白皮书将:

- ▶ 探讨一些将 NVM IP 融入到系统之中的新应用;
- ▶ 描述一些现有的 NVM IP 解决方案;
- ▶ 揭示 NVM IP 的一些独有规格, 如耐擦写次数、保存时间和写干扰, 并描述它们之间的关系以及它们对应用要求的影响;
- ▶ 为设计人员提供如何选择最佳 NVM IP 解决方案的指南。

## 定义 NVM

NVM 是能够在无电源情况下保存数据的存储器。它与无电源时将丢失存储内容的静态随机存取存储器 (SRAM) 和动态随机存取存储器 (DRAM) 等技术不同。NVM 的主要定义如下:

- ▶ **多次可编程 (MTP) NVM:** 可重复电编程 1000 次以上的 NVM。
- ▶ **数次可编程 (FTP) NVM:** 可重复电编程 1000 次以下的 NVM。

- ▶ **一次性可编程 (OTP) NVM:** 只能编程一次、不能重复编程的 NVM。
- ▶ **嵌入式 NVM:** 嵌入到一个单片集成电路 (IC) 设计之中的 NVM 技术，而不是整合到多个多芯片模块中的多个 IC。
- ▶ **NVM IP:** 某个第三方 IP 提供商或代工厂授权使用的 NVM 技术，目的是在某项设计中实现嵌入式 NVM。

其它电路中不常使用的最有用的 NVM IP 规格有：比特数 (bit count)、耐擦写次数 (endurance)、保存时间 (retention) 和写干扰 (write disturb)：

- ▶ **比特数**是指 NVM IP 的总数据存储容量，也被称为存储密度。比特数的单位是比特或字节，1 字节=8 比特。
- ▶ **耐擦写次数**是指 NVM 的可编程/可重复编程次数。耐擦写次数针对的是字。例如，对于一个使用 32-bit 字的 NVM 而言，所有编程和读操作将在所有 32-bit 字上同时进行。如果耐擦写次数的上限是 10 万次编程事件，则每个 32-bit 字最多可编程/可重复编程 10 万次。为了给应用确定合理的耐擦写次数，设计人员必须考虑需要重新写入 NVM IP 的总次数，包括制造和生产测试期间的写入次数。
- ▶ **保存时间**是指 NVM 在无需重新编程的情况下保存数据的时间，时间测量从上一次编程事件开始。某个字每次被重新编程时，保存时间规格将被重置。设计人员应考虑应用的保存时间要求以及它与其它 NVM 规格的关系。本白皮书将针对这些内容进行探讨。
- ▶ **写干扰**是指在干扰此前所写数据的情况下，阵列中能够发生的写操作的累计次数。例如，在一个 32-bit 阵列中，如果阵列中的第一个字被写入数据，则写干扰是指：能够在其余 31 个字上发生的、不干扰第一个字中所写数据的编程事件的累计次数。

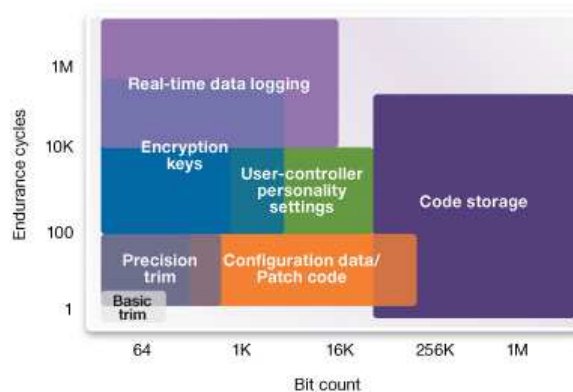
## 新的 NVM IP 应用领域

嵌入式 NVM IP 过去主要用于两个应用领域：代码存储和基本微调。

独立微控制器或嵌入式处理器等代码存储应用需要高密度的 NVM IP (高达几个 Mbit)，而且可能需要或不需要重写数据的能力。基本微调用于调节模拟性能，因此它要求应用拥有较低的比特数 (低于 128-bit)，而且只需在工厂中编程一次。

但是，过去几年中，无线、模拟、MEMS、安全应用等新兴应用开始使用可编程 NVM IP。这些应用既不属于代码存储也不属于基本微调应用领域。根据它们对比特数和耐擦写次数的要求，它们被划分到新的应用领域，如实时数据记录、密钥、用户控制器个性化设置、精确微调和配置数据/补丁代码 (如图 1 所示)。

精确微调应用只需要较小的比特数和最多几次写操作，而实时数据记录应用则需要几个 kbit 的比特数和极高的耐擦写次数 (通常高达 100 万次)。用户控制器个性化设置和密钥等其它应用介于两者之间。



揭开非易失性存储器规格的神秘面纱

图 1: 新的 NVM IP 应用领域

(图中文字: 耐擦写次数 实时数据记录 密钥 用户控制器个性化设置 精确微调 配置数据/补丁代码 代码存储)

## 实时数据记录

远端服务器智能电源管理、电信应用以及汽车和军事应用等高可靠性应用利用实时数据记录和配置设置存储日期代码、保修信息、开/关机顺序或者客户/设备的标识数据。对于这些应用，可以更新 NVM IP 解决方案，以便能在更改设备或要求时更改设置，或在系统停机之前记录故障信息。与那些 3 至 5 年内就会被淘汰、工作温度接近室温的消费类产品相比，产品生命周期较长、大部分时间工作温度较高的工业和汽车产品有着完全不同的保存时间要求。

## 密钥

Flash 控制器、硬盘驱动器、家庭娱乐设备（如配备高清多媒体接口[HDMI]的高清电视[HDTV]）等应用使用各种不同的密钥和计数器。例如，高级加密标准（AES）用于各类内容保护方案，而非易失性计数器用于可信计算等应用。对于这些应用而言，能够对 NVM IP 重复编程可以让 SoC 主动更改密钥，以增加破解它们的难度，或在系统被攻陷时被动更改密钥。例如，在 HDMI 应用中，最终数据和密钥只被写入一次，而在制造过程中，为了全面测试 NVM IP，它们可能需要被写入 2 到 10 次。

## 用户控制器个性化设置

使用无线射频（RF）、WiFi802.11 通信设备、蓝牙耳机音量控制、Zigbee、GPS、RFID 等的应用不仅需要现场编程和更新，而且需要在开机时保持上一次状态。过去，这些应用或者不得不使用分立电可擦编程只读存储器（EEPROM）IC（从而增加体积和功耗），或者不得不使用一个多 Bank OTP（从而增加设计复杂性，降低总体灵活性）。现在，SoC 设计人员可以使用 NVM IP 保存信息，以降低系统的成本和功耗，同时又不牺牲系统的性能。

## 精确微调

高性能数模转换器（DAC）和模数转换器（ADC）、MEMS 压力传感器、加速度传感器、陀螺仪（正成为手机和平板电脑中的常用组件）、硅时钟等精密模拟组件要求进行定期现场校准，以便将环境和老化效应导致的性能下降因素考虑在内。为了使这些应用达到较高的性能，需要更多的比特数（最多 1k）和耐擦写次数。更多的比特数可以提高精度，更多的耐擦写次数可以实现在不同的温度或制造阶段调节性能，以便将包装和系统寄生对总体模拟性能的影响考虑在内。在这种情况下，NVM IP 是 SoC 设计人员的理想解决方案，可提高系统的性能和灵活性，为客户提供可编程能力，并对 NVM 进行 100%的电气测试，从而实现比 OTP 解决方案更加全面的生产测试流程。

## 配置数据/补丁代码

微控制器应用的大部分源代码是恒定不变的，可以存储在一个 OTP 阵列中，或一个内置的只读存储器（ROM）中。存储器的一小部分可能需要存储用于增强各项功能或纠正主代码空间中的某些错误的补丁代码，或者存储由系统现场使用和更新的配置数据。通过在此类应用中使用 NVM IP，设计人员可以降低嵌入式 flash 的成本，同时保持现场更新软件和固件的灵活性。

## NVM IP 使用模式与解决方案

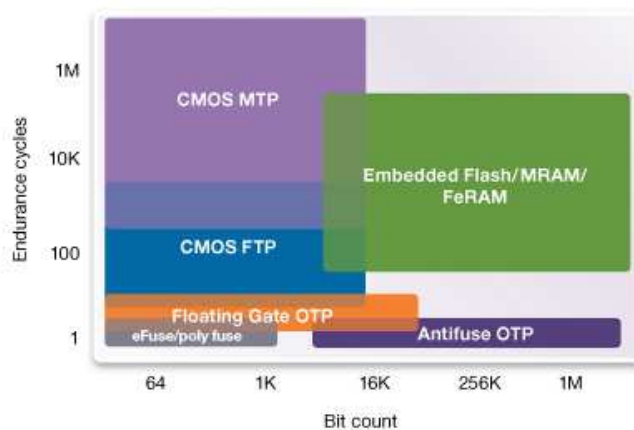


图 2 - NVM IP 使用模式与解决方案

（图中文字：浮栅 OTP 电编程熔丝（eFuse）/多晶硅熔丝 嵌入式 Flash 反熔丝 OTP）

目前有多种嵌入式 NVM IP 解决方案，用于满足这些新应用的不同要求。每个 NVM IP 解决方案都旨在优化某些具体应用的性能，如实时数据记录、精确微调、超低功耗或客户个性化设置。根据它们的耐擦写次数和比特数，这些 NVM IP 解决方案包括：基于 CMOS 的 MTP、基于 CMOS 的 FTP、嵌入式 flash / 磁阻随机存取存储器（MRAM）/ 铁电随机存取存储器（FeRAM）、OTP 和熔丝（如图 2 所示）。

通过对比图 1 和图 2，我们可以发现不同的应用对应不同的 NVM IP 使用模式：基本微调对应熔丝，代码存储对应嵌入式 flash/MRAM/FeRAM，精确微调 and 用户控制器个性化设置对应 CMOS FTP，实时数据记录和密钥对应 CMOS MTP。

但在现实生活中，这些应用并非如上述那样一一对应。我们可以从各个 NVM IP 使用模式之间较小的性能特点重叠区域（图 2）和应用领域（图 1）中发现这一点。在这些应用和很多系统中，嵌入式 NVM IP 需要支持多个使用模式。需要进行实时数据记录的系统通常也需要配置或微调数据；密钥通常被嵌入到也需要使用 NVM IP 存储代码的系统中。

### CMOS MTP 和 CMOS FTP

CMOS MTP 和 CMOS FTP 是新的 NVM IP 解决方案，兼容标准 CMOS 工艺。这些 CMOS 解决方案不同于嵌入式 flash，后者需要额外的工艺/层来创建 NVM IP。CMOS NVM 解决方案可重复电编程 100 至 100 万次，从而为设计人员提供了更大的灵活性。NVM CMOS MTP 和 FTP 目前采用 65 纳米工艺，不久将采用 40 纳米工艺。

CMOS MTP 和 CMOS FTP 适合低于 16-kbit 和最多 100 万耐擦写次数的应用范围，因此，它们适用于各种不同的应用，包括：

- ▶ 使用少量 NVM 持续存储有关芯片环境的“黑盒”类型信息的芯片，例如，便携式设备的电池或增值 RFID 标签中所使用的芯片。这些数据可用于确保电池不会承受过大压力（电压或温度），或者用于跟踪食品运输过程中的温度。
- ▶ 密钥，无论是相对较小的密钥（128-bit 高级加密标准[AES] 密钥），还是大得多的密钥（HDMI 使用的大于 2-kbit 的密钥）。这两种密钥都能受益于 MTP 或 FTP 的可编程性。
- ▶ 个性化设置，如蓝牙耳机上的设置。通常可以使用 1 或 2-kbit 的 FTP NVM IP 存储这些设置。嵌入式 NVM 可减少 OTP 解决方案的体积和功耗，同时增加其灵活性。

- ▶ 精密设备（用于调节功率、速度或精度）通常需要考虑包装或系统对性能的影响，因此，在对设备进行包装之前，最终的微调设置是未知的。能够对 NVM IP 重新编程可以实现 100% 的电气测试。
- ▶ 90% 以上的代码不需要现场更改而且重复编程只用于纠正错误或升级目的的各种设备。在这种情况下，可以使用少量 FTP 补充存储在 ROM 或其它非可再编程 NVM IP 中的较大代码空间。

### 嵌入式 Flash

嵌入式 Flash 主要用于需要能够对 NVM 重复编程的高密度应用。大多数微控制器都提供一个用于存储代码的嵌入式 flash 选项。嵌入式 flash 虽然能够提供一个高密度解决方案，但需要额外的工艺步骤，而且较为复杂，可将晶圆的成本增加 50% 或更多。目前，40 纳米 CMOS 已经大批量生产，28 纳米 CMOS 也开始普及，而嵌入式 flash 落后 2 到 3 个节点，代工厂刚刚开始采用 90 纳米工艺生产嵌入式 flash。

### 反熔丝 OTP

反熔丝 OTP 也主要用于在独立微控制器或嵌入式处理器中存储代码。它支持与嵌入式 flash 类似的密度，主要优点是：能够采用标准 CMOS 工艺制造，因此，不仅可以降低总成本，而且还使其支持 40 纳米等更先进的节点。反熔丝 OTP（以及所有 OTP 解决方案）的主要缺点是：NVM 只能编程一次，从而限制了其现场更新的能力，也限制了测试 NVM 阵列的能力。

### 浮栅 OTP

浮栅 OTP 不支持嵌入式 flash 或反熔丝 OTP 的高密度，但采用标准 CMOS 工艺制造。浮栅 OTP 通常用于介于传统多晶硅熔丝和反熔丝 OTP 之间的比特数应用。与所有 OTP 解决方案一样，浮栅 OTP 解决方案的最大缺点是：NVM 只能编程一次，从而限制了客户进行现场更新的能力，也限制了生产测试能力。

### 电编程熔丝（eFuse）和多晶硅熔丝

熔丝非常适合满足小容量的 NVM IP 需求，通常用于基本微调应用，这些应用中没有值能够对 NVM IP 重新编程。大多数熔丝由代工厂提供，在工艺生命周期的很早阶段、其它 NVM 解决方案被完全开发出来之前就已出现。

表 1 列出了上述各个应用领域的各种 NVM 使用模式的参数和规格。

	CMOS MTP	CMOS FTP	CMOS OTP	嵌入式 Flash	熔丝
工艺	标准 CMOS 工艺 (一直到 65 纳米 /40 纳米)	标准 CMOS 工艺 (一直到 65 纳米/40 纳米)	标准 CMOS 工艺 (一直到 65 纳米/40 纳米)	定制 flash 工艺 (250 纳米 → 90 纳米)	标准 CMOS 工艺 (一直到 28 纳米)
比特数	32-bit 到 8-kbit	32-bit 到 16-kbit	32-bit 到 ~1-Mbit	~32-kbit 到 4-Mbit	1024-bit 或更低
写操作次数	50,000 到 1,000,000 次	100 到 1,000 次	1 次	20,000 到 100,000 次	1 次
保存时间	10 年	10 年	10 年	10 年	10 年
典型应用领域	实时数据记录/密钥	用户控制器个性化设置/精确微调	基本微调/代码存储	可再编程代码存储	基本微调

表 1: 典型应用领域的 NVM 使用模式的参数和规格

针对某个具体应用精心选择最佳的 NVM IP 解决方案时，要求设计人员不仅拥有有关 NVM IP 主要规格的知识，而且了解这些规格的微妙含义，以便降低成本和风险。事实上，NVM IP 关键参数的设计过度有可能增加系统成本，如硅片面积、特性描述成本、认证成本和生产测试成本，而这些参数的设计不足则有可能导致产量损失甚至现场故障。

## NVM 主要规格的微妙含义以及它们对应用要求的影响

### 耐擦写次数 vs. 保存时间

耐擦写次数和保存时间规格是 NVM IP 独有的规格。SoC 设计人员必须了解这两个规格之间的折衷方案和互动关系，以便为每个应用选择一个最佳解决方案。

由于某个字每次被重新编程时，保存时钟将被重置，IC 被编程的次数越多，编程事件之间的时间就越短，意味着耐擦写次数和保存时间之间呈反比关系。因此，降低 IC 的保存时间规格可以被接受。例如，假设产品生命周期为 10 年，编程事件之间的平均时间如下：

- ▶ 耐擦写次数 = 100 次 → 平均保存时间 = 1.2 个月
- ▶ 耐擦写次数 = 1,000 次 → 平均保存时间 = 3.65 天
- ▶ 耐擦写次数 = 10,000 次 → 平均保存时间 = < 9 小时
- ▶ 耐擦写次数 = 100,000 次 → 平均保存时间 = < 1 小时

但在实际应用中，编程事件不可能这样定期发生，因此，有保障的保存时间规格必须留有充足的余量，以便将编程事件之间的时间变化因素考虑在内。图 3 描述了耐擦写次数与保存时间之间的折衷方案，对比了平均保存时间和某个使用合理规格的 NVM IP 解决方案的平均保存时间。对于任何耐擦写次数上限高于 100 次的应用，该规格可确保高于平均要求至少 100 次的余量。

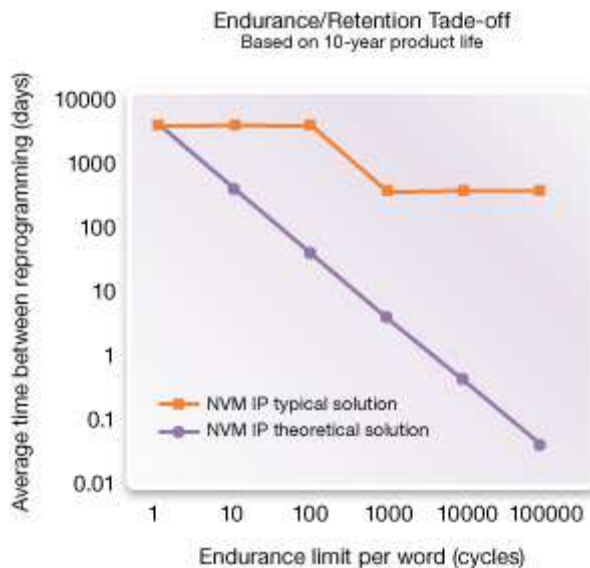


图 3：耐擦写次数与保存时间之间的折衷方案（10 年产品生命周期）

图中文字：编程事件之间的平均时间（天） 耐擦写次数与保存时间之间的折衷方案（10 年产品生命周期） NVM IP 典型解决方案 NVM IP 理论解决方案 耐擦写次数上限/字（次）

虽然 NVM IP 阵列中的各个字或是需要较高的耐擦写次数，或是需要较长的保存时间，但在一些合理的使用模式中，最终用户要求 NVM IP 同时提供这两种性能。一种常见的使用模式是：将 NVM IP 阵列分为两个区：一个用于存储耐擦写次数较低/保存时间较长的数据（如微调设置、厂商/设备 ID 或保修和日期代码信息），另一个用于耐擦写次数较高/保存时间较短的应用（如数据记录）。

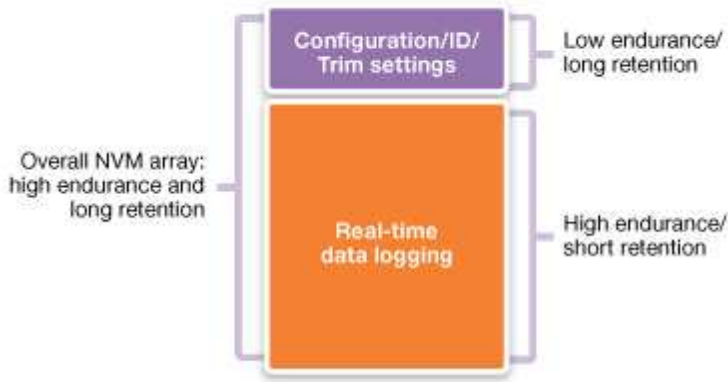


图 4：同时要求较高的耐擦写次数和较长的保存时间的使用模式

(图中文字：整个 NVM 阵列：较高的耐擦写次数和较长的保存时间 配置/ID/微调设置 实时数据记录 较低的耐擦写次数/较长的保存时间 较高的擦写次数/较短的保存时间)

虽然整个 NVM 阵列需要较高的耐擦写次数和较长的保存时间，但每个字只需要其中之一。如图 4 所示，每个字都能被一个较高的耐擦写次数/较短的保存时间规格或一个较低的耐擦写次数/较长的保存时间规格有效覆盖。

设计人员应根据最终系统的要求，仔细审视基于合理使用模式的各个 NVM IP 规格，定义每个字的耐擦写次数和保存时间；或者采用以下使用模式：将一部分 NVM IP 用于存储耐擦写次数较高的数据，另一部分用于存储保存时间较长的数据。为了选择最佳的 NVM IP 解决方案，设计人员应全面了解 NVM IP 在整个产品生命周期内将被如何使用，包括：写操作的次数和频率，整个 NVM IP 阵列是否用于相同的目的，是否应将阵列分区，以满足不同的要求。

## 写干扰

写干扰规格的定义是：需要重新编程数据之前，阵列中其它字上可以发生的编程事件的累计次数。其原因是：NVM IP 阵列中的某个字每次被重新编程后，有可能干扰已编程字中的数据。写干扰的最差使用模式如下图所示（图 5）。

在一个包含  $n$  个字的 NVM IP 阵列中（字[0] → 字[ $n-1$ ]），如果阵列中的第一个字被编程一次，其余  $n-1$  个字将被重复编程，直到达到耐擦写次数上限。字[0]的最大写干扰量为：

$$Max Write Disturb = ENDR \times (n - 1)$$

其中， $n$  表示阵列中的字数， $ENDR$  表示耐擦写次数上限。对于一个包含 32 个字、耐擦写次数上限为 100k 的阵列，任意给定字上的最大写干扰量为 3.1M 编程次数（ $100k \times (32-1)$ ）。

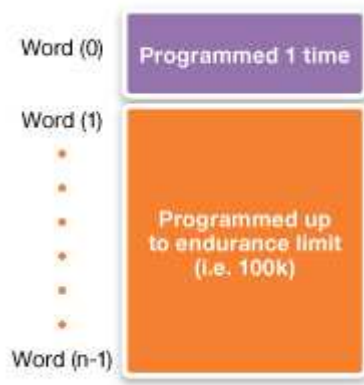


图 5：写干扰的最差使用模式

图中文字：字(0)被编程一次 直到达到耐擦写次数上限（即 100k）

了解 NVM IP 阵列的总体使用模式对于评估需要何种写干扰性能至关重要。对于任何对阵列中的不同区域有着不同耐擦写次数要求的用例而言，应对 NVM 阵列的写干扰性能进行评估。与耐擦写次数类似，大多数的写干扰故障不能在最终测试中被屏蔽掉。

通过了解各种影响或写干扰，设计人员可以对系统进行智能分区，以最大程度减少干扰影响，从而提升嵌入式 NVM IP 的性能。例如，在一个实时数据记录应用中，虽然 NVM IP 阵列的绝大部分将用于持续更新系统温度、电压和性能信息，但设计人员也应利用 NVM IP 阵列的一小部分存储客户 ID、保修信息或用于基本性能微调。

## 总结

随着嵌入式 NVM 超越传统的代码存储和性能微调应用，更多的设计人员需要熟悉各种不同的 NVM IP 解决方案以及 NVM IP 独有的性能规格。为了为某个特定应用选择最佳的嵌入式 NVM IP 解决方案，了解这些独有规格以及它们对彼此的影响至关重要。

在评估耐擦写次数和保存时间规格时，SoC 设计人员不仅应考虑 NVM IP 将要被写入的总次数，而且应考虑写操作的频率、预期的产品生命周期和工作温度。评估写干扰性能时，设计人员必须知道如何对 NVM 阵列进行分区，所有比特的使用模式是否同质，或者阵列中的不同区域是否有不同的要求。这样一来，SoC 设计人员就能生成准确的要求，即不夸大也不低估实际的使用情况。

Synopsys DesignWare® AEON®系列 NVM IP 提供详细、基于硅片的耐擦写次数、保存时间和写干扰性能数据。每一个 DesignWare AEON IP 产品都是为了优化特定应用的性能，包括实时数据记录、精确微调、超低功耗无线应用或客户个性化设置。有关 Synopsys DesignWare AEON NVM IP 解决方案的更多信息，敬请访问：<http://www.synopsys.com/nvm>。