
自举程序设计注意事项

简介

许多现代嵌入式系统需要通过现场固件更新来修复错误或改进功能。通常，此类更新功能通过自举程序来实现。自举程序是一个独立于主应用程序的特殊应用程序，能够更新主应用程序。

本文档介绍了设计稳健的自举程序时必须考虑的一些细节。

目录

简介.....	1
1. 自举程序的类型和固件更新选项.....	3
2. 进入方法.....	4
3. 应用程序和自举程序之间的通信.....	5
4. 映像完整性验证.....	6
5. 安全性.....	7
6. 故障检测和恢复.....	8
Microchip 网站.....	9
变更通知客户服务.....	9
客户支持.....	9
Microchip 器件代码保护功能.....	9
法律声明.....	10
商标.....	10
质量管理体系.....	11
全球销售及服务网点.....	12

1. 自举程序的类型和固件更新选项

单片机自举程序可以多种不同方式工作，具体取决于硬件的复杂度和用户外部通信接口的可用性。

最基本的自举程序可以通过通信接口接收映像，并在通过完整性验证后写入接收的映像。大多数情况下，自举程序不可更新，并且仅限用于简单的接口，如 **UART**、**SPI** 或 **I²C**。最终产品的用户通常无法访问这类接口，因此这类接口比较适合用于已经与主控制器建立通信接口的从 **MCU**。

高级自举程序将实现用户可访问的接口，例如 **USB**、**SD** 卡或以太网。这会增大自举程序的大小，并且要求自举程序自行更新，以修复协议实现中的缺陷或者适应外部设备的变化。例如，原版本产品最高仅支持 **2 GB** 容量的 **SD** 卡，而随着时间的推移，应用经过不断更新后可支持更高容量的 **SD** 卡，但旧版自举程序仍将要求使用 **2 GB SD** 卡（届时相对来说可能很难购买到）。

如果需要高级更新，则要评估主应用程序是否可以接收和存储低级格式的映像，以便确保可供简单自举程序使用。凭借这种方法，可以实现高级更新接口，同时能够让实际自举程序依然保持简单而紧凑。

当无线系统需要更新时，将无法在自举程序中复制无线协议栈。因此，通过无线方式更新无线系统的唯一选择是在应用程序运行时接收新映像，然后让简单的自举程序执行更新。映像可以存储在主闪存阵列的可用空间中，或存储在外部存储器中。当存储在外部存储器中时，映像必须保持加密状态；而当存储在内部存储器中时，则可以对映像进行解密和验证，从而简化自举程序的设计。

2. 进入方法

与主机控制器搭配使用的简单自举程序可以使用以下任一进入方法：

- 专用引脚（在复位时必须置为有效）
- 重复使用其中一个接口引脚
- 应用程序请求
- 没有有效的应用程序

专用引脚是最稳健的方法，但它需要在主机和从 MCU 上分配额外的引脚，这并不总是可行的。

许多接口包括处于已知空闲状态的引脚，例如，SPI 或 I²C 中 SCL 和 SDA 线上的片选。这些引脚通常使用外部上拉电阻保持空闲状态，因此从器件可以在复位时检测到置为有效的状态并保持在自举程序模式。

这两种方法都需要访问从 MCU 的复位引脚。但其优势在于可完全确保稳健性。即使主应用程序已损坏且主通信接口无法正常工作，主机也始终可以请求执行自举程序。

应用程序请求不需要任何附加引脚，并且通过正常的主机到从器件通信接口即可发出自举程序的运行请求。此方法需要正常工作的应用程序来处理请求。

即使应用程序区域为空或已损坏，自举程序也依然可以执行。检测算法既可能简单到仅仅查找闪存存储单元的非擦除状态，也可能复杂到对整个应用程序映像进行 CRC 或哈希计算。必须针对每个应用程序评估错误检测的速度和稳健性之间的权衡结果。

更高级的自举程序可能会检测到 U 盘或 SD 卡上存在更新文件，并以这种方式启动更新。

3. 应用程序和自举程序之间的通信

在某些情况下，应用程序和自举程序之间需要交换更多信息，例如新映像通知、更新状态或一些附加请求。

一些 MCU 具有一组专门为此类用途分配的通用寄存器。这些寄存器可保证在上电时复位为 0，但在复位周期内保持不变。这样即创建了一个稳健的通信通道。

如果没有特殊寄存器，则可以使用系统 RAM。虽然 RAM 在复位周期内的状态通常保持不变，但在上电后的状态并不确定。为避免发生错误通信，建议使用多个命令副本。如果所有副本包含相同的值，则命令一定是有效的。副本数量是误报概率和存储器消耗之间权衡后的结果。至少应使用 4 个副本，对于单字节命令，通常使用 16 个副本就足够了。

如果认为 RAM 不可靠，或者 MCU 的复位过程擦除了 RAM（在一些面向安全的器件上可能出现），则可以转为使用 EEPROM 或闪存。但缺点是许多现代 MCU 上暂无法提供真正的 EEPROM，并且闪存具有擦除和写入粒度要求，这将导致浪费大量的闪存空间。

4. 映像完整性验证

在自举程序中，有两个不同的位置需要进行映像完整性验证。

需要验证新映像的完整性。对于任何自举程序设计而言，此步骤可能是强制性的，因为这一环节最容易受到意外损坏（由不可靠接口导致）和有意损坏（由主动攻击者导致）。如果使用加密，则此步骤通常与映像验证相结合，因为有效验证可自动证明映像完整性。

自举程序可以独立于初始验证在每个复位周期执行映像验证。这一步骤通常是可选的，因为它会延迟应用程序的执行。但是，在某些情况下，如果担心器件安全性，则需要进行二次验证。攻击者可能会尝试中断其他安全的更新过程，致使闪存处于未知状态。如果自举程序稍后尝试在没有验证的情况下执行应用程序，则它将执行从未打算运行的代码，可能导致泄露机密信息。

防止此类攻击的另一种方法是使用持久标志来指示映像有效性。必须在更新过程之前清零该标志，并在第一次成功完成映像验证后将其重新置 1。自举程序必须始终在控制权交给应用程序之前检查该标志。这样，便不需要在每次复位时进行映像验证。

如果自举程序设计允许在闪存编程开始之前接收整个映像，则应在尝试编程之前验证接收到的映像的完整性。但是，在许多情况下，自举程序必须以小块的形式接收和编程映像。在这种情况下，务必使自举程序进入过程在没有有效应用程序映像的情况下也能正常工作，因为更新过程中断可能导致器件无法运行。任何使用二次映像验证（通过完整验证或使用上述标志）的自举程序都会自动受到保护，防止出现此问题。即使应用程序映像损坏，自举程序也将继续运行。主机控制器必须为此情况做好准备，并检测自举程序是否正在运行。因此，必须再一次尝试更新。

选择验证算法时需要在验证速度和性能之间进行权衡。通常，最好使用慢速但安全的算法进行新映像验证，使用快速算法（如 **CRC32**）进行应用程序完整性验证。

5. 安全性

如果目标 MCU 具有对 CRC 或安全哈希算法的硬件支持，则最好使用这些功能进行映像验证，因为它们可能比等效的软件解决方案更为快速。如果硬件不支持高级加密标准，则算法更简单的软件实现通常可提供足够的安全级别，同时保持高速度和低占用空间。通常认为 XTEA、RC4 和 Spritz 等简单算法对于一般用途而言功能太弱，但这并不是自举程序应用时的关注点。功能太弱的一个重要原因是观察大量重复数据的能力太弱，甚至能够影响纯文本。但对于自举程序而言，这些都不重要。映像更新是罕见的事件，映像大小相对较短，因此攻击者无法收集大量的加密数据。

一种不错的安全措施是从不使用主密钥进行数据的实际加密。必须使用主密钥根据映像头中的信息获取映像加密密钥。这样，不同的映像将具有不同的加密密钥，从而进一步限制成功攻击的机会。

在所有情况下，必须注意了解所用算法的局限性，以及如何正确应用它们。始终建议由安全专家进行审查。

安全实现的最重要方面之一是密钥存储。必须使用加密密钥对所有器件进行预配置。假设通用 MCU 没有用于密钥存储的特殊安全功能，则密钥既可能作为自举程序的一部分存储，也可能存储在单独的数据段中。将密钥作为自举程序的一部分存储可为闪存节省一些空间，因为自举程序很少占用分配的整个段。但缺点是如果需要更新密钥，则整个自举程序也必须更新。

密钥也可能存储在一个数据段中，该数据段可能已被应用程序用于存储用户数据。这种方法的缺点是，当需要写入新数据时，应用程序会擦除数据段，此时密钥也会一并被擦除。通常情况下，应用程序会将密钥进行回写，但如果在此期间发生断电，则密钥将丢失。存储密钥最可靠的方法是为密钥分配一个单独的扇区。由于闪存写入粒度小于擦除粒度，因此它可以同时具有多个活动密钥，而不会在密钥更改过程中丢失任何活动密钥。

某些单片机还可以提供一个单独的段来存储密钥，例如熔丝或用户行。

初始密钥配置必须在安全可信的位置完成。如果原始密钥遭到泄露，则所有进一步的密钥更新也将受到影响。

有时，可能无法在安全的位置编程器件。在这种情况下，必须使用虚拟密钥，并且不应编程应用程序映像。这样，主机控制器便可以检测到从器件没有有效的应用程序映像，并执行第一次密钥更新，然后使用真实密钥加密应用程序映像更新。此步骤必须在安全位置执行。

6. 故障检测和恢复

固件更新的常见问题是故障检测和恢复。

如果自举程序正在与主机处理器通信，则解决方案是重试更新。如果主机控制器有办法在没有运行应用程序的情况下向自举程序发出请求，则不存在发生永久性故障的风险。

在独立自举程序的情况下，如果自举程序使用新映像覆盖现有映像而未备份映像，则无法进行恢复。编写新映像以替代活动映像的过程是更新过程中最危险的部分。有几种方法可以缓解或最大程度降低这种危险。

自举程序必须始终执行验证，验证失败时必须重新尝试验证。最终，更新可能成功，也可能因潜在的硬件问题而失败，而这是软件无法解决的。这意味着如果更新过程因循环上电或复位而中断，则将最终处于一种不一致的状态，自举程序必须再次执行更新。

完全避免映像切换过程的一种方法是让自举程序从闪存的任一部分运行应用程序。使用这种方法时，自举程序必须记住闪存的哪个部分包含活动应用程序。该方法的其中一个缺点是必须链接不同的映像才能在不同的地址正常工作。借助一些架构和工具链，可以创建与位置无关的代码，但更通用的解决方案是构建多个映像，即在每个可能的位置构建一个映像。然后，更新过程将下载与非活动槽匹配的映像。只要有足够的存储空间可用，此方法还可以扩展到两个以上的映像。

一些单片机支持双分区闪存，能够使用单条原子级命令切换分区。配备这种硬件功能后，完全可以没有专用的自举程序。在这种情况下，正在运行的应用程序会将新应用程序写入第二个分区，并在写入的数据通过验证后执行切换。这种方法的缺点是无法检测固件故障或损坏并加以恢复。

即便使用双分区闪存，也可以通过自举程序在启动时检查映像完整性，并在出现错误时执行恢复操作。在这种情况下，相同的自举程序代码必须复制两份，每个分区各一份。

双分区闪存可以轻松执行恢复。由于旧映像始终可用且已知功能正常，因此需要一种简单的分区切换。

假设在自举程序准备好将控制权交给应用程序时，更新的映像已经通过验证。这会留下许多潜在的问题，例如有效的应用程序无法正常运行。这可能是由于无意中使用了不正确的映像，或者新映像与环境之间存在某种程度的不兼容。

为了检测这类故障，自举程序可以设置永久标志，指示它将要运行新的应用程序映像。应用程序将检查该标志并运行功能测试，或者至少确保固件更新通道可用。之后，应用程序将清零标志。如果在下一个复位周期，自举程序检测到标志仍置 1，它将假定新映像未正确运行或测试失败。然后，自举程序必须从备份映像（如果可用）执行恢复。

Microchip 网站

Microchip 网站 <http://www.microchip.com/> 为客户提供在线支持。客户可通过该网站方便地获取文件和信息。只要使用常用的互联网浏览器即可访问，网站提供以下信息：

- **产品支持**——数据手册和勘误表、应用笔记和示例程序、设计资源、用户指南以及硬件支持文档、最新的软件版本以及归档软件
- **一般技术支持**——常见问题（FAQ）、技术支持请求、在线讨论组以及 Microchip 顾问计划成员名单
- **Microchip 业务**——产品选型和订购指南、最新 Microchip 新闻稿、研讨会和活动安排表、Microchip 销售办事处、代理商以及工厂代表列表

变更通知客户服务

Microchip 的变更通知客户服务有助于客户了解 Microchip 产品的最新信息。注册客户可在他们感兴趣的某个产品系列或开发工具发生变更、更新、发布新版本或勘误表时，收到电子邮件通知。

欲注册，请登录 Microchip 网站 <http://www.microchip.com/>。在“支持”（Support）下，点击“变更通知客户”（Customer Change Notification）服务后按照注册说明完成注册。

客户支持

Microchip 产品的用户可通过以下渠道获得帮助：

- 代理商或代表
- 当地销售办事处
- 应用工程师（FAE）
- 技术支持

客户应联系其代理商、代表或应用工程师（FAE）寻求支持。当地销售办事处也可为客户提供帮助。本文档后附有销售办事处的联系方式。

也可通过以下网站获得技术支持：<http://www.microchip.com/support>

Microchip 器件代码保护功能

请注意以下有关 Microchip 器件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指标。
- Microchip 确信：在正常使用的情况下，Microchip 系列产品是当今市场上同类产品中最安全的产品之一。
- 目前，仍存在着恶意、甚至是非法破坏代码保护功能的行为。就我们所知，所有这些行为都不是以 Microchip 数据手册中规定的操作规范来使用 Microchip 产品的。这样做的人极可能侵犯了知识产权。
- Microchip 愿意与关心代码完整性的客户合作。
- 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。任何试图破坏 Microchip 代码保护功能的行为均可视为违反了《数字器件千年版权法案（Digital Millennium Copyright Act）》。如

果这种行为导致他人在未经授权的情况下，能访问您的软件或其他受版权保护的成果，您有权依据该法案提起诉讼，从而制止这种行为。

法律声明

提供本文档的中文版本仅为了便于理解。请勿忽视文档中包含的英文部分，因为其中提供了有关 Microchip 产品性能和使用情况的有用信息。Microchip Technology Inc.及其分公司和相关公司、各级主管与员工及事务代理机构对译文中可能存在的任何差错不承担任何责任。建议参考 Microchip Technology Inc.的英文原版文档。

本出版物中所述的器件应用信息及其他类似内容仅为您提供便利，它们可能由更新之信息所替代。确保应用符合技术规范，是您自身应负的责任。Microchip 对这些信息不作任何明示或暗示、书面或口头、法定或其他形式的声明或担保，包括但不限于针对其使用情况、质量、性能、适销性或特定用途的适用性的声明或担保。Microchip 对因这些信息及使用这些信息而引起的后果不承担任何责任。如果将 Microchip 器件用于生命维持和/或生命安全应用，一切风险由买方自负。买方同意在由此引发任何一切伤害、索赔、诉讼或费用时，会维护和保障 Microchip 免于承担法律责任，并加以赔偿。除非另外声明，否则在 Microchip 知识产权保护下，不得暗或以其他方式转让任何许可证。

商标

Microchip 的名称和徽标组合、Microchip 徽标、Adaptec、AnyRate、AVR、AVR 徽标、AVR Freaks、BesTime、BitCloud、chipKIT、chipKIT 徽标、CryptoMemory、CryptoRF、dsPIC、FlashFlex、flexPWR、HELDO、IGLOO、JukeBlox、KeeLoq、Kleer、LANCheck、LinkMD、maXStylus、maXTouch、MediaLB、megaAVR、Microsemi、Microsemi 徽标、MOST、MOST 徽标、MPLAB、OptoLyzer、PackeTime、PIC、picoPower、PICSTART、PIC32 徽标、PolarFire、Prochip Designer、QTouch、SAM-BA、SenGenuity、SpyNIC、SST、SST 徽标、SuperFlash、Symmetricom、SyncServer、Tachyon、TempTrackr、TimeSource、tinyAVR、UNI/O、Vectron 及 XMEGA 均为 Microchip Technology Inc.在美国和其他国家或地区的注册商标。

APT、ClockWorks、The Embedded Control Solutions Company、EtherSynch、FlashTec、Hyper Speed Control、HyperLight Load、IntelliMOS、Libero、motorBench、mTouch、Powermite 3、PrecisionEdge、ProASIC、ProASIC Plus、ProASIC Plus 徽标、Quiet-Wire、SmartFusion、SyncWorld、Temux、TimeCesium、TimeHub、TimePictra、TimeProvider、Vite、WinPath 和 ZL 均为 Microchip Technology Inc.在美国的注册商标。

Adjacent Key Suppression、AKS、Analog-for-the-Digital Age、Any Capacitor、AnyIn、AnyOut、BlueSky、BodyCom、CodeGuard、CryptoAuthentication、CryptoAutomotive、CryptoCompanion、CryptoController、dsPICDEM、dsPICDEM.net、Dynamic Average Matching、DAM、ECAN、EtherGREEN、In-Circuit Serial Programming、ICSP、INICnet、Inter-Chip Connectivity、JitterBlocker、KleerNet、KleerNet 徽标、memBrain、Mindi、MiWi、MPASM、MPF、MPLAB Certified 徽标、MPLIB、MPLINK、MultiTRAK、NetDetach、Omniscient Code Generation、PICDEM、PICDEM.net、PICkit、PICtail、PowerSmart、PureSilicon、QMatrix、REAL ICE、Ripple Blocker、SAM-ICE、Serial Quad I/O、SMART-I.S.、SQI、SuperSwitcher、SuperSwitcher II、Total Endurance、TSHARC、USBCheck、VariSense、ViewSpan、WiperLock、Wireless DNA 和 ZENA 均为 Microchip Technology Inc.在美国和其他国家或地区的商标。

SQTP 为 Microchip Technology Incorporated 在美国的服务标记。

Adaptec 徽标、Frequency on Demand、Silicon Storage Technology 和 Symmcom 为 Microchip Technology Inc.在除美国外的国家或地区的注册商标。

GestIC 为 Microchip Technology Inc.的子公司 Microchip Technology Germany II GmbH & Co. & KG 在除美国外的国家或地区的注册商标。

在此提及的所有其他商标均为各持有公司所有。

© 2019, Microchip Technology Incorporated 版权所有。

ISBN: 978-1-5224-4526-5

质量管理体系

有关 Microchip 质量管理体系的更多信息，请访问 www.microchip.com/quality。

全球销售及服务中心

美洲	亚太地区	亚太地区	欧洲
公司总部 2355 West Chandler Blvd. 钱德勒, 亚利桑那州 85224-6199 电话: 480-792-7200 传真: 480-792-7277 技术支持: http://www.microchip.com/support 网址: www.microchip.com	澳大利亚 - 悉尼 电话: 61-2-9868-6733 中国 - 北京 电话: 86-10-8569-7000 中国 - 成都 电话: 86-28-8665-5511 中国 - 重庆 电话: 86-23-8980-9588 中国 - 东莞 电话: 86-769-8702-9880 中国 - 广州 电话: 86-20-8755-8029 中国 - 杭州 电话: 86-571-8792-8115 中国 - 香港特别行政区 电话: 852-2943-5100 中国 - 南京 电话: 86-25-8473-2460 中国 - 青岛 电话: 86-532-8502-7355 中国 - 上海 电话: 86-21-3326-8000 中国 - 沈阳 电话: 86-24-2334-2829 中国 - 深圳 电话: 86-755-8864-2200 中国 - 苏州 电话: 86-186-6233-1526 中国 - 武汉 电话: 86-27-5980-5300 中国 - 西安 电话: 86-29-8833-7252 中国 - 厦门 电话: 86-592-2388138 中国 - 珠海 电话: 86-756-3210040	印度 - 班加罗尔 电话: 91-80-3090-4444 印度 - 新德里 电话: 91-11-4160-8631 印度 - 浦那 电话: 91-20-4121-0141 日本 - 大阪 电话: 81-6-6152-7160 日本 - 东京 电话: 81-3-6880-3770 韩国 - 大邱 电话: 82-53-744-4301 韩国 - 首尔 电话: 82-2-554-7200 马来西亚 - 吉隆坡 电话: 60-3-7651-7906 马来西亚 - 槟榔屿 电话: 60-4-227-8870 菲律宾 - 马尼拉 电话: 63-2-634-9065 新加坡 电话: 65-6334-8870 台湾地区 - 新竹 电话: 886-3-577-8366 台湾地区 - 高雄 电话: 886-7-213-7830 台湾地区 - 台北 电话: 886-2-2508-8600 泰国 - 曼谷 电话: 66-2-694-1351 越南 - 胡志明市 电话: 84-28-5448-2100	奥地利 - 韦尔斯 电话: 43-7242-2244-39 传真: 43-7242-2244-393 丹麦 - 哥本哈根 电话: 45-4450-2828 传真: 45-4485-2829 芬兰 - 埃斯波 电话: 358-9-4520-820 法国 - 巴黎 电话: 33-1-69-53-63-20 传真: 33-1-69-30-90-79 德国 - 加兴 电话: 49-8931-9700 德国 - 哈恩 电话: 49-2129-3766400 德国 - 海尔布隆 电话: 49-7131-72400 德国 - 卡尔斯鲁厄 电话: 49-721-625370 德国 - 慕尼黑 电话: 49-89-627-144-0 传真: 49-89-627-144-44 德国 - 罗森海姆 电话: 49-8031-354-560 以色列 - 若那那市 电话: 972-9-744-7705 意大利 - 米兰 电话: 39-0331-742611 传真: 39-0331-466781 意大利 - 帕多瓦 电话: 39-049-7625286 荷兰 - 德卢内市 电话: 31-416-690399 传真: 31-416-690340 挪威 - 特隆赫姆 电话: 47-72884388 波兰 - 华沙 电话: 48-22-3325737 罗马尼亚 - 布加勒斯特 电话: 40-21-407-87-50 西班牙 - 马德里 电话: 34-91-708-08-90 传真: 34-91-708-08-91 瑞典 - 哥德堡 电话: 46-31-704-60-40 瑞典 - 斯德哥尔摩 电话: 46-8-5090-4654 英国 - 沃金厄姆 电话: 44-118-921-5800 传真: 44-118-921-5820
亚特兰大 德卢斯, 佐治亚州 电话: 678-957-9614 传真: 678-957-1455 奥斯汀, 德克萨斯州 电话: 512-257-3370 波士顿 韦斯特伯鲁, 马萨诸塞州 电话: 774-760-0087 传真: 774-760-0088 芝加哥 艾塔斯卡, 伊利诺伊州 电话: 630-285-0071 传真: 630-285-0075 达拉斯 阿迪森, 德克萨斯州 电话: 972-818-7423 传真: 972-818-2924 底特律 诺维, 密歇根州 电话: 248-848-4000 休斯顿, 德克萨斯州 电话: 281-894-5983 印第安纳波利斯 诺布尔斯维尔, 印第安纳州 电话: 317-773-8323 传真: 317-773-5453 电话: 317-536-2380 洛杉矶 米镇维荷, 加利福尼亚州 电话: 949-462-9523 传真: 949-462-9608 电话: 951-273-7800 罗利, 北卡罗来纳州 电话: 919-844-7510 纽约, 纽约州 电话: 631-435-6000 圣何塞, 加利福尼亚州 电话: 408-735-9110 电话: 408-436-4270 加拿大 - 多伦多 电话: 905-695-1980 传真: 905-695-2078			