灵活更新固件——IoT 设备的关键

Microchip Technology Inc.

存储器产品部

主任应用工程师

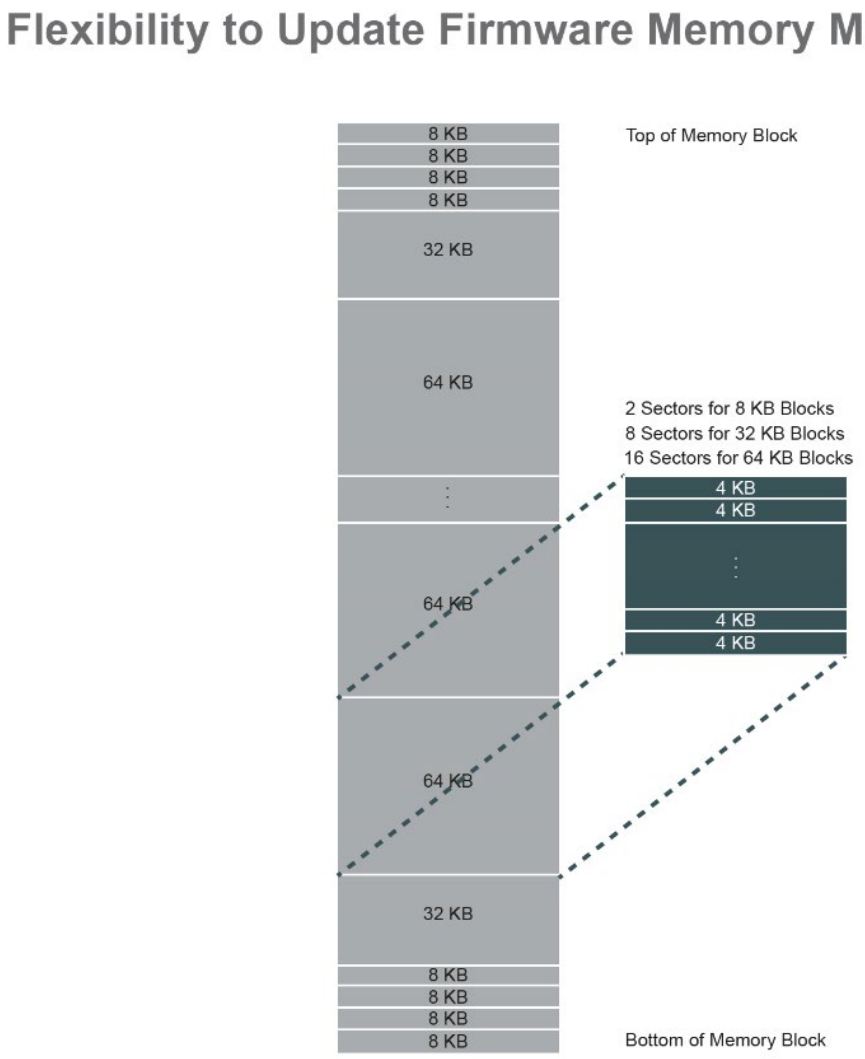
Hardik Patel

物联网（IoT）设备正迅速引入各大市场，从家用电器到医疗设备、再到汽车，应用范围十分广泛；制造商必须通过不断创新和灵活地采用或集成新技术来领先于竞争对手。为了满足新功能的需求和新法规的要求，设计人员必须将灵活性纳入其产品中，以适应不断发展的 IoT 生态系统。固件更新不仅能够在客户现场的初始部署期间进行定制，还可以在产品部署到现场后添加新功能/特性，并且支持在使用过程中修复任何固件问题。NOR 闪存等非易失性存储器件具有可重复编程能力且可靠性极高，通常可用作固件代码存储介质。通过重新编写器件固件代码（位于器件使用的非易失性存储器中）的一部分，制造商可轻松更新器件功能。想要更新固件时，有三件事情需要考虑：更新哪些/多少代码、更新频率以及执行更新所需的时间（速度）。

更新哪些/多少固件代码

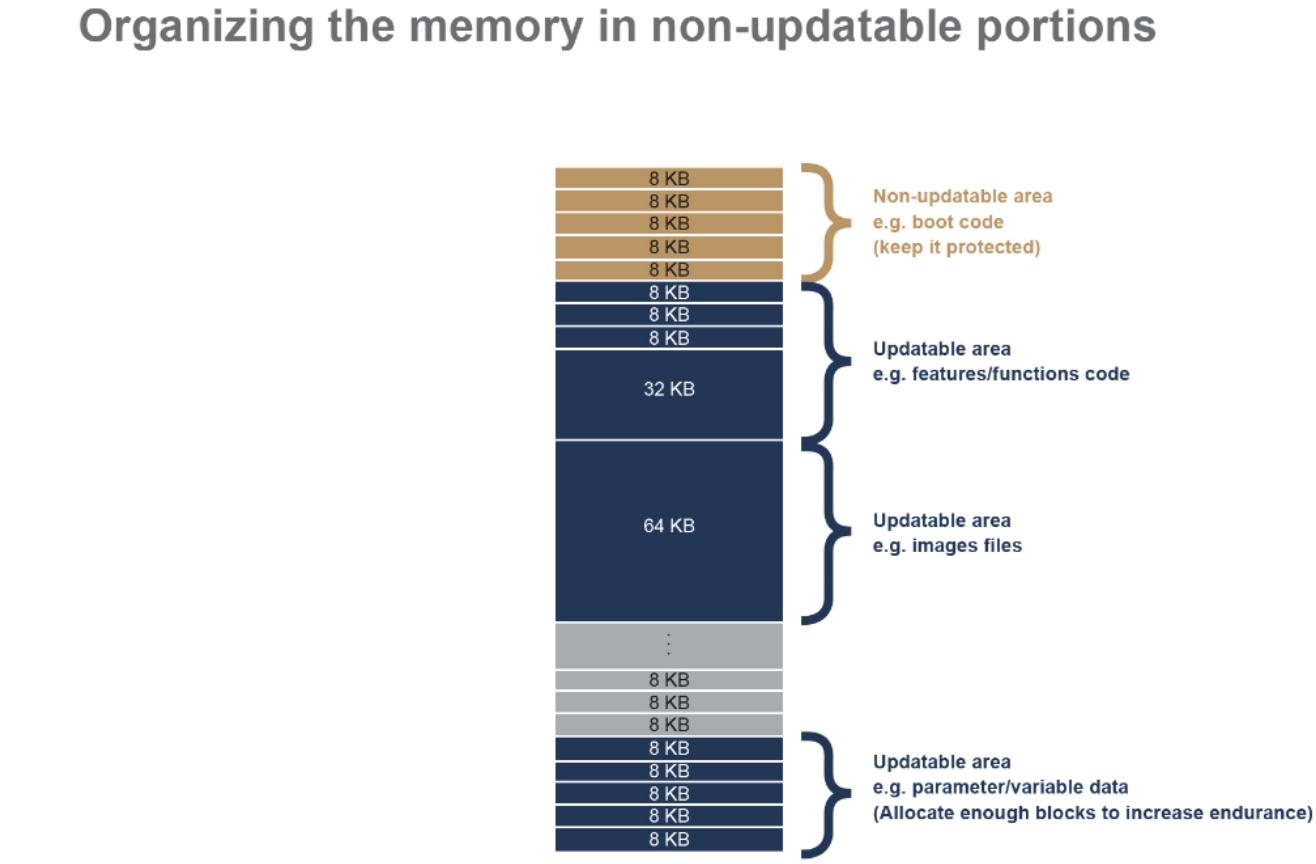
在 IoT 设备的初始设计阶段，必须考虑更新哪些/多少固件代码。相对于不可更新部分，固件的可更新部分必须存储在 NOR 闪存器件的独立区域中。更新 NOR 闪存的任何片段都需要先擦除存储器的这一部分，然后将新信息编程到该部分中。NOR 闪存分为称为扇区和块的多个部分，它们的大小各有不同。NOR 闪存器件（如采用 SST SuperFlash®技术的器件（部件编号 SST26VF064B（64 Mb））分为多个均一的 4 KB 扇区，各个扇区可单独擦除和重新编程（4 KB = 4 * 1024 * 8 位 = 32,762 位）。它还可分为更大的 8 KB、32 KB 和 64 KB 块，这些块也可单独擦除。因此，一个 8 KB 块有 2 个扇区，一个 32 KB 块有 8 个扇区，一个 64 KB 块有 16 个扇区。图 1 给出了采用 8 KB/32 KB/64 KB 块的 SST26VF064B 的存储器构成。各个块也可以单独进行保护。在对闪存的任何部分执行任何更新前，必须取消保护该部分中的块，以允许擦除和编程操作。完成更新后，谨慎地再次对这些块进行保护，以避免意外写入或擦除这些区域。固件的可更新部分必须以足够灵活的方式划分为扇区和块，以便同时支持有限数量和最大数量的特性/功能更新。由于执行更新的速度由需要擦除和重新编程的扇区和块数决定，因此在组

织固件的可更新部分时，最好同时考虑速度和灵活性。图 2 给出了将存储器组织为可更新和不可更新部分的示例。引导代码等不可更新部分存储在受保护区域中。固件的可更新部分（如特性/功能）根据灵活性要求分为较小的块或较大的块。可更新的镜像文件存储在较大的块中，可更新的变量/参数存储在较小的块中。



Flexibility to Update Firmware Memory Map	灵活更新固件存储器映射
Top of Memory Block	存储器块顶部
2 Sectors for 8 KB Blocks 8 Sectors for 32 KB Blocks 16 Sectors for 64 KB Blocks	8 KB 块对应 2 个扇区，32 KB 块对应 8 个扇区，64 KB 块对应 16 个扇区
Bottom of Memory Block	存储器块底部

图 1：SST26VF064B 的存储器构成（映射）——由 8 个 8 KB 块、2 个 32 KB 块和 126 个 64 KB 块组成



Organizing the memory in non-updatable portions	将存储器组织为多个不可更新部分
Non-updatable area e.g. boot code (keep it protected)	不可更新区域，例如引导代码（进行保护）
Updatable area e.g. features/functions code	可更新区域，例如特性/功能代码
Updatable area e.g. images files	可更新区域，例如镜像文件
Updatable area e.g. parameter/variable data (Allocate enough blocks to increase endurance)	可更新区域，例如参数/变量数据（分配足够的块以提高耐擦写次数）

图 2：将存储器组织为多个不可更新部分（例如：引导代码）和可更新部分（例如：功能/特性代码、镜像文件代码和参数变量代码）

更新频率

固件更新频率的主要限制是应用中所使用存储器的耐擦写次数限制。SuperFlash 技术存储器（如 SST26VF064B）的耐擦写次数可达 100,000 次，这意味着每个扇区可编程和擦除 100,000 次。固件可以更新 100,000 次听起来很多；然而，许多 IoT 设备会在使用期间收集数据并将信息存储在 NOR 闪存中，因此在计算最大耐擦写次数限制时必须考虑这一点。考虑到耐擦写次数，必须在存储器中分配足够多的扇区。下面将举例说明：假设 IoT 设备正在收集和存储 16 个字节的信息，并且信息预计在产品的使用寿命期间收集和存储 1 亿次。可以按如下方式计算应当分配的扇区数：

1 个扇区 = 4 KB

假设扇区中的所有地址单元用于存储信息（一次存储 16 个字节的数据），然后写入到一个新的地址单元，直至达到扇区末尾（例如，0x0000-0x000F、0x0010-0x001F、0x0020-0x002F 等）

由于 4 KB/16 字节 = 256，这即是达到扇区容量并擦除扇区中任何数据之前可以写入存储介质的次数

1 个扇区的耐擦写限值 = 100,000 次

因此，如果 1 个扇区可以写入 256 次且耐擦写次数为 100,000 次，则可以收集和存储数据 2560 万次

如果一个应用需要收集和存储数据 1 亿次，则要分配的扇区数量为 100,000,000/25,600,000 = 3.9。因此，在本例中，需要分配 4 个扇区以在应用的生命周期内存储 16 个字节的数据。

IoT 设备工程师需要进行类似的计算，以便为数据记录参数分配足够多的扇区和块，以免超出其 NOR 闪存器件的耐擦写限值。

更新速度

可根据需要擦除和重新编程的块和扇区数来计算更新速度。假设需要重新编程 SST26VF064B 的几个 64 KB 块中存储的 1 Mb、2 Mb 或 4 Mb 固件代码/数据。代码/数据可以由固件代码、镜像文件或需要更新的其他代码组成。更新过程涉及对闪存执行一系列命令指令。序列将从取消保护存储器块开始，然后擦除这些块、用更新的数据/代码进行编程，最后重新进行保护。对于 SST26VF064B，更新 1 Mb/2 Mb/4 Mb 存储器所需的指令序列如表 1 所示。从表 1 中可以看出，两个最重要的时间是擦除时间和编程时间。

SST26VF064B 采用可提供出色擦除性能的 SuperFlash 技术。SuperFlash 技术与传统闪存的擦除和编程性能的比较如表 2 所示。与传统闪存相比，SuperFlash 技术提供的优异擦除性能对于缩短更新时间非常有用。SST26VF064B 支持的最大时钟频率为 104 MHz，最大扇区擦除时间为 25 ms，最大块擦除时间为 25 ms，最大页编程时间为 1.5 ms。此外，从发出每条命令指令到闪存以 104 MHz 时钟频率工作，中间还需要 12 ns 延时（CE 高电平时间）。表 1 所示的命令序列与编程和擦除时间的知识结合使用时，可计算更新 1 Mb/2 Mb/4 Mb SuperFlash 技术存储器和传统闪存所需的时间，具体方法分别如表 3 和表 4 所示。这些计算必须由 IoT 设备工程师完成以估算执行更新的速度，目的是最大程度缩短更新期间的 IoT 设备停机时间。

Steps	Instruction Sequence for Commands	Number of Clocks
1	SPI_WREN	8
2	SPI_Enable_Quad_IO	8
3	SQI_WREN	2
4	SQI_ Write Block Protection Register (to unprotect portion of Flash)	38
5	SQI_Block Erase 64 KB blocks	2
6	SQI_WREN	8
7	**Wait 25 ms for completion of erase for SuperFlash technology memory (or 3000 ms for conventional Flash memory)**	
	Repeat steps 5, 6 and 7 till the required amount of memory is erased	
	To erase 1 Mb of data, steps 5, 6 and 7 will need to be repeated for (1024*1024)/(64*1024*8) = 2 times	
	To erase 2 Mb of data, steps 5, 6 and 7 will need to be repeated for (2*1024*1024)/(64*1024*8) = 4 times	
	To erase 4 Mb of data, steps 5, 6 and 7 will need to be repeated for (4*1024*1024)/(64*1024*8) = 8 times	
8	SQI_WREN	2
9	SQI_Page program command followed by programming 256 bytes of data (260 multiplied by 2)	520
10	**Wait 1.5 ms for completion of page programming for SuperFlash technology memory (or 5 ms for conventional Flash memory)**	
	Repeat steps 8, 9 and 10 until all the data is written	
	To program 1 Mb of data, steps 8, 9 and 10 will need to repeated for 1024*1024/8 divided by 256 = 512 times	
	To program 2 Mb of data, steps 8, 9 and 10 will need to repeated for 2*1024*1024/8 divided by 256 = 1024 times	
	To program 4 Mb of data, steps 8, 9 and 10 will need to repeated for 4*1024*1024/8 divided by 256 = 2048 times	
11	SQI_WREN	2
12	SQI_Write Block Protection Register (to again protect the portion of Flash)	38

步骤	命令指令序列	时钟数
1	SPI_WREN	8
2	SPI_Enable_Ouad_IO	8
3	SQI_WREN	2
4	SQI_写块保护寄存器（取消保护闪存的某个部分）	38
5	SQI_块擦除 64 KB 块	2
6	SQI_WREN	8
7	等待 25 ms 来完成 SuperFlash 技术存储器的擦除（对于传统闪存的擦除，需等待 3000 ms）	
	重复执行步骤 5、6 和 7，直到所需大小的存储空间擦除完毕	
	要擦除 1 Mb 的数据，步骤 5、6 和 7 需要重复 (1024*1024)/(64*1024*8) = 2 次	
	要擦除 2 Mb 的数据，步骤 5、6 和 7 需要重复 (2*1024*1024)/(64*1024*8) = 4 次	
	要擦除 4 Mb 的数据，步骤 5、6 和 7 需要重复 (4*1024*1024)/(64*1024*8) = 8 次	
8	SQI_WREN	2
9	SQI_页编程命令后将编程 256 字节的数据（260 乘以 2）	520
10	等待 1.5 ms 来完成 SuperFlash 技术存储器的页编程（对于传统闪存的擦除，需等待 5 ms）	
	重复步骤 8、9 和 10，直到写入所有数据	
	要编程 1 Mb 的数据，步骤 8、9 和 10 需要重复 1024*1024/8/256 = 512 次	
	要编程 2 Mb 的数据，步骤 8、9 和 10 需要重复 2*1024*1024/8/256 = 1024 次	
	要编程 4 Mb 的数据，步骤 8、9 和 10 需要重复 4*1024*1024/8/256 = 2048 次	
11	SQI_WREN	2
12	SQI_写块保护寄存器（用于再次保护闪存的某一部分）	38

表 1：更新 1 Mb/2 Mb/4 Mb 存储器的闪存命令指令序列

	SST26VF064B	Conventional Flash
Sector erase	25 ms (max)	150 ms to 3000 ms
Block erase	25 ms (max)	750 ms to 3 s
Chip erase	50 ms (max)	15 s to 80 s
Page program	1.5 ms (max)	1 ms to 5 ms

	SST26VF064B	传统闪存
扇区擦除	25 ms（最长）	150 ms 至 3000 ms
块擦除	25 ms（最长）	750 ms 至 3s
芯片擦除	50 ms（最长）	15s 至 80s
页编程	1.5 ms（最长）	1 ms 至 5 ms

表 2：SST26VF064B 和传统闪存的编程和擦除时间

Calculations	Time
Maximum block erase time	25 ms
Maximum page program time	1.5 ms
Clock period for 104 Mhz frequency	9.6 ns
CE high time between each instruction for 104 Mhz	12 ns
Time A. Time for instruction 1 to 4 = (56 clocks * period) + (3 * CE high times)	573.6 ns
Time B. Time for instruction 5 to 7 = (10 clocks * period) + (2 * CE high times) + (25ms wait for block erase)	25000120 ns
Time C. Time for instruction 8 to 10 = (522 clocks * period) + (1 * CE high time) + (1.5 ms wait for page program)	1505023.2 ns
Time D. Time for instruction 11 to 12 = (40 clocks * period) + (1 * CE high time)	396 ns
Total time for all the instructions for block erase and programming 1 Mb of data = (Time A) + (Time B * 2) + (Time C * 512) + (Time D)	**0.820573088 s**
Total time for all the instructions for block erase and programming 2 Mb of data = (Time A) + (Time B * 4) + (Time C * 1024) + (Time D)	**1.641145206 s**
Total time for all the instructions for block erase and programming 4 Mb of data = (Time A) + (Time B * 8) + (Time C * 2048) + (Time D)	**3.282289443 s**

计算	时间
最长块擦除时间	25 ms
最长页编程时间	1.5 ms
104 MHz 频率下的时钟周期	9.6 ns
104 MHz 频率下各指令间的 CE 高电平时间	12 ns
时间 A. 指令 1 至指令 4 的时间 = (56 个时钟 * 周期) + (3 * CE 高电平时间)	573.6 ns
时间 B. 指令 5 至指令 7 的时间 = (10 个时钟 * 周期) + (2 * CE 高电平时间) + (25 ms 块擦除等待时间)	25000120 ns
时间 C. 指令 8 至指令 10 的时间 = (522 个时钟 * 周期) + (1 * CE 高电平时间) + (1.5 ms 页编程等待时间)	1505023.2 ns
时间 D. 指令 11 至指令 12 的时间 = (40 个时钟 * 周期) + (1 * CE 高电平时间)	396 ns
总时间（即，块擦除和编程 1 Mb 数据的全部指令的时间）= (时间 A) + (时间 B * 2) + (时间 C * 512) + (时间 D)	0.820573088 s
块擦除和编程 2 Mb 数据的全部指令的总时间 = (时间 A) + (时间 B * 4) + (时间 C * 1024) + (时间 D)	1.641145206 s
块擦除和编程 4 Mb 数据的全部指令的总时间 = (时间 A) + (时间 B * 8) + (时间 C * 2048) + (时间 D)	3.282289443 s

表 3：更新 1 MB/2 Mb/4 Mb SuperFlash 技术存储器所需的时间

Calculations	Time
Maximum block erase time	3000 ms
Maximum page program time	5 ms
Clock period for 104 Mhz frequency	9.6 ns
CE high time between each instruction for 104 Mhz	20 ns
Time A. Time for instruction 1 to 4 = (56 clocks * period) + (3 * CE high times)	597.6 ns
Time B. Time for instruction 5 to 7 = (10 clocks * period) + (2 * CE high times) + (3000 ms wait for block erase)	3000000136 ns
Time C. Time for instruction 8 to 10 = (522 clocks * period) + (1 * CE high time) + (5 ms wait for page program)	5005031.2 ns
Time D. Time for instruction 11 to 12 = (40 clocks * period) + (1 * CE high time)	404 ns
Total time for all the instructions for block erase and programming 1 Mb of data = (Time A) + (Time B * 2) + (Time C * 512) + (Time D)	**8.562577248 s**
Total time for all the instructions for block erase and programming 2 Mb of data = (Time A) + (Time B * 4) + (Time C * 1024) + (Time D)	**17.12515349 s**
Total time for all the instructions for block erase and programming 4 Mb of data = (Time A) + (Time B * 8) + (Time C * 2048) + (Time D)	**34.25030599 s**

计算	时间
最长块擦除时间	3000 ms
最长页编程时间	5 ms
104 MHz 频率下的时钟周期	9.6 ns
104 MHz 频率下各指令间的 CE 高电平时间	20 ns
时间 A. 指令 1 至指令 4 的时间 = (56 个时钟 * 周期) + (3 * CE 高电平时间)	597.6 ns
时间 B. 指令 5 至指令 7 的时间 = (10 个时钟 * 周期) + (2 * CE 高电平时间) + (3000 ms 块擦除等待时间)	3000000136 ns
时间 C. 指令 8 至指令 10 的时间 = (522 个时钟 * 周期) + (1 * CE 高电平时间) + (5 ms 页编程等待时间)	5005031.2 ns
时间 D. 指令 11 至指令 12 的时间 = (40 个时钟 * 周期) + (1 * CE 高电平时间)	404 ns
块擦除和编程 1 Mb 数据的全部指令的总时间 = (时间 A) + (时间 B * 2) + (时间 C * 512) + (时间 D)	8.562577248 s

块擦除和编程 2 Mb 数据的全部指令的总时间 = (时间 A) + (时间 B * 4) + (时间 C * 1024) + (时间 D)	17.12515349 s
块擦除和编程 4 Mb 数据的全部指令的总时间 = (时间 A) + (时间 B * 8) + (时间 C * 2046) + (时间 D)	34.25030599 s

表 4：更新 1 MB/2 Mb/4 Mb 传统闪存所需的时间

结论

IoT 设备设计工程师需要在更新应用程序代码和数据时提供一定的灵活性。更新哪些/多少代码、更新频率和更新速度是设计 IoT 设备时需要解决的问题。非易失性存储器的选择会影响这些问题，并在计算代码更新的时间和速度方面起到关键作用。